IMPORTANT NOTICE:

This Publication may contain

SAFETY NOTICES or WARNING PAGES

if so, please read before using this publication

AUSTRALIAN DEFENCE FORCE

AUSTRALIAN AIR PUBLICATION

7001.054

AIRWORTHINESS DESIGN REQUIREMENTS MANUAL

Date of Issue: 06 Jun 07

(G.D. SHEPHERD)
Air Marshal
Chief of Air Force

Sponsor: DAIRENG-DGTA

File Reference: SCI/4560/7001/054

RESPONSIBILITIES OF DISTRIBUTEE

AMENDMENTS TO PUBLICATIONS

1. This publication, although issued as an Australian Air Publication (AAP), is authenticated by the ADF Airworthiness Authority because the contents has Tri-Service significance and authority. The single Service markings on the front of the book have been replaced by their Tri-Service equivalents as an interim step toward the formation of a proper, structured, binding Defence Publication System for airworthiness, aircraft, aircraft related equipment and other 'air' matters.

2. Attention is drawn to DI(AF) ADMIN 6–8 in regard to amending this publication. In particular the member to whom this publication is on 'temporary issue' is personally responsible for:

a. keeping it up to date in accordance with amendment lists issued from time to time, and

b. producing it for inspection when required.

3. AAP 5030.001 RAAF Publication System Technical and Non-Technical Manuals, outlines procedures for the incorporation of amendment lists. In particular the distributee is to:

a. acknowledge receipt of ALs by signing the attached DEFPUBS Issue Note and returning it to the library/Technical Publication Office (TPO) promptly,

b. check the amendment certificate to ensure all previous ALs have been incorporated,

c. incorporate the amendment list in accordance with Section 5, Chapter 2, and

d. action the amendment certificate incorporated in this publication.

PLEASE CUT OUT

SPINE CARD

ON THE LINES PROVIDED

cut here

AIRWORTHINESS DESIGN REQUIREMENTS MANUAL

AUSTRALIAN AIR PUBLICATION 7001.054

cut here

LIST OF EFFECTIVE PAGES

Page No	AL
Section 2 (Cont)	
CHAPTER 8	
1 to 6	0
8A–1 to 8A–2	0
CHAPTER 9	
1 to 4	0
CHAPTER 10	
1 to 4	0
10A-1 to 10A-2	0
10B-1 to 10B-2	0
CHAPTER 11	
1 to 18	0
11A–1 to 11A–2	0
11B–1 to 11B–6	0
11C–1 to 11C–12	0
11D–1 to 11D–2	0
11E–1 to 11E–4	0
11F-1 to 11F-10	0
11F1-1 to 11F1-2	0
11G-1 to 11G-2	0
11H-1 to 11H-8	0
11I-1 to 11I-2	0
11J to 11J-2	0
11K-1 to 11K-2	0
11L-1 to 11L-4	0
11M-1 to 11M-2	0
CHAPTER 12	
1 to 2	0
CHAPTER 13	
1 to 4	0
13A–1 to 13A–2	0
13B–1 to 13B–2	0
13C–1 to 13C–4	0
13D–1 to 13D–2	0
CHAPTER 14	
1 to 8	0
CHAPTER 15	
1 to 6	0
15A–1 to 15A–2	0
15B–1 to 15B–2	0
15C–1 to 15C–2	0
15D–1 to 15D–4	0
CHAPTER 16	
1 to 4	0
16A-1 to 16A-2	0
CHAPTER 17	
1 to 6	0
17A–1 to 17A–6	0
CHAPTER 18	
1 to 4	0
18A–1 to 18A–2	0
18B–1 to 18B–2	0
CHAPTER 19	
1 to 4	0
19A–1 to 19A–2	0
19B-1 to 19B-4	0
CHAPTER 20	
1 to 6	0
CHAPTER 21	
1 to 4	0
21A–1 to 21A–4	0
SECTION 3 (Interleaf)	
CHAPTER 1	
1 to 4	0
3A-1 to 3A-2	0
SECTION 4 (Interleaf)	
CHAPTER 1	
1 to 8	0
1A–1 to 1A–2	0
1B–1 to 1B–2	0
1C–1 to 1C–4	0
1D–1 to 1D–4	0
1E–1 to 1E–8	0
1E1-1 to 1E1-2	0
1F–1 to 1F–2	0
1G–1 to 1G–2	0
POST PAGES	
List of Abbreviations 1 to 6	0

COMPLIANCE CERTIFICATE

Certified that the publication has been page checked in accordance with the details on this page.

.....Signature (Distributee)

.....Rank or Title and Name

Date..... .....Appointment and Unit or Section

Blank Page

NOTES TO READERS

This publication, although issued as an Australian Air Publication (AAP), is authenticated by the ADF Airworthiness Authority because the content has Tri-Service significance and authority. The single Service markings on the front of the book have been replaced by their Tri-Service equivalents as an interim step towards the formation of a proper, structured, binding Defence Publication System for airworthiness, aircraft, aircraft related equipment and other 'air' matters.

Attention is drawn to DI(AF) ADMIN 6–8 in regard to amending this publication.

DI(AF) LOG, STIs and Modifications may affect the subject matter of this publication. When such orders or instructions contradict any part of this publication they are to be taken as the overriding authorities. Where a Technical Maintenance Plan (TMP) indicates servicing periodicities at variance with those detailed in this publication, the TMP is at all times the overriding authority.

Reference to items of equipment in this publication does not constitute authority for demanding of the items. Prior to demanding reference should always be made to the appropriate Topic –4 (IPB) and RAAF List of Assessed Spares (LOAS).

This AAP is managed in accordance with AAP 5030.001, RAAF Publication System Technical and Non-Technical Manuals. Reference is to be made to this publication for Unit management of AAPs and for procedures for requesting additional copies of AAPs and Amendments.

Blank Page

TABLE OF CONTENTS

LIST OF FIGURES

Blank Page

LIST OF TABLES

Blank Page

SECTION 1

CHAPTER 1

THE APPLICATION OF DESIGN REQUIREMENTS

INTRODUCTION

1. Airworthiness design requirements, including where appropriate the means of demonstrating compliance, are prescribed by the Technical Airworthiness Regulator (TAR) for the purpose of establishing adequate levels of safety for the design of aircraft, engines, propellers and other aircraft equipment. AAP 7001.053, the Technical Airworthiness Management Manual (TAMM), recognises AAP 7001.054 as the TAR's repository for ADF airworthiness design requirements.

2. ***Purpose.*** This publication provides guidance on the application of airworthiness design requirements within the ADF design acceptance process. It is intended for reference by project staff involved in the acquisition or modification of ADF aircraft, and engineers involved in design changes to ADF aircraft or aircraft systems. At the project manager's discretion it may also provide useful guidance to Contractors in the establishment and completion of airworthiness certification bases.

3. ***Context.*** Until 2004, Section 1 of this publication provided comprehensive guidance on establishing certification bases for ADF aircraft acquisitions and major design changes. This information has now been revised and relocated to AAP 7001.053 Section 3 Chapter 12. To provide context to this publication, it should be read in conjunction with the AAP 7001.053 chapter.

4. ***Design Standards versus Design Requirements.*** This publication refers to both 'design requirements' and 'design standards', which may appear to the reader to be interchangeable. This is often, but not always, the case. The latter specifically refers to a standard published by a civilian or military standards body, for example a US MIL STD or an RTCA standard. The TAR's design requirements, on the other hand, may refer to a single item ("PVC wiring shall not be used on ADF aircraft"), the adoption of a complete design standard ("The TAR's preferred standard for aircraft wiring is SAE AS 50881") or the adoption of a tailored version of a design standard.

ADF DESIGN REQUIREMENTS

5. It is not practical for the ADF to create and maintain its own aircraft design standards; it therefore relies extensively on design standards produced by other civilian and military agencies. Some of these design standards are comprehensive and directly applicable to the ADF. Others may meet many of our requirements, but require supplementation or tailoring to account for:

a. the ADF's particular Configuration, Role and/or operating Environment (CRE);

b. deficiencies in the level of safety provided by the design standard, detected by the ADF through local research or experience (eg investigations into aircraft incidents);

c. intentional ambiguities in the design standard, where it is assumed the standard will be tailored to meet the needs of the specific application; or

d. the ADF's particular approach to through-life support.

6. This publication documents the TAR's preferred design standards, and any tailoring they require to overcome shortfalls. Further, it expounds the TAR's underlying design philosophy for key aircraft technologies or functions, to assist in the evaluation of alternate design standards that might be proposed by Tenderers. Finally, it provides suggested clauses and Data Item Descriptions for insertion into the aircraft acquisition or modification Statements of Requirement.

7. The chapters in this publication are broadly partitioned along aircraft functional lines (eg oxygen, structures, propulsion) or technology lines (eg software, system safety, E^3). Not all aircraft functions are captured in this publication; rather, coverage is limited to those areas where there is potential for the issues in paragraph 5 to become

relevant. For those omitted aircraft functions, common aerospace standards that are accepted by ADF-recognised Airworthiness Authorities will likely provide an adequate level of safety.

Mandatory or Optional ?

8. The ADF, as an independent Airworthiness Authority, interprets and sets standards to assure the airworthiness of State aircraft. DI(G) OPS 2-2 delegates to the TAR the authority to interpret technical airworthiness regulations in the context of specific aircraft designs, and recognises AAP 7001.054 as providing guidance on the application of airworthiness design requirements. The TAR accomplishes this charter by documenting preferred design requirements in AAP 7001.054, but on the understanding that their adoption is not mandatory; in every case, the intention is that Tenderers should be allowed to propose compliance with an alternative condition, provided that the alternative condition can be shown to the ADF's satisfaction to provide an adequate level of safety.

9. Historically, Projects have had difficulty grasping this concept of an 'adequate level of safety' - does it mean the level of safety must be equivalent to the ADF's preferred standard, or merely that it has been accepted as safe by a recognised Airworthiness Authority ? In fact, the TAR's interpretation lies somewhere in between. A good example is polyimide (eg Kapton®) wiring: while civilian Airworthiness Authorities still allow its use, clearly there are 'safer' wire types available for ADF aircraft (although an alternate wire type might impose an unacceptable weight or cost burden). Accordingly, while the TAR's preference is for any alternative condition proposed by a Tenderer to provide an 'equivalent level of safety' to the design requirements in this publication, a lesser (but still adequate) level of safety may be negotiated.

10. So, the airworthiness design requirements in this publication are neither mandatory nor optional. Rather, the TAR expects Project Offices to provide a reasoned justification (assessing factors such as safety impact, cost, engineering complexity, incompatibility with existing systems, standardisation, and so on), if they wish to accept a tendered design that does not provide the level of safety provided by the design requirements in this publication. This is often relevant to aircraft acquisition projects (since the cost of re-engineering existing systems may be cost-prohibitive), but is more difficult to justify for major design changes.

Design Standards for Mission Systems

11. Civilian aircraft design standards primarily focus on ensuring new or modified aircraft are adequately 'airworthy' in their intended CRE. For military aircraft, on the other hand, it is of almost equal importance that they are 'fit-for-purpose', that is, capable of performing their intended function in the worst-case operational CRE. Inadequate mission system integrity may result in mission failure, or may even have safety implications in a hostile environment (hence the concept of 'missionised hazards').

12. One means of assuring adequate mission system integrity is to apply the same airworthiness design requirements to mission systems. However, this is often impractical and can become cost-prohibitive. Rather, a balanced approach often needs to be adopted, one that acknowledges the importance of mission systems but accepts that a level of integrity less than that of safety-critical aircraft systems may be necessary. Key technology chapters in this publication explicitly examine how airworthiness design requirements may be tailored for mission systems.

Non-aircraft Systems

13. Design requirements for simulators, mission planning systems and other non-aircraft systems are not covered in this publication. Rather, where those systems interface (either directly or indirectly) with the aircraft, their airworthiness impact should be assessed via the aircraft system safety program. Should this program highlight hazards that cannot effectively be mitigated by operational means, DGTA staff are able to provide advice on establishing and tailoring design requirements to improve the integrity of the non-aircraft systems.

Interoperability

14. The ADF's interoperability requirements are largely managed through the Air Standardisation Coordination Committee (ASIC) series of standards. While some references to ASIC standards and other interoperability issues are mentioned in this publication, interoperability is not comprehensively covered. A specific interoperability chapter is being considered for a future amendment; in the meantime, project offices (particularly for new acquisitions) should assess their particular interoperability requirements by reviewing the ASIC standards. Assistance in this process may be obtained from the Coordinating Member for ASIC Working Party 25 (which covers engineering and logistics), AMPTS-DGTA.

Chapter Sponsors

15. Each chapter in Section 2, 3 and 4 of this publication is sponsored by a relevant ADF Centre of Expertise or DGTA section. Annex A lists these sponsors, who are the first point of contact for assistance, requests for interpretation or suggestions for improvement.

Annex:

A. AAP 7001.054 Chapter Sponsors

Blank Page

AAP 7001.054 CHAPTER SPONSORS

1. Each chapter in this publication is sponsored by a relevant ADF Centre of Expertise or DGTA section. Table 1-A-1 lists these sponsors, who should be the first point of contact for assistance, requests for interpretation or suggestions for amendment.

Table 1–A–1 Chapter Sponsors

	TITLE	SPONSOR
Section 1:		
Chapter 1	The Application of Design Requirements	OIC SCI-DGTA
Chapter 2	Design, Equipage and Certification Issues for Civil Certified ADF Aircraft	OIC SCI-DGTA
Section 2:		
Chapter 1	Systems Safety	SCI3-DGTA
Chapter 2	Electromagnetic Environmental Effects in Airborne Systems	SCI2-DGTA
Chapter 3	General Avionics Systems	SCI2-DGTA
Chapter 4	Aircraft Lighting	SCI2-DGTA
Chapter 5	Electrical Power Generation, Storage and Distribution	SCI2-DGTA
Chapter 6	Oxygen Systems	SCI2-DGTA
Chapter 7	Software for Airborne and Related Systems	SCI1-DGTA
Chapter 8	Embedded Computer Systems	SCI1-DGTA
Chapter 9	Flight Control Systems and Aircraft Dynamics	DSDE Flight Dynamics AOSG
Chapter 10	Aircraft Mechanical Systems	ESI-DGTA
Chapter 11	Aircraft Structural Integrity	ASI-DGTA
Chapter 12	Aircraft / Stores Compatibility	DASCENG
Chapter 13	Human Factors Engineering	SCI3-DGTA
Chapter 14	Role Equipment	SCI2-DGTA
Chapter 15	Unmanned Aerial Vehicles	OIC SCI-DGTA
Chapter 16	Crash Protection	OIC SCI-DGTA
Chapter 17	In-Service Management of Software Product	SCI1-DGTA
Chapter 18	Carriage of Portable Electronic Devices	SCI2-DGTA
Chapter 19	Health and Usage Monitoring Systems	ESI-DGTA
Chapter 20	Aeronautical Life Support Equipment	SDE ALSLMU
Chapter 21	Airborne Environmental Control Systems	SCI2-DGTA
Section 3:		
Chapter 1	Rotorcraft	RWS-DGTA
Section 4:		
Chapter 1	Propulsion Systems	ESI-DGTA

Blank Page

SECTION 1

CHAPTER 2

DESIGN, EQUIPAGE AND CERTIFICATION ISSUES FOR CIVIL CERTIFIED ADF AIRCRAFT

INTRODUCTION

1. Sponsoring the ab-initio design and construction of a new aircraft type is an enormously complex and costly undertaking. The ADF, like most militaries, recognises the advantages of acquiring existing civilian aircraft designs that largely meet our needs, and then adapting them to fulfil particular operational requirements. Provided the ADF fully understands the role and operating environment for which the civilian aircraft was designed and certificated, and sensibly applies design standards to ADF-unique modifications, these aircraft can become effective military aircraft. However, ADF projects have previously encountered problems due to contracting to a Statement of Requirement (SOR) that inadequately reflects the civilian aerospace design and certification processes. The following clause represents a typical ADF SOR approach to defining a certification basis for the baseline aircraft and its post-production modifications:

> *The …… baseline aircraft, and all modifications to the baseline Aircraft, shall be certified by an ADF recognised National Airworthiness Authority (NAA) as complying with Federal Aviation Regulation 25 (FAR 25).*

While this clause appears to present a comprehensive certification basis for the baseline aircraft and its modifications, it is inadequate for all but the most straightforward of applications. Key shortfalls are as follows:

a. Some civil airworthiness requirements (eg FAR 23/25/27/29) contain several ‘optional’ certifications, for example certification for ditching and flight in icing conditions. An aircraft OEM will normally only pursue certifications perceived as relevant to the target market sector, so some aircraft types are not designed for these optional certifications.

b. Some aircraft equipage options are not mandated by civil airworthiness requirements, but present an improved level of safety. Examples include windshear detection systems, Traffic Alert and Collision Avoidance Systems (TCAS), Ground Proximity Warning Systems (GPWS), life rafts, supplemental oxygen, and so on. These systems may be offered as ‘options’ for production aircraft, but will not be included unless specifically nominated by the purchaser.

c. While a baseline aircraft may be designed to be eligible for certain operational certifications (for example, ETOPS), post-production modifications may impact its eligibility. The contractor may not be compelled to re-validate these features unless specifically required in the SOR.

d. Civil airworthiness standards do not encompass some military-unique functions, for example, aerial refuelling and stores carriage. Civil standards also may not assure an appropriate level of system integrity for mission systems. Unless suitable standards are incorporated in the SOR, aircraft safety and/or mission integrity may be affected in some roles and operating environments.

2. When compiling an aircraft acquisition/modification SOR, the ADF must understand the range of design, equipage and certification options available for the class of civilian aircraft being sought, and assess their impact on the proposed ADF configuration, role and operating environment. While the lack of these design, equipage and certification options may not prevent the aircraft from flying, it may substantially reduce the level of safety for some roles and operating environments. Furthermore, the ADF must assess whether the baseline aircraft design standards will present an acceptable level of safety and mission integrity for ADF-unique modifications.

3. This chapter provides guidance on specifying design, equipage and certification options for new civil aircraft. It also provides guidance on specifying standards for ADF-unique modifications.

CIVIL AIRCRAFT CERTIFICATIONS

4. The ADF relies extensively on civil aircraft certifications by the US Federal Aviation Administration (FAA), the European Aviation Safety Agency (EASA) and other recognised National Airworthiness Authorities (NAAs). These certifications provide confidence to the ADF that the aircraft type will be airworthy for a particular configuration, role and operating environment. There are two fundamental aspects to aircraft certifications provided by a civil NAA:

a. ***Certifications against Airworthiness Requirements***. The NAA is certificating that an aircraft type conforms to an acceptable certification basis, that is, a comprehensive set of airworthiness requirements and associated standards (eg Federal Aviation Regulation (FAR) Parts 23, 25, 27 or 29).

b. ***Certifications against Operating Requirements***. The NAA is certificating that the aircraft operator is able to safely operate the aircraft in the country of certification (eg FAR Pt 91, plus for certain operators Pt 121, 125 or 135).

Intuitively, the first certification appears most relevant to the ADF, since it provides the ADF with confidence that the NAA has ensured the aircraft type meets its certification basis. The second certification (the operator certification), on the other hand, would appear to be largely irrelevant; after all, the ADF is an independent Airworthiness Authority and therefore defines its own regulations for aircraft operations. Unfortunately, this assumption may be misleading, as the following assessments of the FAA's Operating Requirements will illustrate:

a. **FAR Pt 91.** This regulation prescribes rules governing the operation of aircraft within the USA. Many of these rules are primarily relevant to aircrew, for example responsibilities of pilots, flight planning, flight rules, training requirements, and so on. However, some of these rules also prescribe equipment and certification requirements for flight in certain conditions, for example, flight under instrument flight rules (IFR), flights above 12,500 feet, and extended over-water flights. In some cases the relevant Airworthiness Requirements (ie FAR 23/25/27/29) do not make provision for this equipment and certification. In other cases, while there is provision for the equipment and certification in FAR 23/25/27/29, it may not be a mandatory element of the certification program. It is therefore quite permissible for an aircraft to successfully achieve FAR Pt 23/25/27/29 certification, but be severely limited in when and where it can fly. Thus, even though FAR Pt 91 is an operational regulation, it inherently imposes equipage and certification requirements for certain operations.

b. **FAR Pt 121.** This regulation prescribes rules governing the operation of aircraft by air carriers and commercial operators, or aircraft with 20+ passengers (although there are exceptions). In many cases, the rules merely build on the Pt 91 requirements, to improve the level of safety for fare-paying passengers (for example, additional crew training requirements, minimum crew qualifications, rest periods, etc). However, as with Pt 91, Pt 121 also prescribes equipage and certification requirements, for example additional Flight Data Recorder parameters, a windshear detection system, TCAS, GPWS, and numerous other features. Furthermore, it imposes enhancements to the Pt 25 airworthiness standards to improve the overall level of safety of the aircraft, for example, additional fire detector systems, fuel system independence requirements, and so on. Thus, even though FAR Pt 121 is an operational regulation, it inherently imposes substantial addition design, equipage and certification requirements.

c. **FAR Pt 125 and 135.** Pt 125 (applicable to non-commercial carriers) and Pt 135 (air taxis) are analogous to Pt 121, in that they provide additional rules to those prescribed in Pt 91. While not as rigorous as Pt 121, both still prescribe design, equipage and certification requirements to improve the level of safety of the aircraft.

5. From the preceding sub-paragraphs, it is evident that the FAR operating requirements cover much more than aircrew rules; they can invoke 'optional' airworthiness design requirements within FARs 23/25/27/29, they can require additional equipage, and they can impose additional design and certification requirements. An ADF SOR that specifies the airworthiness requirements, but does not consider the impact of operating requirements, is likely to have serious deficiencies.

6. While the preceding section has referred only to the FARs, the equivalent EASA airworthiness and operational requirements are equally valid.

SPECIFYING DESIGN, EQUIPAGE AND CERTIFICATION REQUIREMENTS

7. Establishing a comprehensive aircraft certification basis is a fundamental TAA requirement for a contract SOR. This section provides guidance for deriving a comprehensive certification basis for the baseline civilian aircraft and all post-production modifications.

Specifying a Certification Basis for the Baseline Aircraft

8. The previous section emphasised the importance of evaluating the design, equipage and certification requirements embedded within the FAA's operating requirements. An ADF SOR for an aircraft acquisition and modification project should therefore include the following elements:

a. the relevant FAR airworthiness requirement (ie FAR Pt 23/25 for fixed wing aircraft, and FAR Pt 27/29 for rotary wing aircraft);

b. the propulsion system airworthiness requirements (FAR Pt 33 for the engine, and FAR Pt 35 for the propeller if required) and noise standard (FAR Pt 36);

c. those FAR Pt 91 elements that impact aircraft equipage and/or certification, if those issues are relevant to the ADF's proposed role and operating environment;

d. for large fixed wing aircraft, those FAR Pt 121 elements that impact design, equipage and/or certification, if those issues are relevant to the ADF's proposed role and operating environment; and

e. for smaller fixed wing aircraft and for all rotorcraft, those FAR Pt 135 elements that impact design, equipage and/or certification, if those issues are relevant to the ADF's proposed role and operating environment.

Annex A to this chapter proposes relevant ADF SOR clauses, while annex B lists the key elements in the operational FARs that require Project Office assessment.

Specifying a Certification Basis for Post-production Modifications

9. The civilian approach to post-production modifications is to ensure they meet the same standards as the baseline aircraft, so the overall level of safety of the aircraft should be retained. This approach is largely acceptable to the ADF, but there are some circumstances where the baseline aircraft standards are not sufficient, as follows:

a. Military-specific functions (for example, aerial refuelling) are not encompassed within civilian aircraft design standards, and therefore relevant military standards may need to be added to the certification basis.

b. Civilian aircraft design standards may not adequately encompass challenging military roles and/or operating environments (for example, operation in hostile electromagnetic environments), and may require supplementation.

c. Civilian aircraft design standards may not inherently ensure that aircraft mission systems achieve the higher levels of integrity demanded for military operations.

The SOR certification basis must ensure the above issues are appropriately addressed. The following three sections provide guidance for each issue, while annex A presents SOR clauses that may be used to supplement the baseline aircraft certification basis.

10. Military-specific Functions. Design requirements for military-specific functions such as the carriage of armament, aerial refuelling, NVG-compatible lighting, formation lighting and so on, may not be adequately addressed by civilian standards. If not, relevant military standards and processes from Section 2 of this manual should be included in the acquisition SOR certification basis.

11. Challenging Military Role and/or Operating Environment. Civilian aircraft design standards present an appropriate level of safety for aircraft being operated in 'normal' civilian roles. However, a proposed military role and/or operating environment may extend beyond that encompassed by the civilian design requirements, for example

operation in hostile electromagnetic environments, abrupt evasive manoeuvres, extensive low flying, and so on. If so, these issues need to be carefully examined before the Request for Tender process begins. Where there appear to be significant differences between the civilian and proposed ADF role and/or operating environment, a detailed study may need to be commissioned to fully scope the differences and establish the feasibility of adapting a civilian aircraft to the military role. Section 2 of this manual includes guidance on how civilian standards might need to be supplemented to account for the challenges of ADF roles and/or operating environments.

12. Mission System Integrity. The design standards adopted by civilian NAAs place primary emphasis on assuring the design integrity of safety-related aircraft systems. Aircraft mission systems are not generally included in the NAA's certification process (except to ensure that they do not affect safety-related systems), so mission system integrity is largely left to the system designer. While some civilian aircraft standards do define minimum integrity requirements for mission systems, the requirements are often substantially lower than for safety-related aircraft systems. This may not be acceptable for ADF aircraft, where mission systems are often fundamental to mission success, and failures in some mission systems can have safety implications in hostile environments. The application of more rigorous design standards may therefore be justified for some mission systems. Section 2 Chapter 1 of this manual presents further information on the concept of 'missionised hazards', while several other chapters in Section 2 inherently address this issue. Projects should, however, resist the temptation to simply apply rigorous military standards to mission systems on civilian aircraft; there is rarely any value in designing mission systems to a level of integrity exceeding that of the baseline aircraft's safety-critical systems.

THROUGH-LIFE SUPPORT

13. Several of the design, equipage and certification options available in FARs Pt 91, 121 and 135 may have through-life support implications that are not readily evident. For example, maintaining an ETOPS or RVSM certification can impose an additional maintenance, reporting, periodic verification and training burden. Where the ADF is establishing an SOR for a contractor through-life support contract, particular care should be taken to ensure these additional tasks are included within its scope.

Annexes:

A. Civilian Aircraft SOR Clauses

B. Technical Requirements Embedded in Operational FARs

CIVILIAN AIRCRAFT SOR CLAUSES

Underlying Certification Basis

1. The following clauses will inject the civilian airworthiness design requirements, as presented in FAR Pt 23-36, into the RFT SOR for both the baseline aircraft and the post-production modifications. While they also potentially inject the additional design, equipage and certification issues from FAR Pt 91 and Pt 121/135, this relies on the comprehensiveness of the Operational Concept Document and in addition may be open to interpretation by the Tenderer. The recommended approach is to include the following generic clauses, and then include each relevant item from FAR Pt 91 and 121/135 as individual SOR clauses, as explained below in paras 2 and 3.

> *The <project> Baseline Aircraft shall be certified by an ADF recognised National Airworthiness Authority (NAA) as complying with Federal Aviation Regulation 2x (FAR 2x) or EASA Certification Specification 2x (CS 2x), for safe operation in the ADF's intended roles, configurations and operating environments, detailed in the Operational Concept Document (OCD).* *[Essential]*
>
> *For other than the modifications and equipment specified in paragraph <next para>, all modifications to and equipment fitted to the <project> Baseline Aircraft to meet the requirements detailed in this specification shall be certified by an ADF recognised NAA as complying with current FAR2x/CS2x, as detailed in the Approved <project> Aircraft CBD*
>
> *All military specific modifications and equipment fitted to the <project> Baseline Aircraft, that can not be certified to FAR/CS as civilian standards are not applicable or for which a different certification standard is specified in this specification, shall be certified by an ADF recognised NAA to the standard detailed in the Approved <project>Aircraft CBD*
>
> *Note: Prior certification to an alternative standard by an ADF-recognised Airworthiness Authority (AA) may be accepted by the Commonwealth as providing an equivalent level of safety. The Certification Basis Description (DID-ENG-….) provides the instrument for Tenderers to present a case for acceptance*
>
> *Note: Design work that has not been accepted by an ADF-recognised AA must be presented to the Commonwealth and meet either the airworthiness requirements defined in this specification, or a basis shown by the Tenderer and agreed by the Commonwealth to provide an equivalent level of safety and performance. The Certification Basis Description (DID-ENG-….) provides the instrument for Tenderers to present a case for acceptance.*
>
> *Note: Where reference is made in this Specification to FARs, that reference shall also be deemed to invoke all applicable Technical Standard Orders (TSOs), Advisory Circulars (ACs) and other Federal Aviation Administration (FAA) documents. For Notices of Proposed Rulemaking (NPRMs), the final rule from the NPRM will be invoked as levied by the FAA, not the NPRM itself.*

Additional Design, Equipage and Certification Issues

2. Section 1 Chapter 2 of this manual examined the pitfalls in specifying only the civilian Airworthiness Requirements (ie FARs Pt 23-36) in the SOR. While the SOR clause presented above in para 1 does encompass the additional design, equipage and certification requirements that are encompassed by the FAR operating requirements (ie FARs 91 and 121/135), it still relies on the OCD being sufficiently comprehensive. A better approach may be to assess which of the design, equipage and certification requirements inherent in the operational FARs are relevant to the ADF's configuration, role and operating environment, and then including each as a line item in the SOR, for example:

> *The aircraft shall incorporate a low-altitude windshear warning and flight guidance system meeting the requirements of FAR 121.358.*

Annex B presents a comprehensive list of design, equipage and certification requirements embedded in the operational FARs.

3. Post-production modifications may invalidate certain certifications held by the baseline aircraft, for example Extended Operations of Multi-Engine Airplanes (ETOPS), or flight in icing conditions. Unless the SOR explicitly requires the contractor to fully re-validate the design, sufficient for acceptance by an ADF-recognised NAA, the resultant level of safety cannot be assured. If relevant to the ADF's role and/or operating environment, an SOR clause such as the following may be warranted:

> *The post-modification aircraft shall be verified, to the satisfaction of an ADF-recognised National Airworthiness Authority, as continuing to meet the design requirements for ETOPS per FAA AC 120-42A.*

Annex B presents a comprehensive list of optional certification requirements embedded in the operational FARs.

TECHNICAL REQUIREMENTS EMBEDDED IN OPERATIONAL FARs

1. This annex presents a summary of the design, equipage and certification requirements that are embedded within the operational FARs.

FAR Pt 91

2. FAR Pt 91 prescribes rules governing the operation of aircraft within the United States. Inherent in these operational requirements are a number of issues that impact the design of the aircraft. The issues listed in Table B-1 should be assessed for applicability to the proposed ADF role and operating environment for both fixed wing and rotary wing aircraft, and if applicable included in the acquisition SOR.

Table B-1: FAR Pt 91 Embedded Design Requirements

FAR 91 Embedded Design Requirements	Clause
Subpart C	
Instrument and Equipment Requirements (VFR/IFR required instruments)	91.205
Emergency locator transmitters	91.207
Supplemental Oxygen	91.211
ATC transponder and altitude reporting equipment and use	91.215
Altitude alerting system or device: Turbojet-powered civil aeroplanes	91.219
Subpart F – Large and Turbine Powered Multiengine Aeroplanes	
Equipment requirements: Over-the-top or night VFR operations	91.507
Survival equipment for overwater operations	91.509
Radio equipment for overwater operations	91.511
Emergency equipment	91.513
Passenger information	91.517
Shoulder harness	91.521
Subpart G – Additional equipment and operating requirements for large and transport category a/c	
Aural speed warning device	91.603
Emergency exits for aeroplanes carrying passengers for hire	91.607
Flight recorders and cockpit voice recorders	91.609
Materials for compartment interiors	91.613
Appendix A – Cat 2 ops – required intruments and equipment	App A (2)
Appendix E - Airplane Flight Recorder Specifications	App E
Appendix G – RVSM operations	App G

3. Note that FARs Pt 25 and Pt 29 do inherently include some of the issues highlighted in Table B-1, and therefore may not need to be specifically highlighted in the acquisition SOR. The document ‘Examination of Operational Federal Aviation Regulations’, available on the DGTA website, presents a cross-reference of Pt 91 and Pt 25 requirements.

FAR Pt 121

4. FAR Pt 121 prescribes rules governing the operation of aircraft by air carriers and commercial operators, or aircraft with 20+ passengers (although there are exceptions). Where large civilian fixed wing aircraft are being procured by the ADF, the issues listed in Table B-2 should be assessed for applicability to the proposed ADF role and operating environment, and if applicable included in the acquisition SOR.

Table B-2: FAR Pt 121 Embedded Design Requirements

Pt 121 Embedded Design Requirements	Clause
Flight And Navigational Equipment	121.305
Engine Instruments	121.307
Lavatory Fire Protection	121.308
Emergency Equipment	121.309
Additional Emergency Equipment	121.310
Seats, Safety Belts, And Shoulder Harnesses	121.311
Materials For Compartment Interiors	121.312
Miscellaneous Equipment (Fuses, Windsheild Wipers, Etc.)	121.313
Cargo And Baggage Compartments (Materials)	121.314
Fuel Tanks	121.316
Passenger Information Requirements, Smoking Prohibitions, And Additional Seat Belt Requirements	121.317
Public Address System	121.318
Crewmember Interphone System	121.319
Instruments And Equipment For Operations At Night	121.323
Instruments And Equipment For Operations Under IFR Or Over-The-Top	121.325
Supplemental Oxygen: Reciprocating Engine Powered Aeroplanes	121.327, 121.329, 121.331, 121.333
Protective Breathing Equipment	121.337
Emergency Equipment	121.339, 121.353
Emergency Flotation Means	121.340
Equipment For Operations In Icing Conditions	121.341
Pitot Heat Indication Systems	121.342
Flight Recorders	121.343
Digital Flight Data Recorders	121.344, 121.344a
Radio Equipment	121.345, 121.347, 121.349, 121.351
Terrain Awareness And Warning System	121.354
Equipment For Operations On Which Specialised Means Of Navigation Are Used	121.355
Collision Avoidance System	121.356
Airborne Weather Radar Equipment Requirements	121.357
Low-Altitude Windshear System Equipment Requirements	121.358
Cockpit Voice Recorders	121.359
Ground Proximity Warning – Glide Slope Deviation Alerting System	121.360

5. Note that FARs Pt 25 and Pt 29 do inherently include some of the issues highlighted in Table B-2, and therefore may not need to be specifically highlighted in the acquisition SOR. The document ‘Examination of Operational Federal Aviation Regulations’, available on the DGTA website, presents a cross-reference of Pt 121 and Pt 25 requirements.

6. Table B-3 presents the numerous special airworthiness requirements embedded within FAR Pt 121. Most of these would inherently be included in the design requirements for later revisions of FAR Pt 25 and the ‘commuter’ category in FAR Pt 23. Since most of these requirements would not be presented to customers as ‘options’, most would likely be included as standard in the baseline aircraft, provided the aircraft is currently in civilian use by Pt 121 operators. However, this should be confirmed prior to contract signature.

Table B-3: FAR Pt 121 Special Airworthiness Requirements

Special Airworthiness Requirement	FAR 121- J
Cabin Interiors	121.215
Internal Doors	121.217
Ventilation	121.219
Fire Precautions	121.221
Propeller Deicing Fluid	121.225
Pressure Cross-Feed Arrangements	121.227
Location Of Fuel Tanks	121.229
Fuel System Lines And Fittings	121.231
Fuel Lines And Fittings In Designated Fire Zones	121.233
Fuel Valves	121.235
Oil Lines And Fittings In Designated Fire Zones	121.237
Oil Valves	121.239
Oil System Drains	121.241
Engine Breather Lines	121.243
Fire Walls	121.245
Fire-Wall Construction	121.247
Cowling	121.249
Engine Accessory Section Diaphragm	121.251
Powerplant Fire Protection	121.253
Flammable Fluids	121.255
Shutoff Means	121.257
Lines And Fittings	121.259
Vent And Drain Lines	121.261
Fire-Extinguishing Systems	121.263
Fire-Extinguishing Agents	121.265
Extinguishing Agent Container Pressure Relief	121.267
Extinguishing Agent Container Compartment Temperature	121.269
Fire-Extinguishing System Materials	121.271
Fire-Detector Systems	121.273
Fire Detectors	121.275
Protection Of Other Airplane Components Against Fire	121.277
Control Of Engine Rotation	121.279
Fuel System Independence	121.281
Induction System Ice Prevention	121.283
Carriage Of Cargo In Passenger Compartments	121.285
Carriage Of Cargo In Cargo Compartments	121.287
Landing Gear: Aural Warning Device	121.289
Takeoff Warning System	121.293

FAR Pt 135

7. While FAR Pt 135 prescribes rules governing the operation of air taxis, it is considered by the FAA (and the ADF) as appropriate for smaller fixed wing aircraft and all rotorcraft. For these aircraft types Table B-4 should be assessed for applicability to the proposed ADF configuration, role and operating environment, and if applicable included in the acquisition SOR.

Table B-4: FAR Pt 135 Embedded Design Requirements

FAR Pt 135 Embedded Design Requirements	Clause
Flight and navigational equipment	135.161, 135.165
Emergency equipment	135.167, 135.178
Seats, safety belts, and shoulder harnesses	135.171
Materials for compartment interiors	135.170
Public Address System	135.150
Instruments and equipment for operations under IFR or over-the-top	135.159, 135.159
Supplemental oxygen: Reciprocating engine powered aeroplanes	135.157
Pitot heat indication systems	135.158
Flight Recorders	135.152
Radio Equipment	135.161, 135.165
Terrain Awareness and Warning System	135.154
Collision Avoidance System	135.180
Airborne Weather Radar Equipment Requirements	135.173, 135.175
Cockpit voice recorders	135.151
Ground proximity warning – glide slope deviation alerting system	135.153

Other Issues

8. The certifications and capabilities listed below are optional in the civilian airworthiness system. Further SCI-DGTA research is needed to determine just how the FAA invokes and mandates these certifications, since they are not explicitly included in the operational FARs. Pending the outcome of this research, aircraft acquisition project offices should assess whether the following issues are relevant to the required capability; if so, guidance should be sought from SCI-DGTA:

a. Extended Operations of Multi-Engine Airplanes (ETOPS);

b. Required Navigation Performance (RNP);

c. Global Air Traffic Management (GATM) requirements for Communication, Navigation, Surveillance / Air Traffic Management (CNS/ATM);

d. ditching certification; and

e. certification for flight in icing conditions.

SECTION 2

CHAPTER 1

SYSTEMS SAFETY

INTRODUCTION

The ADF Aerospace Safety Management Framework

1. The ADF's Aerospace Safety Management Framework encompasses operations conduct (both mission and maintenance), technical design and Occupational Health and Safety (OH&S). These three can be broadly described as follows:

a. **ADF Aviation Safety Program (AvSP).** The Directorate of Flying Safety (DFS-ADF), through DI (G) OPS 28-2 and the Defence Aviation Safety Manual (DASM), require the generation and sustainment of AvSPs to help maintain the Operational Airworthiness of each weapon system, in part through the mitigation of operational hazards. Within this context, some aspects of aircraft operational and deeper maintenance are also included, where the opportunity to affect Operational Airworthiness exists. At a local level, AvSPs are coordinated by Squadron or Wing Aviation Safety Officers (ASOs).

b. **System Safety Program (SSP).** Through DI (G) LOG 08-15 and DI (G) OPS 2-2 the TAR is required to maintain a procedural framework for the establishment and maintenance of a technical airworthiness management system. The framework encompasses design, maintenance and quality assurance, together with a robust systematic approach to risk management. To assist with this task, the TAR requires System Safety Programs (SSPs) to be considered throughout the Life-Of-Type (LOT) of weapon systems, from concept development to disposal. The SSP provides confidence that the weapon system is fit for service, and poses acceptable hazards to personnel, public safety, and the environment. Within this context, aspects of aircraft operational and deeper maintenance are also included, where the opportunity to affect Technical Airworthiness exists. At a local level, SSPs are coordinated by SPO or Project Office (PO) System Safety Managers (SSMs).

c. **Occupational Health and Safety Program (OH&SP).** DFS-ADF, through the Air Force Ground Safety Agency (AFGSA), the Defence Safety Management Agency (DSMA), and the Safety Manual (SAFETYMAN), requires a proactive program to allow the Commonwealth to comply with Federal OH&S and Hazardous Substances acts whilst weapon systems are in service. At the local level, OH&SPs are coordinated by SPO or PO Unit Safety Coordinators. Note that whilst there is no direct relationship between *System Safety* and OH&S, by virtue of considering and mitigating *aircraft system hazards*, the SSP will also contain some OH&S considerations. However, a SSP cannot be thought of as suitable alternative to a comprehensive OH&SP.

2. The AvSP and SSP are separate, but complimentary activities, and each needs to be aware of the existence, outputs and available resources of the other. This ensures a systematic and coordinated approach to the total airworthiness management of the weapon system and maximises the benefits of each program.

3. The remainder of this Chapter deals specifically with SSPs and their implementation, leading to Design Acceptance certification and the subsequent issue of Australian Military Type Certificates (AMTCs) and Supplemental Type Certificates (STCs).

System Safety Program

4. In its simplest sense, if '*Mishap*' can be defined to be an accident (or potential accident) with corresponding injury, illness or damage, then *Safety*, in its broadest sense, can be defined as the 'freedom from mishap'. Consequently, in an engineering context, *System Safety* can be defined as 'the application of engineering management principles, criteria and techniques to optimise the safety of a 'system', within the constraints of operational effectiveness, time and cost throughout all phases of the life cycle'. Or, in a practical sense, an engineering risk management process designed to assure that the probability of detecting *hazards* inherent in the system is maximised through its LOT.

5. In the context of Technical Airworthiness, *System Safety* is but one element of the entire certification basis and is concerned with the safety of the aircraft and its on-board systems, and of ground-based systems which interface to it either directly or indirectly (ie. known in total as the *aircraft system*). Effective *System Safety* depends on the correct application of all other certification basis elements, without duplication.

6. *System Safety* is implemented through a System Safety Program (SSP), as documented in a System Safety Program Plan (SSPP). The SSP should decompose all potential *aircraft system hazards* in the system's design, integration, operation, maintenance and disposal phases from the perspective of the three fundamental *hazard* constituent elements: hardware, software and human causal factors. This involves structuring a SSP to detail specific activities and analyses to predict and evaluate the inherent safety of each of these elements in the integrated product. In turn, this allows for the timely identification and mitigation of *hazards*, thus minimising costs and the risk inherent in the final product.

7. For practical purposes, it is also understood that any SSP must be commensurate to the *aircraft system* Configuration, Role, Environment (CRE) and mitigation costs (ie best 'bang for buck' principle). Thus no two SSPs will ever be totally alike – each will require careful consideration of realistic objectives and pragmatic tailoring. Indeed, it is the *System Safety* objectives that will decide the scope of SSP and documentation required, not the other way round.

8. *System Safety* objectives for aircraft acquisition and modification projects are different to those used for the management of in-service aircraft. During acquisition and modification projects the overarching *System Safety* objective is to procure an aircraft with an acceptable level of safety, as defined in the risk acceptance framework discussed below. Once in service, the overarching *System Safety* objective is to assure that the aircraft's inherent level of safety is maintained. The subtle differences between these two perspectives will be discussed in this Chapter.

9. This Chapter will also provide guidance on how to achieve an acceptable level of assurance for the *System Safety* aspects of the *aircraft system* only. However, recognising that POs and SPOs must deal with type design changes to the entire weapon system, the scope of the annexes attached will allow for coverage of a SSP for the entire Weapon System.

10. Throughout this Chapter, some terms or concepts significant to *System Safety* have been identified in *italics*. Definitions for these and all other abbreviations have been included at Annex A.

SYSTEM SAFETY END OBJECTIVES

11. The end objectives for a SSP in any aircraft acquisition and modification project are:

a. For the weapon system integrator to prove that through systematic analysis and reporting, their SSP has maximised the probability of identifying safety risks for the *aircraft system*, and that these have been tracked and mitigated sufficiently, in accordance with safety objectives.

b. To provide a suggested LOT SSP strategy for the *aircraft system* and enough data to support it.

12. The end objectives for an in-service SSP are:

a. To assure that the *aircraft system's* inherent level of safety is maintained through the establishment of a tailored in-service SSP, and pragmatically advocating the generation of *Safety Case Reports* for design changes or assessments.

b. To maximise use of relevant legacy or newly generated SSP data.

c. To maximise use of the extant in-service Engineering Management System (EMS).

d. To minimise impact on organisational resources.

13. After describing key concepts below, Chapter guidance on achieving the above end objectives has been separated into two parts. The first part of this Chapter outlines the TAR's *System Safety* guidance for aircraft acquisition or modification projects and the second part outlines the TAR's *System Safety* guidance for in-service weapon systems.

SYSTEM SAFETY – KEY CONCEPTS

Mission First – Safety Always

14. *System Safety* does not aim to prohibit flying operations, but simply to better disclose the technical risk inherent in an *aircraft system* such that technical and operations staff can be more informed users and make decisions aware of true risk. Throughout their LOT military aircraft will be employed in missions which will be subject to different operational pressures, hence it is accepted that ideal levels of safety may at times be compromised for the good of the mission. It is *System Safety*'s role to document the inherent risk of an aircraft system, no matter what the circumstances, and to provide recommendations for mitigating that risk to acceptable levels: 'Mission First – Safety Always'.

Tailoring of your SSP

15. Each acquisition and modification project, like each in-service organisation, will be different and therefore have different SSP objectives due to *aircraft system* configuration, role and environment, SSP strategies and anticipated LOT. While this Chapter provides guidance on establishing and maintaining the ideal SSP, it is also understood that POs and SPOs must tailor their SSPs to suit their circumstances. If guidance is not directly applicable, its intent may still be, and therefore needs to be considered. With early SCI-DGTA involvement, optimal SSP tailoring alternatives can be justified and *residual risk* acceptance levels adjusted against mitigation requirements.

System Safety Engineering and System Safety Management

16. *System Safety Engineering* (SSE) is an engineering discipline requiring specialised professional knowledge and skills in specific principles, criteria and techniques, to allow the identification and control of *hazards* to acceptable levels. It draws upon professional knowledge and skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis, to specify, predict, and evaluate the safety of the system. To apply successfully and consistently, SSE is a skill acquired only after numerous years of practising in the *System Safety* design and analysis areas.

17. *System Safety Management* (SSM) is a management discipline that defines SSP requirements and ensures planning, implementation and completion of *System Safety Engineering* activities consistent with overall SSP objectives. Intuitively, one cannot be immediately successful as a SSM without prior SSE training, essentially because one must have the foresight that only comes with substantial hands-on experience. Typically, adequately experienced SSMs have 10+ years in the *System Safety* industry and may hold the title of *Certified Safety Professionals* (CSPs) with the US System Safety Society. However, this is by no means a prerequisite and is provided for comparative purposes only. It is still up to individual organisations to determine suitability of SSM credentials, and equivalence to alternate experience is always possible.

18. While Commonwealth staff charged with managing contractor SSPs will probably never have the luxury of extensive prior SSE or SSM skills, this will be offset by the experience of the contractor's SSM. However, as a minimum, Commonwealth staff involved with SSP management or reviews should consider training as detailed at the end of this Chapter. Ultimately, the successful *System Safety Engineer* or *System Safety Manager* is one step removed from the design, can pragmatically think 'outside the square', and asks: 'Can X occur? How? Does it create a hazard? How would you mitigate it? Show me!'

Commercial and Military System Safety Methodologies – The Paradigms

19. Multiple commercial and military *System Safety* standards exist. All are largely acceptable with only minor additions. A brief synopsis of several standards is provided at Annex B to this Chapter. Typically, all *System Safety* standards fall into one of two paradigms, both equally acceptable but not easily interchangeable with the other paradigm once the SSP has already commenced:

a. Top-Down approach – These standards advocate starting from the highest aircraft-level functions, and to derive *System Safety* requirements down through each system and component level functions by virtue of possible failure effects (eg FAR/JAR 2X.1309 and corresponding Advisory Circulars). These tend to be most useful during the early stages of design, when functions may be understood but design implementation is not yet defined.

b. Bottom-Up approach – These typically advocate preliminary conceptual hazard analyses and then commencing with component piece parts or sub-systems to derive safety requirements by virtue of the effect that each piece part failure can have on each next higher assembly (eg some aspects of MIL-STD-882C).

20. The choice of a *System Safety* standard is usually only critical during initial *aircraft system* design, as the in-service management objectives to maintain the aircraft's inherent level of safety usually translates into adopting the *System Safety* design standard previously used. The most likely scenario during aircraft acquisition and modification projects is that the *aircraft system* will already have been designed to some Contractor-preferred *System Safety* standard, but additional modifications will be required for the ADF environment. Continued use of the existing Contractor-applied *System Safety* standard is preferable in this case, as long as equivalency can be shown to ADF-preferred *System Safety* standards, being: MIL-STD-882C for military SSPs and FAR/JAR 2X.1309 for commercial SSPs, as reflected by Annex C for Statement Of Work requirements, and Annexes D and E for Specification requirements.

21. There should be no requirement to impose a military SSP on a system previously designed to commercial *System Safety* standards, or vice versa. Besides not taking advantage of the Contractor's previous (probably extensive) application experience with their preferred *System Safety* standard and extant Quality Management System, it would be forcing a possibly unknown *System Safety* paradigm upon them, requiring re-training and new procedures, thus introducing new program risks and costs.

22. For the unlikely cases where the ADF is involved in the original development of a total *aircraft system*, the application of either of the following is required:

a. MIL-STD-882C or FAR/JAR 2X.1309, and their respective additional requirements shown in attached Annexes, or

b. a TAR endorsed alternative.

23. Further, even if FAR/JAR 2X.1309 is not typically associated with military-specific functions or *hazards* (eg EW Self Protection, Low Altitude Parachute Extraction System, ejection seats, etc), commercial *System Safety* methodologies can still be successfully applied.

Safety Case Report

24. The *Safety Case Report* (SCR) is a well-reasoned summary document detailing what the original SSP aims were versus what was actually achieved, and a risk analysis (with recommendations) of the differences. The weapon system integrator would typically produce this report, which is not necessarily a separate document (ie most SSPs produce *System Safety* documents which already fulfil most SCR requirements). This DGTA definition of a Safety Case or Safety Case Report may differ to other global Air Forces' definitions. For example, a UK MoD 'Safety Case' or 'Safety Case Report' communicates a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context AND it infers the COMPLETE BODY OF EVIDENCE that demonstrates that all risks have been reduced as low as reasonably practicable (ALARP). In doing this, a UK MOD 'Safety Case' may show that the system was designed and integrated correctly to approved standards, by competent people in accordance with approved procedures, with sufficient mitigation, and analysed and tested sufficiently to justify it being acceptably safe (airworthy) for flight. For DGTA, this UK MoD definition aligns almost to the entire Design Acceptance process and includes all elements of the Certification Basis Description!

25. Traditionally the SCR has been presented using conventional textual narrative. However, more recently SCRs are being presented using textual narrative augmented with a graphical argumentation notation such as Goal Structuring Notation (GSN). The graphical notations offer some advantages over solely textual means as they provide a clearer articulation of the relationship between what was actually achieved and the original SSP aims. Further information on GSN and other graphical argumentation notations can be found on the SCI System Safety Intranet site.

26. The concept of the SCR is to provide a brief synopsis of System Safety activities undertaken for Commonwealth Design Acceptance purposes. Consequently, depending on the *System Safety* paradigm used, the intent of the ADF SCR may be satisfied in multiple ways, as follows:

a. *Military System Safety Programs with a TAR-Recognised NAA*. Under this scenario and depending on the CRE argument, a SCR may only be required for design aspects where the Commonwealth is providing compliance findings (ie. for unique modifications). Further, if following a MIL-STD-882C SSP, the requirements of a SCR are almost totally satisfied by Task 402 – Annex C Appendix 8 refers.

b. *Military System Safety Programs without a TAR-Recognised NAA*. Under this scenario a SCR will be required for all design aspects. However, similar to the above, if following a MIL-STD-882C SSP, SCR requirements are almost totally satisfied by Task 402 – Annex C Appendix 8 refers.

c. *Commercial System Safety Programs with a TAR-Recognised NAA*. Under this scenario and depending on the CRE argument, a SCR may only be required for design aspects where the Commonwealth is providing compliance findings (ie. military modifications) – Annex C Appendix 8 refers.

d. *Commercial System Safety Programs without a TAR-Recognised NAA*. Under this scenario, a SCR will be required for all design aspects – Annex C Appendix 8 refers.

27. The TAR accepts that most capital aircraft programs will always have open issues against the SSP which may or may not have been raised as Issue Papers. It is important for the weapon system integrator to present these open issues in the SCR in terms of *residual risk*, and provide mitigating arguments (ie. extensive lab, ground and flight testing, similar service histories, operational limitations/restrictions, etc). In this manner, no matter what outstanding SSP issues exist, management will always be able to make a risk-based service release decision for the *aircraft system*.

Aircraft System Life-Of-Type (LOT) Considerations

28. Even if tailored within the context of a SSP commensurate to platform CRE, a SSP can be expensive to establish. Commonwealth staff must therefore consider maximising SSP return on investment over *aircraft system* LOT, by establishing an adequate self-sustaining SSP. This is especially important for acquisition or modification projects, as the scope of follow-on in-service SSPs is largely dependent on initial project SSP strategies and data produced. To a lesser extent, the same is also true of in-service modifications, whereby the scope of future SSP efforts could be affected by the foresight of in-service modification teams and any planned updates to extant *System Safety* data.

29. Some possible uses for *System Safety* data over LOT include:

a. initial and on-going confirmation of safety objective achievement and design redundancy analysis validation (eg. does the design meet the *Failure Probability Objectives* (FPOs) required by the SSP, or what were the FPOs?);

b. provision of hazard probabilities, especially for the top two hazard severities (ie *Catastrophic* and *Hazardous* for a FAR/JAR 2X.1309 program, or *Catastrophic* and *Critical* for a MIL-STD-882C program), on a ***per flight hour*** basis (eg. probability of Misleading Navigation information simultaneously generated by both Mission Computers = 4.5×10^{-5}, etc);

c. description and architecture of *System Safety* interfaces to assist and accelerate future upgrade hazard impact assessments (eg. system interfaces and hazard assessments will already exist, therefore modifications will only have to assess their delta impact in lieu of recreating entire *System Safety* data sets);

d. assist with pre or post incident and accident analysis (eg. incident or accident causation can either be revealed with existing data, or will show where existing analyses are deficient and thus highlight potential *hazards* that were not originally considered – this alone could save many hours of fault-finding);

e. sustainment of an *aircraft system* lesson-learned historical hazard database (eg. the success or failure of mitigations that had been applied under specific circumstances can be recorded for possible future re-use or avoidance); and

f. assist with engineering or operational ‘what if’ mission scenario analysis to better determine safety risks associated with specific mission circumstances (eg component x of the undercarriage system is redundant, so while correct undercarriage operation can still be expected, what is the probability of failure of the second component (and is it independent?) if the primary has failed and what is the effect on aircraft safety versus mission criticality?).

30. At all times during LOT, but especially during initial acquisition or modification projects, consideration should be given to the anticipated *aircraft system* in-service SSP strategy, and documenting this in the SSP Plan and/or Project Transition Plan accordingly. This should include its complementary data requirements (ie the *System Safety* Baseline) and efficient access to this data. This latter aspect will depend on planned in-service strategic support arrangements with the OEM or integrators through to LOT, and may only require access to electronic documentation – not outright purchase of hardcopy deliverables. Additional project guidance for in-service SSP strategy considerations is provided later in this Chapter and at Annex F.

Hazard Causal Factors

31. All *aircraft system hazards* are composed of combinations of hardware, software and human factors’ causes, inherent in either the *aircraft system* design, its integration, its operation, its maintenance or its disposal. SSP *hazards* need to be identified and analysed in terms of these three fundamental constituents across all these phases if the probability of hazard identification is to be maximised and exact root causes are to be determined and mitigated. The omission of any one of these aspects will lead to a SSP that is only considering part of the overall hazard picture, and will therefore provide a false sense of safety.

32. ***Hardware Causal Factors.*** Generally, hardware causal factors are considered appropriately in SSPs, and information for these is derived through architecture and wiring diagrams, field or predicted Mean Time Between Failure (MTBF) data, and *System Safety* analyses conducted. If predicted MTBF data is to be used in lieu of field MTBF data, Commonwealth personnel need to consider when, during LOT, figures will require validation and possible re-baselining. This is necessary because predicted MTBF data would have been used to determine initial design redundancies, verify requirements and architecture, and justify the SCR for at least Catastrophic systems. Should the observed in-service MTBF be less than the predicted MTBF, the *aircraft system* may not possess the inherent safety levels expressed in the SCR and will therefore either require re-design or acceptance of *residual risk*. Typically, validation of predicted MTBF data can only occur when the original design has stabilised and is sufficiently robust – normally 4-7 years after introduction into service. However, to cater for shorter timeframe requirements, validation with different confidence levels is also possible, and is further described within the Australian Defence Organisation’s Reliability, Availability and Maintainability (RAM) Manual. This aspect should be planned for in the transition of the SSP to the in-service organisation, as described at Annex F.

33. ***Software Causal Factors.*** Historically the analysis of software causal factors is either overlooked or considered too late in the design cycle to have any real positive influence. For an aeronautical industry that is relegating more and more system functions to software, this approach is no longer acceptable. Software must be analysed together with hardware and human factor hazard causes to provide a complete *aircraft system* safety analysis. Standards and guidance discussed at Annex B provide various options to achieve this.

34. Software Safety is defined as a mutually dependent combination of the following two elements, both integral to the success of the SSP:

a. Software Safety Assurance. This aspect spans the entire breadth of the software development life-cycle process and is discussed in greater detail at Section 2 Chapter 7 of this manual. However, given that failure probabilities cannot be assigned to software, Software Safety Assurance provides confidence, commensurate with the most severe hazard to which the software could contribute, that the software complies with its requirements and has no safety effects. This is achieved by increasing the process and product rigour applied to software development through the application of industry best practice (typically by using Software Integrity Levels (SILs)). To be effective, the Software Safety Assurance process requires a proactive Software System Safety approach to:

(1) accept flowed-down SSP requirements at all stages of the product design cycle, and

(2) generate derived software safety requirements for SSP monitoring.

b. Software System Safety. This aspect invokes the application of software safety analyses to code, to optimise *System Safety* in the design, integration, operation, maintenance and disposal of software within *safety-critical* systems. For example, one approach is to provide evidence of the absence or handling of all potential software failure modes, where software failure modes refer to the software's failure to carry out an intended or implied function. Specific software failure modes might include the omission and commission of services, timing inconsistencies (early or late execution of services), and value based failures in services. Services are defined as a communication event within the software. Techniques that specifically support this approach include the Software HAZOP (DefStan 00-58 Computer HAZOP), and Software Hazard Analysis and Resolution in Design (SHARD) – a refinement of Software HAZOP. Other software specific techniques such as software functional failure analysis, software fault tree analysis, markov analysis, petri nets, and sneak software analysis can be used to complement this approach. Furthermore, most other existing hazard analysis techniques can be adapted to consider these issues as long as software system safety is considered as part of the overall hazard analysis. The analyses generate the necessary lower-level software requirements to ensure that the software will execute with an acceptable level of safety risk within the system context. Software requirements may also be derived from general design requirements and guidelines for safety critical software described in the Software System Safety Handbook of the Joint Software System Safety Committee. An acceptable level of safety is achieved by increasing the depth and analysis rigour of safety-critical software applications, based on SIL, architecture, integration methodology and SSP techniques. This occurs through guidance provided at Annex B, typically by a Software Safety Engineer. Like *System Safety Engineers* and *System Safety Managers*, who require the experience of many years to be successful, competent Software Safety Engineers have previously gained significant experience in software development before venturing into, and gaining experience in, *System Safety*. Software Safety Engineers tend to be matrixed within Contractor or sub-Contractor software development teams, providing guidance and conducting Software System Safety analyses at all stages during the software development process, thus dynamically feeding *System Safety* requirements back into design.

35. ***Human Causal Factors.*** Traditionally, *aircraft system* human design requirements are considered adequately through the use of commercial or military guidance documents, supplemented by Commonwealth human design and subject matter experts at DSTO, ARDU, AMAFTU, AVMED and operational squadrons. Similar to the software causal factor analysis argument above, a hazard's human causes can be analysed together with hardware and software causes. However, the pitfall is that human causes to *hazards* are typically analysed and mitigated on a per-hazard basis – and mitigations themselves usually also require human input (ie. aircrew work-arounds, procedures, or training). Seldom during a worst credible *aircraft system* hazard scenario would just one hazard be applicable, typically being a combination of *hazards*. Therefore all designs need to consider performing a *Human Factors Workload Assessment* on the integrated system, to ensure that the average-skill crew member, under a worst credible hazard scenario, can still effectively continue to safely fly and land the *aircraft system*.

36. If a *Human Factors Workload Assessment* is not required due to the low level of inherent risk, then this needs to be justified in the *aircraft system* SCR, however SCI-DGTA advice should be sought early, to ensure that the methodology and justification is adequate. Further advice on human factors in *aircraft system* design and system integration activities is contained in Section 2 Chapter 13 of this manual.

System Safety Document Baseline

37. The System Safety Document Baseline (SSDB) consists of the minimum set of safety-related documents that at any given time during the LOT of the *aircraft system*, is able to accurately disclose the *System Safety* analysis of the final design (and therefore direct and derived *System Safety* design requirements), and the closure status of all *hazards*. This document set is typically identified in the Project's Transition Plan and is detailed in the SCR. The set could include the SSPP, Hazard Log/Database, aircraft-level and system-level Functional Hazard Analyses, aircraft-level and system-level Safety Analyses, System and Sub-System Hazard Analyses, Operating and Support Hazard Analyses, individual ECP and Deviation/Waiver Safety Assessments and SCR, depending on the safety paradigm used.

38. The intent of the SSDB is to provide the most concise record of original and current *System Safety* requirements, hazard identification and analysis, and hazard closure status. This provides the traceability, analysis processes and assumptions, and hazard status of the *aircraft system*, at any point in its LOT, and is the in-service SSP starting point upon project transition. However, the set of documents will largely depend on the tailored SSP strategy applied during acquisition or modification, and the LOT in-service support *System Safety* strategy chosen, and therefore could be as simple as only the SSPP and Hazard Log/Database.

Commonwealth-level System Safety Program Plan

39. Some acquisition and modification projects' or in-service organisations' *System Safety* engineering efforts may be managed through multiple Contractors, Foreign Military Sales, or specialty organisations. Indeed, the PO themselves may be the integrators of the equipment they are attempting to certify. For these cases, as well as individual Contractor organisations generating their own subordinate SSPP, the TAR strongly recommends for the PO to generate an overarching Commonwealth-level SSPP. This overarching plan could then effectively coordinate the *System Safety* efforts of all the disparate entities towards overall SSP aims. This has historically proved invaluable in retaining a SSP focus across multiple SSP participants, and posting cycles, and POs are therefore encouraged to develop their own. An outline of an overarching Commonwealth-level SSPP is provided at Annex G.

40. The generation of a Commonwealth-level SSPP should also be considered for design changes where integration aspects are complex, or there are unusual Contractor or equipment suite circumstances. Alternately, this detail could be included within another existing document. Irrespective of the decision to generate an overarching Commonwealth-level SSPP, for design changes where integration, Contractor or equipment complexities exist, information that would be provided in the plan may eventually be required anyway, as part of the SCR, to support the overall Design Acceptance effort.

Consideration of 'Missionised' Hazards

41. While the TAR seeks an equivalent level of safety to that adopted for civil aircraft, the TAR also understands that with very few exceptions, all a*ircraft systems* to be used by the ADF have military-specific roles, including specialised wartime functions. This is the nature of ADF business and therefore design requirements are levied to achieve these operational imperatives.

42. Consequently, for the CRE, the TAR recommends that the SSP needs to not only consider *hazards* in benign operating environments, but also *aircraft system hazards* with airworthiness implications that could exist in worst credible missionised scenarios, reflecting the Statement of Operating Intent (SOI). However, as most analyses of this type can only be qualitative, the System Safety Working Groups (SSWGs), with operational input from the OAAR, will need to provide basic mission assumptions to facilitate practical and realistic solutions.

43. The TAR recognises that the application of System Safety to *hazards* that may only exist during wartime (or war-gaming) is a novel and therefore unfamiliar concept to most Contractors, hence the following additional considerations may assist:

a. The number and scope of missionised *hazards*, leading to a cost-benefit analysis.

b. The availability and content of a Technical Review and Audit Program, leading to the consideration of these *hazards* through other means.

c. The existence and scope of an operational effectiveness and suitability test phase, leading to the consideration of these *hazards* through other means.

44. Early DGTA advice is recommended when establishing the SSP to consider these *hazards*, and when in doubt about their practical resolution.

SYSTEM SAFETY PROGRAM REQUIREMENTS FOR AIRCRAFT ACQUISITION OR MODIFICATION PROJECTS

45. A SSP needs to be considered for all major *Type Design Changes*. This requirement should be captured in the project Certification Basis Description (CBD), and compliance must be shown as part of the Design Acceptance process (and to subsequently receive a TAR recommendation for an AMTC or STC).

46. For minor *Type Design Change* modification projects, SSP requirements are typically subject to the pragmatic tailoring by the Design Acceptance Representative (DAR), commensurate with risk. However, even if SSP rigour is not anticipated to be as extensive as for major *Type Design Changes*, SSP considerations are the same. Consequently, minor *Type Design Changes* will not be separately discussed again within this Chapter.

47. The following paragraphs outline the TAR's *System Safety* requirements with respect to the design change process for all *Type Design Changes*: establishing the CBD, conducting the SSP, and Compliance Finding. Alternative approaches may be used, however these should be discussed with DGTA in the first instance.

ESTABLISHING SYSTEM SAFETY CBD ENTRIES

48. Typically projects will rely upon a component of the existing *System Safety* Program from a previously certified aircraft baseline, and require additional *System Safety* activities for changes resulting from the ADF CRE. Sample CBD entries are provided at Annex H.

CONDUCTING THE SSP

SSP Scope

49. The scope of the SSP comprises the identification and mitigation of *aircraft system hazards* that impact airworthiness, including consideration of missionised *hazards*, to acceptable levels. This includes *hazards* directly and indirectly associated with the *aircraft systems* and their reliability, degraded states, failure modes, and complex interactions, caused by hardware, software or human factors in *aircraft system* design, integration, operation, maintenance and disposal. Many *hazards* and their causes will be self-evident, however less obvious examples include:

a. *hazards* associated with interfaces between ground equipment and the aircraft (ie flight maintenance data or mission planning loading systems which could lead to loss or corruption of flight safety related data or functions);

b. *hazards* caused by aircraft stores' integration (either due to the influence of the store on the aircraft system, or vice versa – note that Section 2 Chapter 12 of this manual specifies *System Safety* requirements for Weapon Certification and Stores Clearance, typically the domain of ASCENG, and further discussed below in 'SSP Additional Considerations'); and

c. chemical, biological or radiological *hazards* to aircrew, passengers and maintainers (eg due to long term exposure to radiation or toxic material presence).

SSP Objectives

50. While the objective of any SSP must be to aim for zero *mishaps* through LOT, probabilistic theory ensures that this is theoretically unachievable. However, to discharge the Commonwealth's responsibility to both its personnel and the community at large, and to approach *aircraft system* design professionally, Commonwealth personnel should strive for zero *mishaps* within the bounds of a SSP commensurate with *aircraft system* CRE and costs. This is established by demonstrating that:

a. the *aircraft system* design does not include unacceptable *catastrophic* system or sub-system failure mechanisms,

b. *aircraft system* related *hazards* are mitigated to an acceptable level of risk (as outlined in discussions below, and conceptually referred to as 'As Low As Reasonably Practical (ALARP)'), and

c. the intended LOT *System Safety* strategy is being satisfied by the transition of sufficient *System Safety* data to the in-service organisation.

SSP Overview

51. A comprehensive schedule of SSP deliverables is included at Annex C. At the outset the Contractor should develop a SSPP which outlines the SSP's scope and objectives, and the planned manner in which they will be achieved. All activities that the Contractor intends to undertake as part of the SSP should be described, and the timing of these activities outlined against the project's schedule. This includes defining the Contractor's planned approach to the identification, analysis, tracking, treatment, verification and acceptance of *hazards*. Additional guidance is provided at Annex C Appendix 1.

52. At an early stage in the project (typically no later than System Definition Review (SDR), or equivalent) the Contractor should assign criticalities to:

a. all *aircraft systems* for an acquisition project, or

b. all new and modified *aircraft systems* for a modification/upgrade project.

53. The assignment of *aircraft system* criticalities will influence documentation requirements and the depth of analysis within that documentation. Criticalities will also allow tailoring of the level of oversight required by the Commonwealth.

54. At the completion of the SSP, unless a NAA provides the equivalent of a Type Certificate to match the ADF CRE, the Contractor should submit a SCR in accordance with Annex C, to:

a. assess and document the SSP's achievements with respect to its safety objectives (ie verification), and

b. justify the level of technical risk inherent in the *aircraft system* (ie validation).

SSP Additional Considerations

55. ***Integration of Aircraft Stores***. Section 2 Chapter 12 of this manual deals specifically with generating and verifying safety requirements for Stores' Certification per se, and its Stores Clearance. This is ASCENG's domain of *System Safety* and therefore will not be discussed further here. However, integration *hazards* due to the influence of the Store on the *aircraft system*, and vice versa, can be considered by either ASCENG or the acquisition and modification project, as mutually agreed. Responsibility for this facet of *System Safety* is purposely not discussed in detail as it is dependent on the level of *aircraft system* integration and developmental maturity of the Store.

56. For acquisitions and modifications involving Stores, agreement on where the *System Safety* responsibility boundaries lie between ASCENG and the PO need to be documented early (either in the Commonwealth-level or Contractor SSPP) to ensure all aspects of integration *hazards* are considered.

57. ***Explosive Ordnance Integration.*** Similar to the Stores' integration philosophy above, the integration of explosives onto an *aircraft system* may require involvement from ASCENG and/or JALO and the Ordnance Safety Group (OSG). Again, for acquisitions and modifications involving explosives, agreement on where the *System Safety* responsibility boundaries between ASCENG, JALO, the OSG and the PO lie need to be documented early (either in the Commonwealth-level or Contractor SSPP) to ensure all aspects of integration *hazards* are considered.

58. ***Chemical, Biological or Radiological Toxicity.*** Hazards involving the introduction of components with these properties, even if temporarily, are generally governed by OH&S and national legislation and statutes, and their inclusion into the SSP would simply reflect these governance requirements. However, generally the Contractor would also be required to submit justification as to why alternative, benign components that achieve the same objectives could not be used in lieu. These items tend to be considered on a case-by-case basis through the relevant federal regulatory body.

59. ***Integration of Propulsion System Reliability.*** Successful integration of the propulsion system into the SSP requires an understanding of its reliability under the ADF CRE. A thorough understanding of propulsion system reliability becomes critical for single engine aircraft and when pursuing extended range operations. Propulsion systems are usually designed to meet a number of performance, durability and structural integrity requirements. Propulsion system reliability will be influenced by the reliability of a number of sub-systems and components such as fuel, lubrication, pneumatic, electronic, anti-icing, cooling, instrumentation, speed reduction, fire protection and in some cases, thrust reversers. The engine OEM will normally perform a safety analysis to support the engine design objectives, such that there would not be any likely single failures that would result in fire, an un-contained event, exceedence of engine ultimate loads, or prevent the engine from being shut down. The engine OEM should therefore be able to provide an In-Flight Shut Down (IFSD) rate for the propulsion system. This can then be incorporated into the overall aircraft *System Safety* assessment process.

60. Propulsion system reliability will be based on a number of design assumptions and hence, the ADF CRE should be evaluated to confirm that it does not invalidate IFSD rates. IFSD rates will also be based on a prescribed maintenance program, which may require scheduled maintenance activities to mitigate hazards, or unscheduled 'on-

condition' maintenance activities. The latter requires an effective condition monitoring program to ensure that in-service operations are not causing engine deterioration at a rate faster than that assumed during design. Refer to Section 4 Chapter 1 of this manual for more guidance on propulsion system design requirements.

61. ***Integration of Airframe and Engine Fatigue Life Management.*** Due to the nature of cyclical loading on airframe structure and rotating parts in gas turbine engines, they are prone to fatigue. Mismanagement of fatigue in service may lead to the development of catastrophic events, which can occur without prior warning. Whilst *System Safety* standards such as FAR/JAR 2X.1309 encourage redundant designs to achieve the *fail-safe* design concept, this becomes impractical for some critical structures and all critical engine rotating parts. However, a *fail-safe* design can still be effectively achieved by in lieu applying factors of safety during design, applying life limits in service, and by ensuring responsible management of accumulated fatigue. Whatever the approach, it subsequently needs to be validated by in service usage and condition monitoring, as described in its ASI Management Plan (ASIMP) and ESI Management Plan (ESIMP). Effectively, the requirement for these two documents is an adjunct to the *Aircraft System* SSPP, to ensure that fatigue on critical airframe and engine parts is managed responsibly to LOT. For further details refer to Section 2 Chapter 11 for ASI management and Section 4 Chapter 1 for ESI management.

62. ***Engineering Change Proposals (ECPs).*** Inevitably, all projects require the inclusion of ECPs in their *aircraft system* during its life cycle, either due to unforeseen circumstances or to ensure all original requirements are indeed captured. The later in the life cycle they are introduced, the more the *System Safety* effort could be disrupted.

63. To update *System Safety* documents with ECP effects, two options exist. Either the update of *System Safety* documents is negotiated into the ECP price, or at their next revision, ECP changes are introduced retrospectively. For this latter option, a stand-alone ECP *System Safety* Report (ECPSSR), generated by the integrator, may be used to provide the adequate safety assurance required of the design change, in anticipation of updated safety documents. Obviously the more complex and risky the ECP, the more the ECPSSR is unsuitable in providing such assurance. Early SCI-DGTA advice is therefore recommended on ECPs where organisations propose using ECPSSRs as the initial method of documenting safety compliance.

64. ***Test and Evaluation (T&E) Safety***. While the SSP will consider *aircraft system* hazards in design, integration, operation, maintenance and disposal from the perspective of hardware, software and human causal factors, T&E phases provide their own unique safety challenges. Depending on the scope of new development, many test procedures could be required to validate operating envelopes as well as functionality, and albeit that highly qualified aircrew are usually given this task, the physical lack of training and experience with the new aircraft type creates hazards that need to be accepted by management. Similarly, to support the test procedures, operations and maintenance may need to be exercised with sequences and techniques that are not anticipated under normal conditions. All carry hazards that need to be accepted by management.

65. To account for the nominally higher levels of risk expected during T&E phases, a Test and Evaluation Risk Matrix (TERM) may be specifically developed. The TERM mirrors the format of the Hazard Risk Index (HRI) matrix, but the qualitative risk acceptance levels are adjusted to suit the higher risk expected. Test procedures are analysed from the training, experience, operational and maintenance risks perspective and mitigated and accepted according to the TERM. Responsibility for the conduct and coverage of the T&E hazard assessment is usually required to be negotiated with the responsible Commonwealth test organisation, and decisions recorded in the Commonwealth-level SSPP. If a T&E Hazard Analysis Report is required by the PO or contractor, additional guidance is provided at Annex C.

Failure Probability Objectives

66. Safety of an *aircraft system* is described in terms of risk. Risk is typically expressed in terms of *hazard* probability and *hazard* severity categories. In turn, *Hazard* probabilities are expressed in either qualitative or quantitative terms (eg. as shown in Tables 1–1 and 1–2 for FAR/JAR 25/29 aircraft). The minimum quantitative probability values allowed are known as Failure Probability Objectives (FPOs). Typically, any project with *hazard* severities in the top two severity classes require FPOs to verify sufficient mitigation. A MIL-STD-882C SSP approach would require similar definition tables and FPOs, but the severity and probability categories will be differently named.

Table 1–1 Hazard Severity Definitions for FAR 25/29 Aircraft

Severity			
Catastrophic	**Hazardous**	**Major**	**Minor**
Failure conditions that would result in fatality/ies, usually with loss of the airplane.	Failure conditions that would reduce the capability of the airplane or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be, for example: • a large reduction in safety margins or functional capabilities; or • physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or • serious or fatal injuries to a relatively small number of persons other than the flight crew.	Failure conditions that would reduce the capability of the airplane or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be, for example: • a significant reduction in safety margins or functional capabilities; • a significant increase in flight crew workload or in conditions impairing flight crew efficiency; • discomfort to the flight crew; or • physical distress to passengers or cabin crew, possibly including injuries.	Failure conditions that would not significantly reduce airplane safety, and involve flightcrew actions that are well within their capabilities. Minor failure conditions may include, for example: • a slight reduction in safety margins or functional capabilities; • a slight increase in flight crew workload, such as routine flight plan changes; or • some physical discomfort to passengers or cabin crew.

Table 1–2 Hazard Probability Definitions for FAR 25/29 Aircraft

Probability *per Flight Hour*			
Extremely Improbable	**Extremely Remote**	**Remote**	**Infrequent**
Quantitative: $P<10^{-9}$ **Qualitative:** So unlikely that it is not anticipated to occur during the entire operational life of all airplanes of the type.	**Quantitative**: $10^{-9}<P<10^{-7}$ **Qualitative**: Not anticipated to occur to each airplane during its total life, but which may occur a few times when considering the total operational life of all airplanes of the type.	**Quantitative**: $10^{-7}<P<10^{-5}$ **Qualitative**: Not anticipated to occur to each airplane during its total life, but which may occur numerous times when considering the total operational life of all airplanes of the type.	**Quantitative**: $10^{-5}<P<10^{-3}$ **Qualitative**: Not anticipated to occur to each airplane every year, but which may occur one or more times during the entire operational life of each airplane.

67. ADF aircraft with roles similar to civil industry aim for design safety probabilities equivalent to civil requirements. However, ADF aircraft with military roles generally operate in harsher environments, tend to utilise less mature technology and include more highly optimised designs, therefore the ADF **may** accept lower safety objectives in order to achieve mission aims. Therefore, upon presentation of suitable arguments, the TAR will consider less onerous FPOs for ADF *aircraft systems*. Further, OEM advice can be sought on FPOs required, and indeed this advice could provide part of the PO argument in recommending *aircraft system* FPOs.

68. Typical system FPO ranges are outlined in Table 1–3. The basis of these FPOs is in the statistical history of commercial large transport airline accidents, calculated to be less than one Catastrophic aircraft accident due to a ‘system failure’ (ie hardware-related only) for every 10^7 operating hours. Assuming a combined total of 100 Catastrophic system-level failure conditions for the *aircraft system*, again based on historical commercial *hazard* number averages, each one of these system Catastrophic failures should occur no more than once every 10^9 operating

hours. That is, the probability of any catastrophic hardware-related 'system level' hazard must be less than 10^{-9} ***per flight hour*** for all FAR/JAR 25/29 aircraft. A similar argument applies to FAR/JAR 23/27 commuter category aircraft, albeit probability requirements are less onerous.

Table 1–3 Relative System-Level FPOs

	System FPOs (*per flight hour*)	
Probability Level	**FAR 25/29 Civil Certified Aircraft Systems**	**Military Aircraft Systems Historically (Combat/Transport/Training/Utility)**
Infrequent	10^{-3}	10^{-3} - 10^{-2}
Remote	10^{-5}	10^{-5} - 10^{-3}
Extremely Remote	10^{-7}	10^{-7} - 10^{-4}
Extremely Improbable	10^{-9}	10^{-9} - 10^{-5}

69. For *hazards* related to loss of a function, the reliability expected above can usually only be achieved through redundancy. For *hazards* related to incorrect or misleading provision of a function, reliability and integrity must usually be sought through independent monitoring or comparison of redundant units. For *hazards* related to the provision of a function when not desired, interlocks or other appropriate *fail-safe* mechanisms are normally used.

70. As an example, consider 'Total Loss of All Hydraulic Power', as shown below in Figure 1, as a Catastrophic failure condition. For a FAR/JAR 25 commercial aircraft the probability of total loss of hydraulic power must be less than 10^{-9} *per flight hour*. Assume that the hydraulic system consists of 3 identical independent sub-systems, each with 5 independent failure modes which can cause loss of hydraulic power to that sub-system (eg valve failure, drive belt failure, shaft failure, etc). Assume also that the probability of failure for each failure mode can be estimated as 2×10^{-4} per hour. This would give a combined probability of failure for each sub-system of 10^{-3} per hour. Therefore the probability of loss of hydraulic power (ie failure of all sub-systems) would equate to 10^{-9} per hour, which is acceptable from an initial design solution perspective. Additional analysis would then also be required to establish that there are no Common Cause failures that would invalidate this argument (eg maybe the 3 sub-systems all have components in close proximity to one engine, thus an uncontained engine failure could sever all three systems' lines simultaneously).

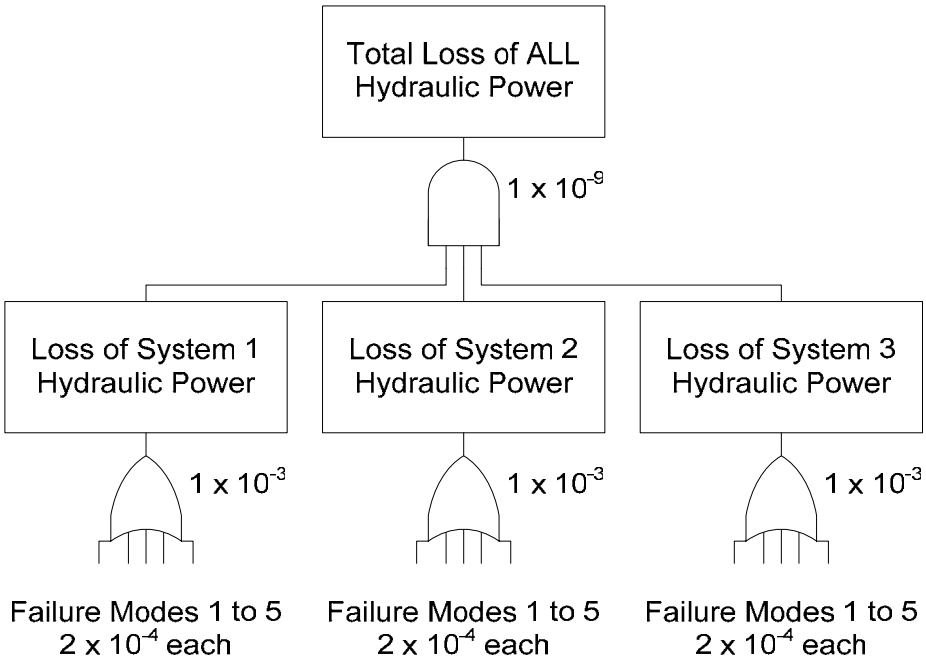


Figure 1–1 Hydraulic Power Fault Tree

71. The FPO ranges in Table 1–3 are provided to show potential relative risk and historical averages, however this is not to be used as sole justification for FPO choice. FPOs for ADF aircraft projects should be established in consultation with the integrator and the TAR, and should commensurately reflect the *aircraft system's* CRE. There is an argument for "at risk" intervals to be considered when performing calculations to meet FPOs, however, this

typically makes the safety case more difficult to justify. Issues arise about how we can guarantee that an activity is limited to the “at risk” time. The TAR preference is that no credit should be taken for limited exposure intervals. For example, where the Statement of Operating Intent identifies a low level military flying profile, calculations should be performed assuming low level flight for 100% of the flight time. Similar assumptions should be made for formation flights, overwater operations etc. Where an OEM proposes using “at risk” time to meet agreed FPOs advice should be sought from DGTA-SCI.

72. Unlike hardware, software and human-factors-related *hazard* probabilities cannot typically be quantified and therefore a qualitative methodology must be applied to minimise these types of *hazards*. This is discussed in other parts of this Chapter.

Hazard Analysis Guidance

73. The TAR does not mandate specific hazard analysis techniques for aircraft SSPs as each has its merits for specific applications, and is therefore dependent on circumstances. The following paragraphs provide guidance on what should be considered by the weapon system integrators for all analysis techniques, but is not exclusive. With CRE defined, hazard analyses should consider *hazards* associated with:

a. the baseline *aircraft system*, and

b. departures from that certified baseline.

74. When considering departures from the certified baseline, hazard analyses should address *hazards* associated with:

a. legacy aircraft systems;

b. new and modified *aircraft systems*’ design, integration, maintenance, operation and disposal;

c. the interface between new and legacy *aircraft systems*; and

d. complex system interactions, including *Common Cause*, *Zonal* and *Particular Risk* Analyses.

75. When considering *hazards* associated with new and modified *aircraft systems*’ design, integration, maintenance, operation and disposal, the hazard analysis should, as a minimum, address their:

a. failure modes and degraded states,

b. potential impact upon safety related systems,

c. contained energy sources,

d. physical location, and

e. susceptibility to events such as:

(1) fire,

(2) humidity/moisture/water/seaspray/hail/ice/snow/temperature changes,

(3) lightning,

(4) dust,

(5) bird strike,

(6) tyre/wheel disintegration,

(7) leaking fluids,

(8) depressurization,

(9) crash landing/impact/shock/vibration,

(10) high intensity radiated fields, and

(11) release of high energy devices.

Hazard Mitigation

76. Identified *hazards* should be reduced to an acceptable level of risk, in accordance with the project's tailored *Hazard Risk Index* (HRI) matrix. *Hazard* mitigation is typically conducted in the following order of precedence due to the inherent effect of each:

a. design *hazard* out to reduce risk or eliminate it (ie through re-design make the *hazard* scenario irrelevant),

b. incorporate safety devices to reduce the *hazard* risk to an acceptable level (eg automatic override on Terrain Following Radar),

c. provide warning devices to reduce *hazard* risk to an acceptable level (eg Ground Proximity Warning System audio and visual indications), and

d. develop procedures and training to attempt to avoid the *hazard* (eg safe distances when operating radar on the ground, or use of personal protective equipment).

77. Typically, the incorporation of mitigations do not alter *hazard* severity, only probability (ie a *Catastrophic hazard* will still be Catastrophic after mitigation, just that its probability of occurrence may be reduced), however there are exceptions (eg 'burst' disks in pressure systems). Also, procedures and training are not typically used as the sole mitigation method for *Catastrophic hazards*.

Hazard Tracking

78. *Hazards* need to be tracked throughout the *aircraft system's* LOT. This should be accomplished by maintaining a Hazard Log, or database of all *hazards*. All *hazards* identified during any SSP analysis, whether during initial design or during in-service management should be added to the Hazard Log, making it a historical document for closed *hazards*, and a status document for *hazards* in-work. Consequently, the Log's configuration needs to be carefully updated to match its corresponding SSP analyses updates. At a minimum, the Hazard Log should include the following fields:

a. an unique identifying reference number;

b. a short title that captures the nature of the *hazard* (the 'when' and 'where' it is a *hazard*);

c. a detailed description of the *hazard*;

d. a description of any necessary mitigation, and whether short or long-term fixes;

e. assignment of responsibility for treating the *hazard*;

f. probability, severity and accompanying HRI before mitigation;

g. probability, severity and accompanying HRI after short or long-term mitigations have been incorporated;

h. evidence that necessary mitigation has been implemented (eg test report, inspection, etc);

i. confirmation that the *residual risk* has been accepted at the appropriate level, in accordance with HRI criteria (eg correspondence reference); and

j. status of the *hazard* (open, closed or in-work with an expected close-out date).

Hazard Closure

79. The following activities are requisites for *hazard* closure:

a. The Contractor and/or Commonwealth have confirmed that all necessary mitigations have been implemented, and that the HRI was correctly assigned pre and post mitigation. Post mitigation HRIs should be demonstrated by test, analysis, demonstration, simulation, past experience or expert opinion.

b. The *hazard's residual risk* has been accepted, in writing, in accordance with agreed HRI sign-off levels.

Residual Risk and Risk Acceptance

80. The 'go/no-go' risk acceptance methodology used by FAR/JAR 2X.1309 aircraft, as outlined in Table 1-4 below is unlikely to be appropriate for military aircraft. In lieu, the TAR accepts a flexible approach whereby *hazards* that would be unacceptable in the civil environment may be accepted on behalf of the Commonwealth by persons with appropriate engineering or operational authority. Notwithstanding this, reasonable effort should still be made to reduce the risk of a given hazard as low as reasonably practicable. An example of this approach is outlined in Tables 1-5, however projects **must** generate and be able to justify their own HRI table, and this table could equally apply to MIL SSP.

81. HRI matrices for ADF aircraft acquisition and modification projects must be established in consultation with the TAR. Further, these tables can be referred to as either Hazard Risk Index (HRI) matrices, or Risk Hazard Index (RHI) matrices, simply dependent on the parent safety standard used. For consistency this Chapter will continue to refer to them as HRI matrices, understanding that the alternate could also apply.

Table 1-4 Hazard Risk Index/Acceptance Matrix for Commercial FAR/JAR 2X.1309 Aircraft

	Severity			
Probability	**Catastrophic**	**Hazardous**	**Major**	**Minor**
Infrequent	1	2	4	7
Remote	3	5	8	11
Extremely Remote	6	9	12	14
Extremely Improbable	10	13	15	16

1-6	Unacceptable
7-16	Acceptable

Table 1-5 Example Hazard Risk Index/Acceptance Matrix for ADF FAR/JAR 2X.1309 Aircraft

	Severity			
Probability	**Catastrophic**	**Hazardous**	**Major**	**Minor**
Infrequent	1	2	4	7
Remote	3	5	8	11
Extremely Remote	6	9	12	14
Extremely Improbable	10	13	15	16

1-3	Unacceptable
4-6	Requires mitigation, unless acceptance given by the DAR and OAAR
7-10	Acceptable, with approval from the designated Commonwealth authority
11-16	Acceptable with approval from the designated Contractor authority

82. All mitigation strategies should consider the periodic review of hazards to ensure the risk likelihood does not increase and/or the CRE context has not changed.

Integration of Sub-Contractors

83. The TAR expects the Contractor's SSP, and SSPP, to integrate sub-contractors, such that:

a. the prime Contractor's requirements for the SSP are communicated to the sub-contractors, and audited for compliance during the SSP; and

b. results from sub-contractor's *System Safety* activities are incorporated back into the overall prime Contractor's *aircraft system* SSP (eg sub-contractor safety analysis results are rolled into the prime Contractor's analyses).

Interface with Software Safety Program

84. Historically, software's contribution to *hazards* (ie. software causal factors) tend to be either overlooked or considered too late in the development cycle to have any positive influence on design. This usually results in a product where the software's potential contribution to hazards, and its effective mitigation, is poorly understood. A *Software Safety Program* (SwSP) is required to coordinate hazard identification and mitigation efforts for hazards with software-related causal factors. By definition, the SwSP is a subset and integral part of the SSP, and is a systematic approach to reducing software risks within the system. All SSP analyses and reports must integrate software hazard considerations and activities as part of their conclusions, including the SCR.

85. As described earlier, the SwSP can be thought of as a combination of the following two aspects:

a. software development assurance requirements (ie build the product right), known as Software Safety Assurance (for more guidance see Section 2 Chapter 7 of this manual); and

b. software safety requirements determination (ie build the right product), known as Software System Safety (SSS), and where results of the SSS analyses are fed back to the SSP to ensure that the Hazard Log correctly tracks software related *hazards* and causal factors.

86. Both of these aspects are required for a successful SwSP, and indeed, both depend on one another and cannot survive in isolation without elevated risk. Their application therefore needs to be integral to the SSP, as described within the SSPP, and use the same definitions for key terms. Further, cross-referencing to the Software Development Plan may also be required if this latter plan is used to document aspects of the SwSP.

87. Guidance that can be applied in the establishment and maintenance of SwSPs and SSS includes IEEE 1228 'Standard for Software Safety Plans', whose intent should be included within the SSPP, and the Software System Safety Handbook of the Joint Software System Safety Committee for analysis conduct. A short synopsis of each is provided at Annex B.

Interface with Human Engineering Program

88. In the context of the SSP, human *System Safety* requirements are determined through analysis of the contribution of human factors to *hazards*. Similar to the SwSP discussed above, all SSP analyses and reports must integrate human factor considerations as part of their conclusions, including within the SCR.

89. The Human Engineering Program (HEP) consists of a combination of design human *System Safety* requirements determination, and system integration human workload validation. A brief description of both is provided below, but additional guidance is provided at Section 2 Chapter 13 of this manual.

90. ***Human Factors' System Safety Design Considerations***. Consideration of human factors' influence on *System Safety* at the design stage is generally constrained to:

a. the application of a recognised human engineering and anthropometric design standards,

b. Subject Matter Expert (SME) and human factors' specialists involvement in design considerations, and

c. determining and mitigating the contribution of humans in *hazards*.

91. To successfully achieve this, a compromised balance between the SOI, the technology used and human capacities must be struck. Typically this subjective balance is achieved by agreement of SMEs, human factors' specialists and PO staff, through interfaces with the System Safety Working Group.

92. ***Human Factors' System Integration Validation***. As described earlier, it is necessary to consider a *Human Factor Workload Assessment* during system integration, to ensure that an average-skill aircrew member, under all the worst credible representative hazard scenarios (eg. lightning strike during single Mission Computer back-up mode of operation) can still continue to safely fly and land the aircraft. For further advice, refer to Section 2 Chapter 13 of this manual.

93. Should a *Human Factor Workload Assessment* not be required due to perceived low inherent risk, the SCR is to provide justification. However, early SCI-DGTA involvement in this decision is strongly recommended.

Interface with the RAM Program

94. The RAM Program is a multi-discipline program that has close links with System Engineering, Integrated Logistics Support (ILS) and the SSP, and concentrates on the provision of the following information throughout the equipment's life cycle:

a. Defining RAM requirements (eg. Mission Reliability, Fleet Availability, Mean Time to Repair (MTTR), etc) including for RAM testing/demonstration.

b. Review of RAM prediction models (eg. Mean Time Between Failure (MTBF) models).

c. Evaluation of RAM test data.

d. Evaluation of field data from a Failure Reporting, Analysis and Corrective Action System (FRACAS) such as CAMM2.

95. The main interface between the RAM Program and the SSP is with the provision of potential failure modes and corresponding MTBFs from the Failure Mode and Effects Analyses (FMEA). Whilst typically the RAM Program provides this data to the SSP, there will be instances where the SSP will identify new failure modes or altered MTBFs to be reflected back into the various RAM products. Close liaison with the RAM Program is therefore suggested to maximise the benefits of this relationship. Additional information on RAM processes or products can be found in the ADO RAM Manual.

System Safety Working Group

96. The PO should ensure that a System Safety Working Group (SSWG) is established as soon as practical after contract signature. The SSWG will comprise of active working-level members of project, operator and Contractor teams, that are either SSMs, SMEs or engineers and specialists in specific technical or operational disciplines.

97. The primary aim of the SSWG is to facilitate communication between the program executives, *aircraft system* design teams, safety organisations, and the Commonwealth, and to allow for the agreed mitigation of safety *hazards* as early as possible in the design phase. For maximum effectiveness, SSWGs need to include representatives from the users, *System Safety Engineering*, Contractor, design engineering, maintenance engineering and, if required, OH&S. Further, these individuals need to be empowered by their parent organisations to either make decisions on the organisation's behalf, or to be able to get priority endorsement/veto of SSWG recommendations. The necessity and aims of the SSWG could be detailed in the Commonwealth-level SSPP. The Contractor SSPP would further define SSWG processes.

98. The SSWG is particularly useful for gaining wide agreement of particular mitigation strategies where only qualitative data and subjective opinions are available, or may affect military utility. For example, in mitigating some hazards, either a technological limit or mission effectiveness compromise is required such that further mitigation of a hazard to achieve the necessary HRI is either not feasible or not militarily desirable. Some hazards just cannot be eliminated satisfactorily (eg. loss of thrust in a single engine aircraft), while others could be mitigated but their implementation would consequently erode the military utility of the type. Each of these cases requires different levels of involvement or oversight by the OEM, DAR, TAR and OAR dependent on potential solutions, their respective military utility, and the residual risk in the compromise that each delegate is prepared to accept.

99. Various sub-groups of the SSWG might also exist to support specialist programs. For example, the SwSP will stipulate requirements for a Software Safety Working Group (SwSWG) and the HEP will stipulate requirements for a Human Factors Working Group (HFWG). To provide adequate visibility of the higher-level system safety objectives, these sub-groups are then often linked by specialists common to both the sub-groups and the SSWG.

100. A sample SSWG Charter is provided at Annex I. The Charter's main purpose is to establish aims, membership, agenda procedures, voting rights, and responsibilities, thus maximising SSWG discussions on design hazard issue resolution.

SSP Audits

101. Contractor SSP audits should be conducted within the context of on-going Commonwealth AEO or AMO audits required as part of periodical Contractor Engineering Management System or Quality Management System reviews. There should be no need to hold independent Contractor SSP audits unless warranted by Commonwealth assessed risk.

Transition to In-service System Safety Management

102. As part of the Weapon System LOT in-service strategy, the PO must consider what pragmatic *System Safety* approach is best suited to the *aircraft system*. Importantly, the vast majority of the in-service *System Safety* strategy will be constrained by default, through the SSP approach applied during the acquisition and modification phase, and by the foresight of PO personnel. Typically, in determining a LOT SSP strategy, considerations must include the expected volume of future modifications and their significance, anticipated Weapon System LOT, possible *aircraft system* operational role expansions, and inherent relative platform risks. Resources which may then be required to support these LOT SSP considerations include:

a. a PO transition plan that documents the LOT SSP strategy and out-refers to the draft in-service SSP for detail;

b. the provision of a draft in-service SSPP (and accompanying procedures and training), outlining anticipated *System Safety* strategies and how to pragmatically maintain the FPOs and/or HRIs established during the acquisition and modification phase;

c. a consolidated Hazard Log of all *hazards*, their mitigations, and acceptance sign-off; and

d. sufficient document and personnel resources to maintain the *System Safety* strategy envisaged, including Contractor and sub-contractor *System Safety* deliverables (ie the new System Safety Document Baseline).

COMPLIANCE FINDING

103. To support Design Acceptance, a Compliance Finding must be made against an acquisition and modification project's *System Safety* CBD entry. The results of the Compliance Findings are to be documented in the SCR.

Compliance Finding Responsibilities

104. The PO should approach SCI-DGTA early to identify a suitable agency to be the *System Safety* Compliance Finding Agency (CFA). Typically, the CFA will either be a NAA, the PO, the parent System Program Office (SPO), an *Independent Safety Assessor* (ISA) or DGTA, or a combination thereof. Specific TAR policy on ISAs is under development and may be incorporated into future Chapter amendments, however, if POs wish to engage the services of an ISA in the meantime, early consultation with DGTA is recommended.

Compliance Finding Activities

105. The CFA can make Compliance Findings at any time to support safety objectives for the scope of intended operations. However, Compliance Findings are typically conducted progressively during the acquisition and modification phase to spread the workload sensibly. Typical levels of confidence for a Compliance Finding are established by undertaking activities listed at Annex G, and could be described within the Commonwealth SSPP.

106. All Contractor and sub-contractor SSP documentation may be reviewed as part of the Compliance Finding. The SCR is typically the prime document used to support Compliance Finding, however, further audit against lower-level SSP documentation may also be necessary. Certainly, before any flight testing or flight operations with Commonwealth involvement, the TAR would expect an SCR to have been generated and accepted for the scope of flying expected.

SYSTEM SAFETY PROGRAM REQUIREMENTS FOR IN-SERVICE AIRCRAFT

Introduction

107. Commonwealth responsibilities and risk acceptance requirements do not end with the transition of a project to the in-service organisation. The *aircraft system* SSP may have been created to mitigate hardware, software and human factors' *hazards* identified during either design, integration, operation, maintenance and disposal considerations during the project phase, however, each of these will also be continuously applicable during in-service management, albeit probably on a smaller scale. It is for this reason that the PO is initially best placed to determine the most effective LOT In-Service SSP (ISSSP) strategy, and therefore SSPs developed for *aircraft systems* during the acquisition and modification phase should transition seamlessly to the in-service organisation for on-going *System Safety* management.

108. As ISSSP strategies could be constrained by acquisition approaches, typical SSP transition considerations were discussed earlier in this Chapter. These considerations, together with necessary DGTA oversight during projects, and early in-service organisation awareness of the SSP they are accepting, should ensure optimal ISSSP strategies are prepared for project transition. Nonetheless, as *aircraft system* CRE changes over the LOT, in-service organisations may need to continually tailor their ISSSP to suit, whilst maintaining their original CBD. When tailoring ISSSPs, the intent of the guidance provided herein is important, and if not directly applicable, its intent may still apply. With early DGTA involvement, ISSSP tailoring alternatives, and justifications can be explored.

109. Given most methodologies to be applied to an ISSSP are the same as those applied during acquisition and modification phases, and discussed earlier, they will not be repeated here. Aspects discussed below represent System Safety considerations unique to ISSSPs.

Conducting the In-Service SSP (ISSSP)

110. While SPOs are encouraged to develop ISSSPs which provide an adequate level of confidence within the bounds of their end objectives, typical System Safety Engineering activities for in-service *aircraft systems* would, as a minimum, include:

a. establishing an ISSSP;

b. monitoring the reliability of *safety critical aircraft items/systems*;

c. undertaking hazard analyses for design changes or assessments, commensurate to risk, and accepting identified risks within a formal framework;

d. generating a tailored SCR for the more complex design changes to summarise the system safety strategy used and its achievements; and

e. presenting results of key ISSSP activities to the annual Airworthiness Boards.

111. ***Establishing an ISSSP***. During PO transition to the in-service organisation, the optimum LOT in-service *System Safety* strategy, commensurate to *aircraft system* CRE and cost, should have been agreed. This includes consideration of the following:

a. *People*. An ISSSP Manager needs to be appointed to coordinate *system safety* activities. This person would typically be an experienced senior engineer who could provide guidance and mentor less experienced staff. This position could be established as a secondary duty, however at least one deputy is then also recommended, to assist with the intermittent workload and ensure the ISSSP does not stall in the absence of the Manager.

b. *Processes.* The organisation's EMS should be used to the maximum extent possible, by embedding any ISSSP requirements or procedures into usual processes. An ISSSP Plan (ISSSPP) should be created, either through a transitioning major project providing a draft, or by the in-service organisation for a legacy *aircraft system*. ISSSPP content should reflect requirements of the *System Safety* Certification Basis standard used, and include guidance for the pragmatic generation of safety analyses and *SCRs* for design changes or technical assessments dependent on their *significance* and complexity. All ISSSP activities, and their timing, should be described. This includes defining the planned approach to the identification, tracking, treatment, verification and acceptance of *hazards*. A sample ISSSPP is included at Annex F.

c. *Data.* To introduce a weapon system into service the design organisation would have likely established a robust SSP with corresponding reports (ie the *System Safety Document Baseline*). To maximise the return on weapon system investment, maximum use of legacy or newly generated SSP data should be made, and updated through LOT with modifications, to retain a *System Safety Baseline*. Strategies on optimum use of data will depend on the expected LOT ISSSP approach, and therefore may only require electronic access to data rather than outright purchase.

d. *Training*. All technical personnel should at least attend a System Safety Awareness briefing. All personnel directly involved in conducting, analysing or reviewing a design assessment or change's *System Safety* impact should attend the System Safety Intermediate Course. Both are organised through DGTA. Additional specialist courses may also be required, depending on the ISSSPP approach, and can be organised with DGTA assistance.

112. ***Safety Critical Items/Systems Reliability Monitoring***. Typically, the loss of the function provided by *Safety Critical Items/Systems* (SCI/S) could, in a worst credible representative environment, directly (ie without additional events occurring) affect the aircraft's ability for continued safe flight and landing (ie. a 'direct failure'). Through monitoring therefore, adverse failure rates of SCI/S can be used to gauge the relative risks of in-service aircraft. Designed failure rates would have been used by the OEMs to introduce an inherent level of safety through redundancy, and therefore justify sufficient hazard mitigation. Any reduction between field failure rates and originally designed (or predicted) values could therefore highlight areas of *residual risk* for re-design or acceptance.

113. Without original design (or predicted) failure data it is difficult to determine whether design safety margins are being retained. However, even if original data is available, aircraft system architecture needs to have remained reasonably static to allow for meaningful comparisons. Or conversely, original design data needs to have been updated to reflect significant design changes up to the current configuration. Notwithstanding, in the absence of original design failure data, a considered hypothesis can be applied to historical real-time reliability data to infer design safety levels, albeit with a lower level of confidence. Either way, a baseline for SCI/S can be established, thus allowing better future trend analysis and failure-cause diagnosis (ie the SCI/S may only be failing due to out-of-bounds transients).

114. ***Hazard Analysis***. When design changes (assessments, modifications, deviations and substitutions) are made to in-service aircraft, either new *hazards* may be introduced or they may alter the risk associated with existing *hazards*. Hazard analyses should therefore be conducted to determine the *System Safety* impact and to determine whether the proposed mitigations are sufficient to retain extant safety levels. In particular, the analysis should consider impacts of on SCI/S, which would be included as part of the Judgement Of Significance (JOS) process. The optimal technique for analysing or assessing the design change will depend on the system and the complexity of the change, as described within the ISSSPP. At the very least, for significant design, the in-service organisation should produce a tailored SCR to:

a. assess and document the design change's *System Safety* achievements with respect to its safety impact and the safety objectives defined in the ISSSPP, and

b. justify the level of technical risk inherent in the *aircraft system* post design change.

ISSSP Failure Probability Objectives

115. To ensure that the *aircraft system's* inherent level of safety is maintained, ISSSP Failure Probability Objectives should at least reflect legacy design FPOs. Changes to legacy FPOs are possible, however DGTA consultation is required.

Residual Risk and Risk Acceptance

116. As a starting point, upon project transition, the HRI matrix used by the PO (or provided in the draft ISSSPP) should be adopted by the in-service organisation. If after a settling-in period, the matrix proves to be inadequate for ISSSP purposes additional tailoring should be considered. The matrix is a key element of the ISSSP and will assist with:

a. determining acceptable and unacceptable risks associated with all identified hazards, and therefore simplify JOS assignment;

b. determining residual risk levels when all mitigations (whether short or long-term) have been incorporated; and

c. identifying appropriate personnel to accept residual risk levels.

SYSTEM SAFETY TRAINING OFFERED BY DGTA

117. The following System Safety courses are provided by DGTA:

a. System Safety Awareness Course – Designed for staff either not directly involved with SSPs, or with minimal involvement, and desirous of generic SSP concepts, applications, outputs, and their use within the ADF context. Typically this course is of two hours' duration and is run by SCI3-DGTA on location, on an as-required basis.

b. Aircraft System Safety Engineering Course (PMKeys Code 112689) – Designed for staff directly involved with SSPs, or in the review of related documentation. This course familiarises members with SSP elements and the different analyses and their applications, and traps, and is typically of five-day duration. This course is run by training contractors through SCI3-DGTA at central locations at least twice a year.

Annexes:

A. Definitions and Abbreviations

B. Comparison Of System Safety Related Standards And Guidance

C. Statement Of Work For Military And Commercial-Based Aircraft

Appendix 1 CDRL-1 Project Aircraft System Safety Program Plan (SSPP) For Military-Based Aircraft Or Project Aircraft System Safety Program Plan (SSPP) For Commercial-Based Aircraft

Annex to Appendix 1 System Safety Program Plan Outline

Appendix 2 CDRL-2 System Safety Program Progress Report (SSPR)

Appendix 3 CDRL-3 Project Aircraft Sub-System Hazard Analysis Report (SSHAR) Or System Hazard Analysis Report (SHAR)

Appendix 4 CDRL-4 Project Aircraft Test And Evaluation Hazard Analysis Report

Appendix 5 CDRL-5 Hazard Log

Appendix 6 CDRL-6 ECP System Safety Report (ECPSSR)

Appendix 7 CDRL-7 Safety Verification Report

Appendix 8 CDRL-8 Safety Case Report (SCR)

Annex to Appendix 8 Safety Case Report Outline

Appendix 9 CDRL-9 Aircraft-Level Functional Hazard Assessment (AFHA) Or System-Level Functional Hazard Assessment (SFHA)

Appendix 10 CDRL-10 Preliminary System Safety Assessment (PSSA) Or System Safety Assessment (SSA)

Appendix 11 CDRL-11 Common Cause Analysis (CCA)

Appendix 12 CDRL-12 Health Hazard Assessment (HHA)

Appendix 13 CDRL-13 Operating and Support Hazard Analysis (O&SHA)

Appendix 14 CDRL-14 Safety Requirements/Criteria Analysis (SR/CA)

Appendix 15 CDRL-15 Preliminary Hazard Analysis (PHA)

D. FAR/JAR Based System Safety Program Weapon System Specification

E. MIL-STD-882 Based System Safety Program Weapon System Specification

F. In-Service System Safety Program (ISSSP) Guidance

Appendix 1 Example In-Service System Safety Program Plan (SSPP) for XXSPO

G. Commonwealth-level *System Safety* Program Plan Outline

Appendix 1 Typical SSPP Compliance Finding Activities

H. Sample CBD Entries for Military and Commercial-based System Safety Programs

I. Example System Safety Working Group Charter

Appendix 1 Sample System Safety Working Group Agenda

Blank Page

DEFINITIONS AND ABBREVIATIONS

1. This Annex provides a listing of all abbreviations used in the parent section of this Chapter. Additionally, all terms which have a specific meaning within System Safety, identified in *italics* in the parent Chapter, have been included.

Table 1–A–1 Definitions and Abbreviations

Term/ Abbreviation	Definition	Found in
Aircraft System	The aircraft, all its on-board systems, and ground-based systems which interface to it, directly or indirectly	AAP 7001.054 S2 C1
Catastrophic	Tailorable, but a failure condition that almost always involves death, system loss or severe environmental damage	MIL-STD-882C
	Failure conditions that could result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane	AC 23.1309-1C
Continued safe flight and landing	The airplane is capable of continued controlled flight and landing, possibly using emergency procedures, without requiring exceptional pilot skill or strength. Some airplane damage may occur as a result of the failure condition	AC 23.1309-1C
Critical	Tailorable depending on program goals, but a failure condition that almost always involves severe injury/death, severe occupational illness, major system damage	MIL-STD-882C
	Loss of this function would prevent the continued safe flight and landing of the airplane. The term is associated with a Catastrophic failure condition	AC 23.1309-1C
CSP	Certified Safety Professional – Postnominal used by US System Safety Society for accredited individuals that have passed rigorous system safety related tests, interviews and experience criteria	
ECPSSR	Engineering Change Proposal System Safety Report	MIL-STD-882C
Fail-safe	A design feature that ensures that the system remains safe, or in the event of a failure will cause the system to revert to a state which will not cause a *mishap*	MIL-STD-882C
	In any system or sub-system, the failure of any single element, component or connection during any one flight should not prevent continued safe flight and landing	FAR/JAR AC 25.1309-1C
Failure Probability Objectives	See *FPOs*	
Flight hour	The probability of the subject hazard occurring during a typical flight of mean duration for the airplane type, divided by the mean flight's duration in hours, expressed as a probability per flight hour	AC 23.1309-1C
FPOs	*Failure Probability Objectives* – minimum quantitative probability values assigned to hazard categories	AAP 7001.054 S2 C1

Term/ Abbreviation	Definition	Found in
Hazard	A condition which is a pre-requisite to a *mishap*	MIL-STD-882
	Any condition that compromises the overall safety of the airplane or that significantly reduces the ability of the flight crew to cope with adverse operating conditions	AC 23.1309-1C
Hazard Risk Index	See *HRI*	
Hazardous	A failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be the following: (i) A large reduction in safety margins or functional capabilities; (ii) Physical distress or higher workload such that the crew cannot be relied upon to perform their tasks accurately or completely; or (iii) Serious or fatal injury to an occupant other than the flight crew	AC 23.1309-1C
HEP	Human Engineering Program	
HEPP	Human Engineering Program Plan	
HRI	*Hazard Risk Index* – A program-specific numerical priority assigned to hazards, pre and post-mitigation, based on their risk level (combination of hazard severity and hazard probability). The acceptance of a hazards' HRI is commensurately assigned to program and vendor management dependent on risk	MIL-STD-882C
Human Factor Workload Assessment	Considered in system integration, to ensure that an average crew member, under worst case representative hazard scenarios, can still effectively continue to safely fly and land the *aircraft system*.	AAP 7001.054 S2 C1 AAP 7001.054 S2 C13
Independent Safety Assessor	See *ISA*	
ISA	*Independent Safety Assessor* – a program-independent specialist body responsible for the review of the SSP against the requirements of the standard quoted in the CBD, or with SSP compliance finding	AAP 7001.054 S2 C7
ISSSP	In-Service System Safety Program	AAP 7001.054 S2 C1
Latent Failure	A latent failure is one which is inherently undetected when it occurs (ie failure of the Warning and Caution light system). A significant latent failure is one which, in combination with one or more other specific failures or events, result in a hazardous failure condition	AC 25.1309-1A
Mishap	An unplanned event or series of events resulting in death, injury, illness or damage to equipment, property or environment. Includes incidents and accidents	MIL-STD-882C
MoD	Ministry of Defence, UK	

Term/ Abbreviation	Definition	Found in
Residual Risk	From the perspective of an individual hazard, the risk remaining when all agreed mitigation measures have been implemented, requiring commensurate acceptance as per HRI matrix	MIL-STD-882C
	From the perspective of the total program, the risk left over after all system safety efforts have been fully employed. It is the sum of acceptable risk and unidentified risk – this is the total risk passed onto the user	US Air Force System Safety Handbook
RHI	Risk Hazard Index – See *HRI*	
SAE ARP	Society of Automotive Engineers Automotive Recommended Practice	
Safety	Freedom from mishap	MIL-STD-882C
Safety Case Report	A well-reasoned summary document listing the activities undertaken to satisfy the goals of the SSP, and the artefacts that prove that your systematic analysis and reporting SSP maximised the probability of identifying all risks for your *aircraft system*, tracking, mitigating and accepting them adequately, and that the system is safe and fit for its intended purpose	AAP 7001.054 S2 C1
	NOTE: Different global Air Forces' definition of 'Safety Case' is not necessarily the same as an ADF *Safety Case Report* (ie UK MoD refers to a Safety Case as being the complete body of evidence that an item was designed and integrated correctly to approved standards, by competent people in accordance with approved procedures, with sufficient mitigation, and tested sufficiently to justify being safe (airworthy) for flight – ie the entire ADF Design Acceptance process)	
Safety critical	A term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use (eg safety critical function, safety critical path, safety critical component)	MIL-STD-882C
Safety Critical Items/ Systems	Typically, these are items/systems whereby loss of the function provided by that item/system could, in a worst credible representative environment, directly (ie without additional events occurring) affect the aircraft's ability for continued safe flight and landing. This is consistent with AAP 7001.038-2, which calls this a 'direct failure'	AAP 7001.054 S2 C1 AAP 7001.038-2 S10
SCR	See *Safety Case Report*	AAP 7001.054 S2 C1
SME	Subject Matter Experts	
SSDB	System Safety Document Baseline	AAP 7001.054 S2 C1
SSE	System Safety Engineer - an engineering discipline requiring specialised professional knowledge and skills in applying specific principles, criteria and techniques to identify and eliminate *hazards* in order to reduce associated risk to an acceptable level within the system. It draws upon professional knowledge and specialised skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, and evaluate the safety of the system.	MIL-STD-882C

Term/ Abbreviation	Definition	Found in
SSM	System Safety Manager - a discipline that defines SSP requirements and ensures planning, implementation and completion of *System Safety Engineering* activities consistent with overall SSP objectives.	MIL-STD-882C
SSP	System Safety Program	
SSPP	System Safety Program Plan	
SSWG	System Safety Working Group	
SwSP	Software Safety Program	AAP 7001.054 S2 C1
System Safety	The application of engineering management principles, criteria and techniques to optimise the safety of a ‘system’, within the constraints of operational effectiveness, time and cost throughout all phases of the life cycle.	MIL-STD-882C
Type Design Change	Can be Major or Minor, dependent on the introduction of new or significantly different existing capabilities, or an appreciable effect on weight, balance, structure, reliability, operation, or airworthiness	AAP 7001.053 S2 C1

COMPARISON OF SYSTEM SAFETY RELATED STANDARDS AND GUIDANCE

Table 1–B–1 System Safety Related Design Guidance

Standard/Handbook	Strengths	Weaknesses
Defence Standard 00-970 *'Design and Airworthiness Requirements for Service Aircraft'*	• Provides well defined high-level safety objectives for specified aircraft systems	• Does not provide sufficient low-level detail to address System Safety
Defence Standard 00-55 *'Requirements for Safety Related Software in Defence Equipment'*	• Presents the most rigorous requirements for safety related software of all standards. • Designed to be used in an integrated manner with DEF STAN 00-56 Issue 2	• Could be expensive to implement in total
Defence Standard 00-56 Issue 2 *'Safety Management Requirements For Defence Systems '*	• Very rigorous requirements for System Safety Programs • Designed to be used in an integrated manner with DEF STAN 00-55 • Emphasises use of Independent Safety Auditors • Emphasises management separation • Provides clear guidance on safety analyses to be conducted	• Could be expensive to implement in total
Interim Defence Standard 00-56 Issue 3 *'Safety Management Requirements for Defence Systems'*	• Has taken a goal based approach. • The means of complying in terms of technology, documentation and development is unconstrained. • Only mandates what must be achieved for a demonstrably safe system. • Forces developers to actually consider why and how to make a system safe, rather than merely following activities called out under a prescriptive standard.	• Requires both developers and regulators to be suitably experienced with the technology to ensure that the approach meets the required level of safety. • Regulators are required to make assessments on a case by case basis. • Regulators may not always be resourced sufficiently for this approach. • The acceptability hinges on the safety argument presented as part of the safety case. Thus developers require skills in presenting defensible safety arguments. Likewise, regulators require training in interpreting and assessing safety arguments.
FAR 25.1309 *'Equipment, systems and installations'* including (for Large Transport Aircraft)	• Provide clear system safety objectives	• Applicable to civil aircraft • Does not provide a well defined System Safety Program structure • Does not provide detailed guidance on demonstrating

Standard/Handbook	Strengths	Weaknesses
AC 25.1309-1A *'System Design and Analysis'* of 21 Jun 88 and (for Commuter Category Aircraft) AC 23.1309-1C *'Equipment, Systems and Installations in Part 23 Airplanes'* of 12 Mar 99		achievement of safety objectives • Use 'Go/No-go' hazard acceptance philosophies that may not be easily applied to military aircraft
SAE ARP 4754 *'Certification Considerations for Highly-Integrated or Complex Aircraft Systems'* and SAE ARP 4761 *'Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment'*	• Considered industry best practice with respect to System Safety certification of civil aircraft • Provide detailed guidance on how to undertake System Safety analysis for aircraft	• Applicable to civil aircraft • Does not provide a System Safety Program structure that is easily tailorable to acquisition and modification projects for military aircraft • Does not provide guidance for the contents of a SSPP
MIL-STD-882C *'System Safety Program Requirements'*	• Applicable to military projects • Provides well defined System Safety Program structure • Does not specifically have an aircraft focus, designed for use on any equipment where System Safety compliance is required	• Does not provide guidance on how to undertake system safety analysis
IEEE 1228 *'Standard for Software Safety Plans'*	• Establishes minimum acceptable requirements for software safety plans • Requires Software Safety to be embedded within the System Safety Program • Can be applied throughout the life cycle of software • Provides a comprehensive risk-based Software Safety analysis approach concept	• Provides no example software safety analyses either as stand-alone documents or embedded as part of System Safety analyses • Provides little guidance on how to actually conduct software safety analyses
IEC 61508 'Functional Safety Of Electrical/Electronic/Programmable Electronic Safety-Related Systems'	• Integrates software and hardware as part of the safety process • Requires the application of the integrity levels methodology of other popular standards • Requires a degree of independence	• Is not aircraft–specific • Is designed for use at the system and/or box level, not to integrate results into the overall aircraft level • Does not provide an overall aircraft-level SSP methodology • Does not provide a holistic human factors design approach
Joint Software System Safety Committee 'Software System Safety Handbook' of Dec 99	• Extremely detailed explanations about what and how to ensure a successful Software Safety Program	• Extremely detailed explanations about what and how to ensure a successful Software Safety Program • While structured to integrate

Standard/Handbook	Strengths	Weaknesses
	• Requires Software Safety to be embedded within the System Safety Program • Structure of document and artefacts allows complete integration into a MIL-STD-882 System Safety Program	into a MIL-STD-882 System Safety Program, the intent of document and artefacts can be merged into a Commercial System Safety Program if a knowledgeable Software Safety individual is used to assist • As a handbook, it may be difficult to distil information and incorporate its guidance into specifications and Statements Of Work

Blank Page

STATEMENT OF WORK FOR MILITARY - BASED SYSTEM SAFETY PROGRAMS

1. In establishing a System Safety Program SOW, the Project Manager should note that:

a. the Contractor's draft System Safety Program Plan (SSPP) is a RFT deliverable;

b. the composition, frequency, responsibilities and Charter of the System Safety Working Group should be resolved between the Contractor and the Commonwealth prior to contract signature (guidance on Charter content is provided in this Chapter);

c. if a Commonwealth-level SSPP is required, it should be created before contract signature as it may influence the structure and content of the Contractor's SSP;

d. additional tailoring to guidance provided below is possible depending on NAA involvement, Life-Of-Type maintenance and engineering support philosophy and corresponding SSP strategy;

e. Data Item Descriptions (DIDs) for the specific MIL-STD-882C tasks/reports discussed below are available from SCI-DGTA if required; and

f. a Safety Case Report will probably only be required for design aspects where the Commonwealth has compliance finding responsibilities, therefore early consultation with DGTA is recommended.

2. The following System Safety requirements should be included in a Statement of Work (SOW). A delivery schedule for documents required in accordance with this SOW is included at Table 1–C–1.

SYSTEM SAFETY ENGINEERING

System Safety Program

3. The Contractor shall establish and conduct an integrated System Safety Program (SSP) for [Project Name]. The SSP shall consider potential hazards in the design, integration, operation, maintenance and disposal of the [Project Name], from the perspective of hardware, software and human causal factors. All hazard analyses and assessments conducted shall document and integrate these aspects.

The SSP shall meet the requirements of:

a. MIL-STD-882C 'System Safety Program Requirements';

b. IEEE 1228 'IEEE Standard for Software Safety Plans';

c. AAP 7001.054, Section 2, Chapter 1 'System Safety'; and

d. the Commonwealth-level SSPP.

The scope, details and conduct of the SSP shall be documented in the SSPP, in accordance with CDRL 1 (Appendix 1 to Annex C).

4. The Contractor shall prepare the following CDRLs as part of the SSP and deliver them in accordance with the document delivery schedule shown at Table 1–C–1. Each CDRL shall include hardware, software and human factors' aspects relevant to it:

a. SSPP, in accordance with CDRL – (Appendix 1 to Annex C).

b. SSP Progress Report (SSPPR), in accordance with CDRL – (Appendix 2 to Annex C).

c. System Hazard Assessment Report (SHAR) and Sub-System Hazard Assessment Report (SSHAR), in accordance with CDRL – (Appendix 3 to Annex C).

d. Test and Evaluation Safety Report (T&ESR), in accordance with CDRL - (Appendix 4 to Annex C).

e. Hazard Log/Database, in accordance with CDRL – (Appendix 5 to Annex C).

f. ECP System Safety Report (ECPSSR), in accordance with CDRL – (Appendix 6 to Annex C).

g. Safety Verification Report, in accordance with CDRL – (Appendix 7 to Annex C).

h. Safety Case Report (SCR), in accordance with CDRL – (Appendix 8 to Annex C)

i. Common Cause Analysis (CCA), in accordance with CDRL – (Appendix 11 to Annex C).

j. Health Hazard Assessment (HHA), in accordance with CDRL – (Appendix 12 to Annex C).

k. Operation and Support Hazard Analysis (O&SHA), in accordance with CDRL – (Appendix 13 to Annex C).

l. Safety Requirements/Criteria Analysis (SR/CA), in accordance with CDRL – (Appendix 14 to Annex C).

m. Preliminary Hazard Analysis (PHA), in accordance with CDRL – (Appendix 15 to Annex C).

Table 1–C–1 SOW Document Delivery Schedule

CDRL	Qty	Delivery	Frequency	Review Period	Commonwealth Review Rights
SSPP	2	RFT, ED+30	Annual, and as required	30	Approve
SSPPR	2	Start at SFR-30	6 monthly	30	Review
SSHAR (each includes CCA where appropriate) PHL PHA, SR/CA, draft SSHA SSHA, draft SHA, draft O&SHA SHA, O&SHA, HHA, T&ESR	2	 SDR-30 PDR-30 DDR-30 TRR-30	Once for each batch listed	30	Approve
ECPSSR	2	As Required	As Required	30	Approve
HL/Database	2	Start at PDR-30	6 monthly	30	Approve
Safety Verification Report Draft Final	2	 FTRR-45 On completion of FCA/PCA and Flight Test +30	Once	30	Approve
Safety Case Report Draft Final	2	 FTRR-60 On completion of FCA/PCA and Flight Test +30	Once	30	Approve

Appendices:

1. CDRL-1 Project Aircraft System Safety Program Plan (SSPP) for Military Based Aircraft

2. CDRL-2 System Safety Program Progress Report
3. CDRL-3 Project Aircraft Sub-System Hazard Analysis Report or System Hazard Analysis Report
4. CDRL-4 Project Aircraft Test and Evaluation Hazard Analysis Report
5. CDRL-5 Hazard Log/Database
6. CDRL-6 ECP System Safety Report (ECPSSR)
7. CDRL-7 Safety Verification Report
8. CDRL-8 Safety Case Report (SCR)
9. CDRL-11 Common Cause Analysis (CCA)
10. CDRL-12 Health Hazard Assessment Report
11. CDRL-13 Operating and Support Hazard Analysis Report
12. CDRL-14 Safety Requirements/Criteria Analysis
13. CDRL-15 Preliminary Hazard Analysis

STATEMENT OF WORK FOR COMMERCIAL-BASED SYSTEM SAFETY PROGRAMS

1. In establishing a System Safety Program SOW, the Project Manager should note that:

a. the Contractor's draft System Safety Program Plan (SSPP) is a RFT deliverable;

b. the composition, frequency, responsibilities and Charter of the System Safety Working Group should be resolved between the Contractor and the Commonwealth prior to contract signature (guidance on Charter content is provided in this Chapter);

c. if a Commonwealth-level SSPP is required, it should be created before contract signature as it may influence the structure and content of the Contractor's SSP;

d. additional tailoring to guidance provided below is possible depending on NAA involvement, Life-Of-Type maintenance and engineering support philosophy and corresponding SSP strategy;

e. Data Item Descriptions (DIDs) for the specific MIL-STD-882C tasks/reports discussed below are available from SCI-DGTA if required; and

f. a Safety Case Report will probably only be required for design aspects where the Commonwealth has compliance finding responsibilities, therefore early consultation with DGTA is recommended.

2. The following System Safety requirements should be included in a Statement of Work (SOW). A delivery schedule for documents required in accordance with this SOW is included at Table 1–C–2

SYSTEM SAFETY ENGINEERING

System Safety Program

3. The Contractor shall establish and conduct an integrated System Safety Program (SSP) for [Project Name]. The SSP shall consider potential hazards in the design, integration, operation, maintenance and disposal of the [Project Name], from the perspective of hardware, software and human causal factors. All hazard analyses and assessments conducted shall document and integrate these aspects.

4. The SSP shall meet the requirements of:

a. FAR/JAR 2x.1309;

b. AC 23.1309-1C or AC 25.1309-1A (also respectively applicable to FAR/JAR 27.1309 and 29.1309);

c. SAE ARP 4754;

d. SAE ARP 4761;

e. MIL-STD-882C Task 101 'System Safety Program';

f. MIL-STD-882C Task 102 'System Safety Program Plan';

g. IEEE 1228 'IEEE Standard for Software Safety Plans';

h. AAP7001.054, Section 2 Chapter 1 'System Safety'; and

i. the Commonwealth-level SSPP.

The scope, details and conduct of the SSP shall be documented in the SSPP, in accordance with CDRL 1 (Appendix 1 to Annex C).

5. The Contractor shall prepare the following CDRLs as part of the SSP and deliver them in accordance with the document delivery schedule shown at Table 1–C–2. Each CDRL shall include hardware, software and human factors' aspects relevant to it:

a. SSPP, in accordance with CDRL – (Appendix 1 to Annex C).

b. Aircraft-level Functional Hazard Assessment (AFHA), in accordance with CDRL - (Appendix 9 to Annex C).

c. System-level Functional Hazard Assessments (SFHAs) for each system, in accordance with CDRL - (Appendix 9 to Annex C).

d. Preliminary System Safety Assessments (PSSAs) for each system, in accordance with CDRL - (Appendix 10 to Annex C).

e. System Safety Assessments (SSAs) for each system, in accordance with CDRL - (Appendix 10 to Annex C).

f. Test and Evaluation Safety Report (T&ESR), in accordance with CDRL – (Appendix 4 to Annex C).

g. Hazard Log/Database, in accordance with CDRL – (Appendix 5 to Annex C).

h. ECP System Safety Report (ECPSSR), in accordance with CDRL – (Appendix 6 to Annex C).

i. Common Cause Analysis, in accordance with CDRL – (Appendix 11 to Annex C).

j. Safety Case Report, in accordance with CDRL – (Appendix 8 to Annex C).

k. Health Hazard Assessment, in accordance with CDRL – (Appendix 12 to Annex C).

Table 1–C–2 SOW Document Delivery Schedule

CDRL	Qty	Delivery	Frequency	Review Period	Commonwealth Review Rights
SSPP	2	RFT, ED+30	Annual, and as required	30	Approve
Safety Assessments (each includes CCA where appropriate) AFHA SFHA for each system PSSA for each system SSA for each system T&E Safety and HHA	2	 ED+90 PDR-60 DDR-60 TRR-60 TRR-30	Once for each batch listed	30	Approve
ECPSSR	2	As Required	As Required	30	Approve
HL/Database	2	Start at PDR-30	6 monthly	30	Approve
Safety Case Report Draft Final	2	 TRR-60 (as part of the T&E Safety report) On completion of FCA/PCA and Flight Test +30	Once	30	Approve

Appendices:

1. CDRL-1 Project Aircraft System Safety Program Plan (SSPP) for Military Based Aircraft
2. CDRL-4 Project Aircraft Test and Evaluation Hazard Analysis Report
3. CDRL-5 Hazard Log/Database
4. CDRL-6 ECP System Safety Report (ECPSSR)
5. CDRL-8 Safety Case Report (SCR)
6. CDRL-9 Aircraft- Level Functional Hazard Assessment (AFHA) or System-Level Functional Hazard Assessment (SFHA)
7. CDRL-10 Preliminary System Safety Assessment (PSSA) or System Safety Assessment (SSA)
8. CDRL-11 Common Cause Analysis (CCA)
9. CDRL-12 Health Hazard Assessment Report

CDRL-1 PROJECT AIRCRAFT SYSTEM SAFETY PROGRAM PLAN (SSPP) FOR MILITARY-BASED AIRCRAFT

Description/Purpose of Deliverable

1. The SSP describes the Contractor's System Safety tasks and activities that will be performed during the Project to identify, evaluate, and eliminate or reduce hardware, software and human causal factor hazards associated with design, integration, operation, maintenance, and disposal of the system.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-STD-882C 'System Safety Program Requirements'.

b. MIL-STD-882C Task 101'System Safety Program'.

c. MIL-STD-882C Task 102 'System Safety Program Plan'.

d. DI-SAFT-80100A 'System Safety Program Plan'.

e. AAP 7001.054 'Airworthiness Design Requirements Manual'.

f. System Specification.

g. Program Statement of Work.

h. IEEE 1228 'IEEE Standard for Software Safety Plans'.

i. Joint Software System Safety Committee's 'Software System Safety Handbook'.

j. SAE ARP 4761 'Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment'.

Content

NOTE

The Commonwealth expects Tenderers to have conducted such a program during previous development efforts with some additional activity now being required for new unique ADF requirements of the proposed aircraft.

SSP requirements are to be based on MIL-STD-882C. However, Tenderers can propose to use standards that provide an equivalent level of safety and are acceptable to the Commonwealth. The Commonwealth places the onus on Tenderers to demonstrate that the proposed SSP provides an equivalent level of safety to the program outlined below.

3. The Contractor shall develop a System Safety Program Plan (SSPP) describing the Contractor's MIL-STD-882C SSP for the *[Project Name]*. The plan shall describe the safety and hazard assessment, analysis and documentation process, and the necessary tasks and activities of system safety management and system safety engineering required to identify, track, evaluate and eliminate or reduce hardware, software and human factor safety hazards identified in design, integration, operation, maintenance and disposal to acceptable levels.

4. The SSPP shall include details of the Contractor's implementation of hazard analysis, assessments and safety assurance activities for the system to meet the requirements of MIL-STD-882C, IEEE 1228, AAP 7001.054 Section 2 Chapter 1 (tailored as necessary), and the System Safety requirements of the System Specification and Program Statement of Work.

5. The SSPP shall describe the Contractor's tailoring of System Safety activities to reflect the Contractor's SSP. All tailoring shall include justification. The SSPP shall include descriptions of how the Contractor will undertake all safety Tasks and activities as tailored.

6. The SSPP shall describe:

a. the Contractor's SSP in accordance with the requirements of MIL-STD-882C Task 101 and 102, and DI-SAFT-80100A;

b. the relationship of this plan to the Human Engineering Program, and if a Human Engineering Program does not exist, how human causal factors will be considered in the SSP;

c. the relationship of this plan to other related plans;

d. how each of the SSP requirements will be met;

e. the extent and activities of the hardware, software and human factor safety programs and how they will be integrated into a single SSP through the conduct of required analyses and assessments;

f. where the System Safety responsibility boundaries lie between the Contractor, ASCENG, JALO, OSG and the PO, for projects involving stores or explosive ordnance;

g. how it plans to address, perform and document hazard analyses and assessments for waivers, deviations, trade studies and post contract signature Engineering Change Proposal (ECP) effects on the weapon system design, integration, operation, maintenance and disposal; and

h. the process of reviewing project Discrepancy Reports (DRs) and System Trouble Reports (STRs) for potential safety implications and how safety assessments and recommendations for all safety-related DRs and STRs shall be documented.

7. The SSPP shall describe how the SSP's System Safety Document Baseline (SSDB) shall be developed, controlled and continually updated to reflect design changes or modifications, therefore providing an on-going snapshot of weapon system System Safety health.

8. The SSPP shall describe the Contractor's Software Safety Program in accordance with the requirements of IEEE 1228 and the guidance of the Software System Safety Handbook. The Software Safety Program shall be an integral part of the SSP, and shall describe:

a. how to establish software safety-critical requirements for the *[Project Name]* and ensure these requirements are flowed down to the applicable subcontractors;

b. how the Contractor's safety representative shall participate in software evaluations and reviews at both company and sub-contractor level if the highest-level hazard that can be attributed to the software under review is either Catastrophic or Critical;

c. how software safety assessments/analyses shall document and substantiate requirement traceability and that safety-critical software provides an acceptable level of safety risk; and

d. how new, Commercial-Off-The-Shelf (COTS) and modified software, including its interfaces to existing software and hardware shall be categorised to, and evaluated against, RTCA DO-178B.

9. In describing the safety assurance activities for the system, the SSPP shall include the following:

a. the Hazard Risk Indices (HRIs) and Failure Probability Objectives (FPOs) to be achieved (including both quantitative and qualitative objectives);

b. HRI acceptance levels commensurate with risk;

c. Residual risk acceptance procedures;

d. closed-loop hazard tracking procedures;

e. the type of analysis methods used and why they were chosen above others;

f. the Charter of the System Safety Group/System Safety Working Group;

g. what historical *System Safety* data will be used to assist in the design, and how it will be used;

h. the procedures used to conduct each assessment or analysis, and the inclusion of hardware, software and human factors' considerations into each;

i. the expected outcomes of the SSP;

j. the generation of a Test and Evaluation Risk Matrix (TERM) for ground and flight test purposes; and

k. how the results of the assessments/analyses lead to the generation of a Safety Case Report.

10. The SSPP shall use safety design risk acceptability levels defined in the SSPP HRI matrix as design goals, or may ask for a deviation or waiver from the Commonwealth as appropriate. The safety design risk acceptability levels for equipment and systems shall be established based on the relationship of the failure condition probability and the severity of that failure condition. Catastrophic and Critical category hazards shall be mitigated using quantitative HRI values, unless otherwise approved by the Commonwealth.

11. The Contractor shall implement a safety assessment process for safety requirement generation and verification. This process shall provide a methodology to evaluate functions and the design of new or modified systems performing these functions to determine that the associated hardware, software and human factors failure conditions and hazards, and their effects, have been properly addressed. The process shall provide the necessary assurance and documentation to ensure that all failure conditions and hazards have been identified and that all combinations of failures that could cause those failure conditions and hazards, have been considered.

12. **SSP System Safety Program Management and Control Tasks**. The SSP shall include the following MIL-STD-882C program management and control tasks, as described in the SSPP:

a. Task 101 'System Safety Program'.

b. Task 102, 'System Safety Program Plan' (SSPP).

c. Task 103, 'Integration/Management of Associate Contractors, Sub-contractors, and Architect and Engineering Firms'.

d. Task 104, 'System Safety Program Reviews/Audits'.

e. Task 105, 'System Safety Group/System Safety Working Group (SSG/SSWG) Support'. The Contractor shall also produce the Minutes of these meetings.

f. Task 106, 'Hazard Tracking and Risk Resolution'.

g. Task 107, 'System Safety Program Progress Report' (SSPPR).

NOTE

Tailoring of these tasks in accordance with Table 1–C1-1, or further where warranted, should be considered.

13. **SSP Design and Integration Tasks**. The SSP shall include the following MIL-STD-882C design and integration tasks, as described in the SSPP:

a. MIL-STD-882C Task 201, 'Preliminary Hazard List' (PHL).

b. MIL-STD-882C Task 202, 'Preliminary Hazard Analysis' (PHA).

c. MIL-STD-882C Task 203, ‘Safety Requirements/Criteria Analysis’ (SR/CA).

d. MIL-STD-882C Task 204, ‘Subsystem Hazard Analysis’ (SSHA).

e. MIL-STD-882C Task 205, ‘System Hazard Analysis’ (SHA).

f. MIL-STD-882C Task 206, ‘Operating and Support Hazard Analysis’ (O&SHA).

g. MIL-STD-882C Task 207, ‘Health Hazard Assessment’ (HHA).

h. SAE ARP 4761 Common Cause Analysis (CCA - incorporating Zonal Safety Analysis, Particular Risks Analysis and Common Mode Analysis), as sub-part of the applicable analyses produced above.

NOTE

Tailoring of these tasks in accordance with Table 1–C1-1, or further where warranted, should be considered.

14. SSP Design Evaluation Tasks. The SSP shall include the following MIL-STD-882C design evaluation tasks, as described in the SSPP:

a. Task 302, ‘Test and Evaluation Safety’.

b. Task 303, ‘Safety Review of Engineering Change Proposals (ECPs), Specification Change Notices (SCNs), Software Problem Reports, and Requests for Deviation/Waiver’ (ECPSSR), as follows:

(1) This task shall be conducted on Class 1 ECPs, SCNs, all Problem Reports, Deficiency Reports, System Trouble Reports, Deviations and Waivers, and Trade Studies where safety is impacted or could be affected. Where not impacted or affected, the parent documents shall record the justification.

(2) The complexity and scope of the Class 1 ECP shall dictate what other hazard analyses and assessments shall also be submitted as part of the ECP incorporation process, as described in the ECPSSR. The ECPSSR shall also contain justification as to why particular assessments and analyses may not be required.

(3) The ECP proposal shall also describe any requested tailoring of the ECPSSR DID and of SSP assessments and analyses, providing justification.

NOTE

Tailoring of these tasks in accordance with Table 1–C1-1, or further where warranted, should be considered.

15. SSP Safety Compliance Verification Tasks. The SSP shall include the following MIL-STD-882C compliance and verification tasks, as described in the SSPP:

a. Task 401, ‘Safety Verification’.

b. Task 402, ‘Safety Compliance Assessment’ (also to incorporate requirements of Task 301).

NOTE

Tailoring of these tasks in accordance with Table 1–C1-1, or further where warranted, should be considered.

Table 1–C1–1 Example MIL-STD-882C System Safety Program Tailoring Guidance

Low Technical Risk Program	Medium Technical Risk Program	High Technical Risk Program
TASK 101 - SSP	TASK 101 - SSP	TASK 101 - SSP
TASK 102 – SSPP TASK 105 – SSG/SSWG TASK 106 – Hazard Tracking	TASK 102 – SSPP TASK 104 – Reviews/Audits TASK 105 – SSG/SSWG TASK 106 – Hazard Tracking	TASK 102 – SSPP TASK 103 – Mgmt of Contractors TASK 104 – Reviews/Audits TASK 105 – SSG/SSWG TASK 106 – Hazard Tracking TASK 107 – SSPPR
(Note: All below Tasks include CCA where applicable) TASK 202 – PHA TASK 204 – SSHA TASK 205 – SHA TASK 206 – OS&HA TASK 207 – HHA	(Note: All below Tasks include CCA where applicable) TASK 201 – PHL TASK 202 – PHA TASK 203 – SR/CA TASK 204 – SSHA TASK 205 – SHA TASK 206 – OS&HA TASK 207 – HHA	(Note: All below Tasks include CCA where applicable) TASK 201 – PHL TASK 202 – PHA TASK 203 – SR/CA TASK 204 – SSHA TASK 205 – SHA TASK 206 – O&SHA TASK 207 – HHA
TASK 303 – ECPSSR	TASK 302 – T&E Safety TASK 303 – ECPSSR	TASK 302 – T&E Safety TASK 303 – ECPSSR
TASK 402 – Safety Compliance Assessment (incorporating TASK 301, and both forming part of the Safety Case Report)	TASK 402 – Safety Compliance Assessment (incorporating TASK 301, and both forming part of the Safety Case Report)	TASK 401 – Safety Verification TASK 402 – Safety Compliance Assessment (incorporating TASK 301, and both forming part of the Safety Case Report)
Note: The intent of some Tasks may also be suitably achieved through amalgamation with other tasks		

16. The SSPP shall generate a draft In-Service System Safety Program Plan (ISSSPP) for the in-service organisation prior to fielding the aircraft system, outlining anticipated System Safety strategies and how to pragmatically maintain the FPOs and HRIs established during the acquisition and modification phase.

CDRL-1 PROJECT AIRCRAFT SYSTEM SAFETY PROGRAM PLAN (SSPP) FOR COMMERCIAL-BASED AIRCRAFT

Description/Purpose of Deliverable

1. The SSPP describes the Contractor's System Safety tasks and activities that will be performed during the Project to identify, evaluate, and eliminate or reduce hardware, software and human causal factor hazards associated with the design, integration, operation, maintenance, and disposal of the system.

Preparation Instructions

2. The following documents are referenced herein:

a. FAR/JAR 23.1309/25.1309/27.1309/29.1309.

b. SAE ARP 4754 'Certification Considerations for Highly-Integrated or Complex Aircraft Systems'.

c. SAE ARP 4761 'Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment'.

d. AAP 7001.054 'Airworthiness Design Requirements Manual'.

e. System Specification.

f. Program Statement of Work.

g. IEEE 1228 - 'IEEE Standard for Software Safety Plans'.

h. Joint Software System Safety Committee 'Software System Safety Handbook'.

i. MIL-STD-882C 'System Safety Program Requirements'.

j. DI-SAFT-80100A 'System Safety Program Plan'.

Content

NOTE

The Commonwealth expects Tenderers to have conducted such a program during previous development efforts with some additional activity now being required for new unique ADF requirements of the proposed aircraft.

These SSP requirements are to be based on FAR/JAR 23.1309, 25.1309, 27.1309 or 29.1309 (hereafter referred to as FAR/JAR 2x.1309) and associated Advisory Circulars, Notices and Orders, SAE ARP 4754 and SAE ARP 4761. However, Tenderers can propose to use standards that provide an equivalent level of safety and are acceptable to the Commonwealth. The Commonwealth places the onus on Tenderers to demonstrate that the proposed SSP provides an equivalent level of safety to the program outlined below.

3. The Contractor shall develop a System Safety Program Plan (SSPP) describing the Contractor's FAR/JAR 2x.1309 SSP for the *[Project Name]*. The plan shall describe the safety and hazard assessment, analysis and documentation process, and the necessary tasks and activities of system safety management and system safety engineering required to identify, track, evaluate and eliminate or reduce hardware, software and human factor safety hazards identified in design, integration, operation, maintenance and disposal to acceptable levels.

4. The SSPP shall include details of the Contractor's implementation of hazard analysis, assessments and safety assurance activities for the system to meet the requirements of FAR/JAR 2x.1309, SAE ARP 4754, SAE ARP 4761, MIL-STD-882C, IEEE 1228, AAP 7001.054 Section 2 Chapter 1 (tailored as necessary), and the System Safety requirements of the System Specification and Program Statement of Work.

5. The SSPP shall describe the Contractor's tailoring of System Safety activities to reflect the Contractor's SSP. All tailoring shall include justification. The SSPP shall include descriptions of how the Contractor will undertake all safety Tasks and activities as tailored.

6. The SSPP shall describe:

a. the Contractor's SSP in accordance with the requirements of SAE ARP 4754 and 4761;

b. the Contractor's SSP in accordance with the requirements of MIL-STD-882C Tasks 101 and 102, and DI-SAFT-80100A;

c. the relationship of this plan to the Human Engineering Program, and if a Human Engineering Program does not exist, how human causal factors will be considered in the SSP;

d. the relationship of this plan to other related plans;

e. how each of the SSP requirements will be met;

f. the extent and activities of the hardware, software and human factor safety programs and how they will be integrated into a single SSP through the conduct of required analyses and assessments;

g. where the System Safety responsibility boundaries lie between the Contractor, ASCENG, JALO, OSG and the PO, for projects involving stores or explosive ordnance;

h. how it plans to address, perform and document hazard analyses and assessments for waivers, deviations, trade studies and post contract signature Engineering Change Proposal (ECP) effects on the weapon system design, integration, operation, maintenance and disposal; and

i. the process of reviewing project Discrepancy Reports (DRs) and System Trouble Reports (STRs) for potential safety implications and how safety assessments and recommendations for all safety-related DRs and STRs shall be documented.

7. The SSPP shall describe how the SSP's System Safety Document Baseline (SSDB) shall be developed, controlled and continually updated to reflect design changes or modifications, therefore providing an on-going snapshot of weapon system System Safety health.

8. The SSPP shall describe the Contractor's Software Safety Program in accordance with the requirements of IEEE 1228 and the guidance of the Software System Safety Handbook. The Software Safety Program shall be an integral part of the SSP, and shall describe:

a. how to establish software safety-critical requirements for the *[Project Name]* and ensure these requirements are flowed down to the applicable subcontractors;

b. how the Contractor's safety representative shall participate in software evaluations and reviews at both company and sub-contractor level if the highest-level hazard that can be attributed to the software under review is either Catastrophic or Hazardous;

c. how software safety assessments/analyses shall document and substantiate requirement traceability and that safety-critical software provides an acceptable level of safety risk; and

d. how new, Commercial-Off-The-Shelf (COTS) and modified software, including its interfaces to existing software and hardware shall be categorised to, and evaluated against, RTCA DO-178B.

9. In describing the safety assurance activities for the system, the SSPP shall include the following:

a. the Hazard Risk Indices (HRIs) and Failure Probability Objectives (FPOs) to be achieved (including both quantitative and qualitative objectives);

b. HRI acceptance levels commensurate with risk;

c. residual risk acceptance procedures;

d. closed-loop hazard tracking procedures;

e. the type of analysis methods used and why they were chosen above others;

f. the Charter of the System Safety Group/System Safety Working Group;

g. what historical *System Safety* data will be used to assist in the design, and how it will be used;

h. the procedures used to conduct each assessment or analysis, and the inclusion of hardware, software and human factors' considerations into each;

i. the expected outcomes of the SSP;

j. the generation of a Test and Evaluation Risk Matrix (TERM) for ground and flight test purposes; and

k. how the results of the assessments/analyses lead to the generation of a Safety Case Report.

10. The SSPP shall use safety design risk acceptability levels defined in the SSPP HRI matrix as design goals, or may ask for a deviation or waiver from the Commonwealth as appropriate. The safety design risk acceptability levels for equipment and systems shall be established based on the relationship of the failure condition probability and the severity of that failure condition. Catastrophic and Hazardous category hazards shall be mitigated using quantitative HRI values, unless otherwise approved by the Commonwealth.

11. The Contractor shall implement a safety assessment process for safety requirement generation and verification. This process shall provide a methodology to evaluate functions and the design of new or modified systems performing these functions to determine that the associated hardware, software and human factors failure conditions and hazards, and their effects, have been properly addressed. The process shall provide the necessary assurance and documentation to ensure that all failure conditions and hazards have been identified and that all combinations of failures that could cause those failure conditions and hazards, have been considered.

12. **System Safety Program Management and Control Activities**. The SSP shall include the following MIL-STD-882C program management and control tasks, as described in the SSPP:

a. Task 101 'System Safety Program'.

b. Task 102, 'System Safety Program Plan' (SSPP).

c. Task 103, 'Integration/Management of Associate Contractors, Sub-contractors, and Architect and Engineering Firms'.

d. Task 105, 'System Safety Group/System Safety Working Group (SSG/SSWG) Support'. The Contractor shall also produce the Minutes of these meetings.

e. Task 106, 'Hazard Tracking and Risk Resolution'.

NOTE

Tailoring of these tasks in accordance with Table 1–C1-2, or further where warranted, should be considered.

13. **System Safety program Design and Integration Activities**. The SSP shall include the following SAE ARP 4761 design and integration assessments, as described in the SSPP:

a. Aircraft-level Functional Hazard Assessment (AFHA).

b. System-level Functional Hazard Assessments (SFHAs) for each system.

NOTE

Tailoring of these tasks in accordance with Table 1–C1-2, or further where warranted, should be considered.

14. System Safety Program Design Evaluation Activities. The SSP shall include the following design evaluation activities, as described in the SSPP:

a. SAE ARP 4761 Preliminary System Safety Assessments (PSSAs) for each system.

b. MIL-STD-882C Task 302, 'Test and Evaluation Safety'.

c. MIL-STD-882C Task 207, 'Health Hazard Assessment'.

NOTE

Tailoring of these tasks in accordance with Table 1–C1-2, or further where warranted, should be considered.

15. System Safety Program Safety Compliance Verification Activities. The SSP shall include the following SAE ARP 4761 compliance and verification assessment, as described in the SSPP:

a. System Safety Assessments (SSAs) for each system.

NOTE

Tailoring of these tasks in accordance with Table 1–C1-2, or further where warranted, should be considered.

16. System Safety Program Continuous System Safety Assessments. The SSP shall include the following specialist analyses, either as stand-alone documents or embedded within above assessments, as described within the SSPP:

a. SAE ARP 4761 Common Cause Analysis (incorporating Zonal Safety Analysis, Particular Risks Analysis and Common Mode Analysis), as part of the Safety Assessments produced above.

b. MIL-STD-882C Task 303, 'Safety Review of Engineering Change Proposals (ECPs), Specification Change Notices (SCNs), Problem Reports, and Requests for Deviation/Waiver' (ECPSSR), as follows:

(1) This task shall be conducted on Class 1 ECPs, SCNs, all Problem Reports, Deficiency Reports, System Trouble Reports, Deviations and Waivers, and Trade Studies where safety is impacted or could be affected. Where not impacted or affected, the parent documents shall record the justification.

(2) The complexity and scope of the Class 1 ECP shall dictate what other hazard analyses and assessments shall also be submitted as part of the ECP incorporation process, as described in the ECPSSR. The ECPSSR shall also contain justification as to why particular assessments and analyses may not be required.

(3) The ECP proposal shall also describe any requested tailoring of the ECPSSR DID and of SSP assessments and analyses, providing justification.

NOTE

Tailoring of these tasks in accordance with Table 1–C1-2, or further where warranted, should be considered.

Table 1–C1–2 Example Commercial System Safety Program Tailoring Guidance

Low Technical Risk Program	Medium Technical Risk Program	High Technical Risk Program
MIL-STD-882C TASK 101 - SSP	MIL-STD-882C TASK 101 - SSP	MIL-STD-882C TASK 101 - SSP
MIL-STD-882C TASK 102 – SSPP MIL-STD-882C TASK 105 – SSG/SSWG MIL-STD-882C TASK 106 – Hazard Tracking	MIL-STD-882C TASK 102 – SSPP MIL-STD-882C TASK 105 – SSG/SSWG MIL-STD-882C TASK 106 – Hazard Tracking	MIL-STD-882C TASK 102 – SSPP MIL-STD-882C TASK 103 – Mgmt of Contractors MIL-STD-882C TASK 105 – SSG/SSWG MIL-STD-882C TASK 106 – Hazard Tracking
(Note: All below activities include CCA where applicable) SAE ARP 4761 SSA for each system MIL-STD-882C TASK 207 – HHA	(Note: All below activities include CCA where applicable) SAE ARP 4761 SFHA for each system SAE ARP 4761 SSA for each system MIL-STD-882C TASK 207 – HHA	(Note: All below activities include CCA where applicable) SAE ARP 4761 AFHA SAE ARP 4761 SFHA for each system SAE ARP 4761 PSSA for each system SAE ARP 4761 SSA for each system MIL-STD-882C TASK 207 – HHA
MIL-STD-882C TASK 303 – ECPSSR Safety Case Report	MIL-STD-882C TASK 302 – T&E Safety MIL-STD-882C TASK 303 – ECPSSR Safety Case Report	MIL-STD-882C TASK 302 – T&E Safety MIL-STD-882C TASK 303 – ECPSSR Safety Case Report
Note: The intent of some activities may also be suitably achieved through amalgamation with other tasks		

17. The SSPP shall generate a draft In-Service System Safety Program Plan (ISSSPP) to the in-service organisation prior to fielding the aircraft system, outlining anticipated System Safety strategies and how to pragmatically maintain the FPOs and HRIs established during the acquisition and modification phase.

SYSTEM SAFETY PROGRAM PLAN (SSPP) OUTLINE

1. The following outline is provided as an example outline of a typical SSPP. More information on content is included in both the parent Chapter and Annex.

System Safety Program Plan	
SSPP.1	**Authorship**
SSPP.1.1	Identify people and organisation responsible for the SSP and for producing the SSPP
SSPP.2	**Scope**
SSPP.2.1	Reference the Project which this SSPP forms part of.
SSPP.2.2	Define the System
SSPP.2.3	Define the SSPP's scope. Note that it must at least cover the mitigation of hazards caused by hardware, software and human causal factors that could occur during weapon system design, integration, operation, maintenance and disposal.
SSPP.2.4	Define the SSPP's objectives (ie the safety objectives of your program)
SSPP.3	**Compliance**
SSPP.3.1	Outline the regulatory basis for the SSPP
SSPP.4	**System Safety Organisation**
SSPP.4.1	Describe the structure of the System Safety organisation, including interfaces between the Contractor and subcontractors
SSPP.4.2	Describe what lower level procedures will be used to conduct the analyses/assessments and who will peer review and approve safety outputs
SSPP.4.3	Describe how SSP resources (including hardware safety, software safety and human factors specialists) allocated to the System Safety Program have been determined as adequate for the workload and tasks to be completed. Also describe the frequency of workload reviews and how additional manpower will be gained to overcome short or long-term shortfalls.
SSPP.5	**Program Activities**
SSPP.5.1	Describe what organisational activities will be undertaken as part of the SSP
SSPP.5.2	Describe the hazard analysis activities that will be undertaken
SSPP.5.3	Outline what documentation will be produced
SSPP.5.4	Relate SSP milestones to Project milestones
SSPP.6	**Hazard Classification, Tracking and Control**
SSPP.6.1	Provide clear qualitative and quantitative definitions of hazard categories and probabilities, including the Hazard Risk Index (HRI) matrix
SSPP.6.2	Provide risk control and acceptance criteria
SSPP.6.3	Describe the contents of the Hazard Log/Database, and process for maintaining it
SSPP.6.4	Describe the procedures for confirming hazards have been mitigated adequately
SSPP.6.5	Describe the format, purpose, attendees and Charter of the System Safety Group and System Safety Working Group
SSPP.7	**Software Safety Interface**
SPPP.7.1	Describe the interfaces between the SSP and the Software Safety Program
SSPP.8	**Human Engineering Interface**
SPPP.8.1	Describe the interfaces between the SSP and the Human Engineering Program
SSPP.9	**Commonwealth**
SPPP.9.1	Describe the interfaces between the SSP and the Commonwealth
SSPP.10	**Tables/Appendices**
SSPP.10.1	As required

Blank Page

CDRL-2 SYSTEM SAFETY PROGRAM PROGRESS REPORT

Description/Purpose

1. The System Safety Program Progress Report (SSPPR) shall summarise activities, progress and status of the SSP since the last report. This shall demonstrate that system safety considerations for hardware, software and human causal factors are being iteratively and proactively addressed in system and sub-system considerations, working groups, analyses and assessments, for hazards identified in design, integration, operation, maintenance and disposal.

2. The SSPPR documents the Contractor's efforts in conducting Task 107, System Safety Progress Summary, of MIL-STD-882C.

Preparation Instructions

3. The following documents are referenced herein:

a. MIL-STD-882C, Task 107 'System Safety progress Summary'.

b. DI-SAFT-80105A, 'System Safety Program Progress Report'.

Content

4. The content of the SSPPR shall comply with the requirements specified in Task 107 of MIL-STD-882C and DI-SAFT-80105A, and integrate hardware, software and human factor aspects of the System Safety Program into the report.

5. The SSPPR shall review System Safety activities and any significant outcomes since the previous reporting period.

6. The SSPPR shall preview the System Safety activities to be undertaken in the forthcoming reporting period.

Blank Page

CDRL-3 PROJECT AIRCRAFT SUB-SYSTEM HAZARD ANALYSIS REPORT AND SYSTEM HAZARD ANALYSIS REPORT

SUB-SYSTEM HAZARD ANALYSIS REPORT (SSHAR)

Description/Purpose

1. A Sub-system Hazard Analysis (SSHA) shall be created for each sub-system and shall:

a. verify sub-system compliance with safety requirements contained in specifications, statements of work and other applicable documents;

b. identify previously unidentified hazards associated with the design of sub-systems including component failure modes, hardware, software and human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem;

c. recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels, in accordance with the SSPP; and

d. confirm the hardware criticality and software developmental assurance levels required of the system and sub-system.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-STD-882C Task 204, ‘Sub-System Hazard Analysis’.

b. DI-SAFT-80101B, ‘System Safety Hazard Analysis Report’.

Content

3. The content of the SSHAR shall comply with the requirements specified in MIL-STD-882 Task 204 and DI-SAFT-80101B, and integrate hardware, software and human factor aspects of the System Safety Program into the report. The report shall also include, but not be limited to, analysis of hazards from the following potential sources:

a. isolation of energy sources,

b. fuels and propellents,

c. system environmental constraints,

d. external environmental impact,

e. explosive devices,

f. compatibility of materials,

g. electromagnetic environmental effects,

h. pressure vessels,

i. crash safety,

j. operation and maintenance hazards,

k. training hazards,

l. egress, rescue and survival hazards,

m. life support requirements,

n. fire ignition and propagation,

o. shock/damage resistance,

p. equipment layout and lighting,

q. fail safe design,

r. vulnerability and survivability,

s. protective clothing, equipment or devices, and

t. direct and indirect lightning effects.

4. In each ECP proposed subsequent to contract signature, the Contractor shall propose the amendment of SSHARs already generated.

5. ***Initial (Draft) Delivery in Support of Preliminary Design Review (PDR).*** For each sub-system, the SSHAR delivered to support PDR shall contain relevant results of the system Preliminary Hazard Analysis (MIL-STD-882C Task 202), the system Safety Requirements/Criteria Analysis (MIL-STD-882C Task 203), and initial results of the Subsystem Hazard Analysis (MIL-STD-882C Task 204) of that sub-system. It shall include definition of the failure condition criticality and design requirements that are to be satisfied for each sub-system. Failure severity classifications shall be Catastrophic, Critical, Marginal and Negligible. A sub-system's severity classification shall be at least as severe as its most severe hazard.

6. ***Delivery in Support of Detailed Design Review (DDR).*** For each sub-system, the SSHAR delivered to support DDR shall contain the final results of the Sub-System Hazard Analysis (MIL-STD-882C Task 204) and updates to the previous analyses as necessary.

SYSTEM HAZARD ANALYSIS REPORT (SHAR)

Description/Purpose

1. One System Hazard Analysis (SHA) shall be created to:

a. verify system compliance with safety requirements contained in system specifications, statements of work, and other applicable documents;

b. identify previously unidentified hazards associated with the sub-system interfaces and system functional faults, providing descriptions of hazards, failure modes and effects, assessment of the level of risk, assessment of mitigation actions, and assessment and documentation of sub-system criticalities;

c. assess the risk associated with the total system design, integration, operation, maintenance and disposal, including hardware, software and human factors, and specifically of the sub-system interfaces by examining proposed weapon system architecture and to determine how failures can cause the failure conditions/hazards identified;

d. recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels, in accordance with the SSPP; and

e. document the individual hazard analysis activities carried out on the system and sub-systems as part of the overall SSP.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-STD-882C Task 205, ‘System Hazard Analysis’.

b. DI-SAFT-80101B, ‘System Safety Hazard Analysis Report’.

Content

3. The content of the SHAR shall comply with the requirements specified in MIL-STD-882C Task 205 and DI-SAFT-80101B, and integrate hardware, software and human factor aspects of the SSP into the report. The report shall also include, but not be limited to, analysis of hazards from the following potential sources:

a. isolation of energy sources,

b. fuels and propellents,

c. system environmental constraints,

d. external environmental impact,

e. explosive devices,

f. compatibility of materials,

g. electromagnetic environmental effects,

h. pressure vessels,

i. crash safety,

j. operation and maintenance hazards,

k. training hazards,

l. egress, rescue and survival hazards,

m. life support requirements,

n. fire ignition and propagation,

o. shock/damage resistance,

p. equipment layout and lighting,

q. fail safe design,

r. vulnerability and survivability,

s. protective clothing, equipment or devices, and

t. direct and indirect lightning effects.

4. The SHAR shall also:

a. verify the weapon system design meets all qualitative and quantitative safety requirements;

b. document all hazards and their probabilities and severities for that system.

5. The SHARs shall include Fault Tree Analyses to identify causal factors, and shall extend at least to the point where there are no single point failures leading to the top level event and at least two independent actions must be undertaken to reach the top level event. All mitigating actions shall be identified within the SHARs, and shall be easily traceable and identifiable on the Fault Trees.

6. In each ECP subsequent to contract signature the Contractor shall propose the generation or update of SHARs.

7. ***Initial (Draft) Delivery in Support of Detailed Design Review (DDR).*** The SHAR delivered to support the DDR shall contain the results of the system Preliminary Hazard Analysis (MIL-STD-882C Task 202), the system Safety Requirements/Criteria Analysis (MIL-STD-882C Task 203), Subsystem Hazard Analysis (MIL-STD-882C Task 204) for each sub-system, and the initial results of the System Hazard Analysis (MIL-STD-882C Task 205) for the entire system. It shall include definition of the failure condition criticality for each sub-system, and design requirements that are to be satisfied for each sub-system. Failure severity classifications shall be Catastrophic, Critical, Marginal and Negligible. A sub-system's severity classification shall be at least as severe as its most severe hazard.

8. ***Delivery in Support of Test Readiness Review (TRR).*** The SHAR delivered to support the TRR (ground test or flight test, or both) shall contain the final results of the System Hazard Analysis (MIL-STD-882C Task 205) and the results of the Operating and Support Hazard Analysis (MIL-STD-882C Task 206) for the system. Any required updates to the previous analysis should also be included.

CDRL-4 PROJECT AIRCRAFT TEST AND EVALUATION HAZARD ANALYSIS REPORT

Description/Purpose

1. The purpose of the Test and Evaluation Hazard Analysis Report is to:

a. ensure that for ground and flight test and evaluation, safety is considered (and safety responsibility assigned);

b. produce a Test and Evaluation Risk Matrix (TERM) to base hazard acceptance decisions on for training, experience, operational and maintenance risks;

c. to summarise existing analysis reports, open design hazards which could affect testing, and other safety data; and

d. to respond to all safety requirements of the System Specification and Statement of Work necessary for testing in-house, at other contractor facilities, and at Government-specified locations, bases, ranges, centres, and laboratories.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-STD-882C Task 302, ‘Test and Evaluation Safety’.

Content

3. The content of the Test and Evaluation Hazard Analysis Report shall comply with the requirements specified in MIL-STD-882 Task 302, and integrate hardware, software and human factor aspects of the System Safety Program into the report. The Test and Evaluation Hazard Analysis Report shall also describe how all safety requirements of the System Specification and Statement of Work necessary for testing in-house, at other contractor facilities, and at Government-specified locations, bases, ranges, centres, and laboratories, have been satisfied.

4. ***Delivery in Support of Test readiness Review (TRR).*** For both the Ground Test Readiness Review (GTRR) and Flight Test Readiness Review (FTRR), the Test and Evaluation Hazard Analysis Report delivered shall contain relevant results of other System Safety Program hazard analyses which could affect testing, ensuring coverage of relevant hardware, software and human factors’ hazards considered in design, integration, operation, maintenance and disposal of the system.

5. Expected test procedures will also be analysed from the training, experience, operational and maintenance risk perspective and mitigated appropriately. Failure severity classifications shall be Catastrophic, Critical/Hazardous, Marginal/Major and Negligible/Minor. All hazards identified from the training, experience, operational and maintenance risk perspectives will be accepted by the Commonwealth in accordance with the Test and Evaluation Risk Matrix (TERM) developed for the program.

Blank Page

CDRL-5 HAZARD LOG

Description/Purpose

1. The Hazard Log provides a closed loop hazard tracking system or database of all identified hazards. The Hazard Log shall be produced and maintained by the Contractor and the Commonwealth shall have the ability to remotely view and add, but not delete, information therein. At a minimum, the Hazard Log shall be electronic and easily sharable between computers at remote sites, without the need of specific proprietary tools.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-STD-882C, Task 106 'Hazard Tracking and Risk Resolution'.

b. DI-SAFT-80105B, 'System Safety Progress Report'.

Content

3. The Hazard Log shall comply with the requirements of MIL-STD-882C Task 106 and DI-SAFT-80105B, and contain as a minimum:

a. description of each hazard;

b. person(s) responsible for hazard closure and their organisational element;

c. associated pre-mitigation Hazard Risk Index (HRI);

d. proposed hazard mitigators to reduce it to an acceptable level;

e. post-mitigation HRI(s), for both short-term and long-term fixes to the hazard (if applicable);

f. traceability and status of resolution of each hazard mitigating action;

g. identification of residual HRI when all mitigating actions have been incorporated;

h. signatures of personnel authorised to accept residual risk, in accordance with the SSPP HRI Matrix, thus effecting closure of the Hazard Log item; and

i. status of each hazard and expected closure date if open or in-work.

4. At the completion of the contract, a fully updated final copy of the Hazard Log will be delivered to the Commonwealth.

Blank Page

CDRL-6 ECP SYSTEM SAFETY REPORT (ECPSSR)

Description/Purpose

1. This CDRL shall provide the mechanism for the safety review/analysis of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, Requests for Deviation/Waiver, Problem Reports, System Trouble Reports and Trade Studies where safety is impacted or could be affected. Where not impacted or affected, these documents shall record the justification.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-STD-882C, Task 303 'Safety Review Of Engineering Change Proposals, Specification Change Notices, Software Problem Reports And Requests For Deviation/Waiver'.

b. DI-SAFT-80103B, 'ECPSSR'.

c. DI-SAFT-80104B, 'Waiver or Deviation System Safety Report (WDSSR)'.

Content

3. The content of the ECPSSR or WDSSR shall comply with the requirements specified in Task 303 of MIL-STD-882C, and DI-SAFT-80103B or DI-SAFT-80104B, respectively, and integrate hardware, software and human factor aspects of the System Safety Program into the report. The report shall also include, but not be limited to, analysis of the following potential hazards:

a. isolation of energy sources,

b. fuels and propellents,

c. system environmental constraints,

d. external environmental impact,

e. explosive devices,

f. compatibility of materials,

g. electromagnetic environmental effects,

h. pressure vessels,

i. crash safety,

j. operation and maintenance hazards,

k. training hazards,

l. egress, rescue and survival hazards,

m. life support requirements,

n. fire ignition and propagation,

o. shock/damage resistance,

p. equipment layout and lighting,

q. fail safe design,

r. vulnerability and survivability,

s. protective clothing, equipment or devices, and

t. direct and indirect lightning effects.

4. For an ECPSSR, it shall also document the effect of this separate analysis on the updating of existing aircraft, system and sub-system analyses and assessments, providing recommendations for their subsequent immediate or delayed update. If the updates of existing system and sub-system analyses and assessments to reflect the ECPSSR are to be delayed, the ECPSSR shall also document how the Contractor change management system shall ensure that the their update is not forgotten.

5. For a WDSSR, it shall also document the aggregate safety effect of all active Deviations and Waivers and provide recommendations for any aggregate risks classified higher than acceptable by the SSPP.

CDRL-7 SAFETY VERIFICATION REPORT

Description/Purpose

1. This CDRL documents the actual tests, demonstrations, simulations, inspections or analyses required to verify safety requirements (direct and derived) for hardware, software, human factors and procedures.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-STD-882C, Task 401 ‘Safety Verification’.

b. DI-SAFT-80102B, ‘Safety Assessment Report’.

Content

3. The content of the Safety Verification Report shall comply with the requirements specified in Task 401 of MIL-STD-882C and DI-SAFT-80102B, and integrate hardware, software and human factor aspects of the System Safety Program into the report.

4. Mitigation requirements for all Catastrophic and Critical hazards shall be included.

5. Results of safety requirement verification activities shall be included within existing program test reports.

Blank Page

CDRL-8 SAFETY CASE REPORT (SCR)

Description/Purpose

1. The purpose of this report shall be to identify and verify compliance of the product with all direct and derived safety requirements (ie from the Statement of Work and Specification) to ensure a safe system from the perspective of design, integration, operation, maintenance and disposal, for hardware, software and human factor hazard considerations. The report shall comprehensively evaluate the residual safety risk being assumed by the Commonwealth prior to initial testing (initial Safety Case Report) or prior to Design Acceptance for the system (final Safety Case Report).

2. The SCR shall provide a reasoned summary argument, supported by referenced evidence, which justifies that the system is safe and fit for purpose. The SCR is raised in support of the overall Certification Basis Description and forms part of the certification basis for the aircraft or modification. The SCR shall contain summaries of all safety assessments and analyses conducted during the program, and a summary of the operating limitations of the system.

3. To achieve these above aims the SCR shall include, but not be limited to, the following:

a. Discussions on all activities undertaken to satisfy the goals of the SSP.

b. A summary of all the artefacts that prove that systematic analysis and reporting methods were used to maximise the probability of identifying risks for the *aircraft system*, and then tracking, mitigating and accepting them adequately in accordance with the SSPP.

c. Discussion on the acceptance of residual risk for any open safety issues, and their individual recommendations and closure plans.

d. A declaration of the safety of the system and its fitness for its intended purpose.

Preparation Instructions

4. The following documents are referenced herein:

a. MIL–STD–882C, Task 402 ‘Safety Compliance Assessment’.

b. MIL–STD–882C, Task 301 ‘Safety Assessment’.

c. DI–SAFT–80102B, ‘Safety Assessment Report’.

Content

5. The SCR shall document the results of the safety compliance activities undertaken in accordance with the MIL-STD-882C Task 402, Task 301, and DI–SAFT–80102B.

6. The SCR shall also:

a. summarise the status of the SSP against what was envisaged in the SSPP, including the hardware, software and human factors’ system safety strategies;

b. summarise the results of the system integration Human Factors Workload Assessment (or if not required, justify why not);

c. summarise the certification basis of any previous System Safety Program for a modified system.

d. identify the Certification Basis Description requirements that are proposed to be satisfied by its delivery;

e. a technical description of the functional and physical elements of the system including interfaces;

f. a summary of, and reference to, all program hazard analyses and assessment reports, describing aircraft or modification residual risk;

g. a summary listing of all Catastrophic and Critical/Hazardous hazards that exist, that have not been accepted in accordance with the SSPP HRI matrix;

h. a summary listing of all open hazards which are undesirable for the scope of flying operations expected;

i. a summary of all testing activities used to verify safety requirements;

j. results of human engineering verification activities applied to ensure human causal factors have been appropriately mitigated both during design and system integration;

k. a summary of all operating limitations that are applicable to the final system configuration;

l. a signed statement by the contractor's System Safety Manager saying that:

(1) the product has been analysed for hazards in the design, integration, operation, maintenance and disposal phases;

(2) all identified hazards have been analysed for hardware, software and human causal factors and have been eliminated or controlled in accordance with the SSPP; and

(3) that the system is ready to be tested or released to service, as required.

m. Provide closure and acceptance recommendations for the Commonwealth for any hazards where residual risk is above 'acceptable by contractor'.

n. summarise SSP achievements, analyses and assessments conducted, System Safety residual risks with a HRI greater than 'Acceptable', and recommendations for the Commonwealth acceptance of these risks.

Issuance of Special Flight Permits

7. To support the issuance of a Special Flight Permit (SFP), the following *System Safety* requirements should be satisfied:

a. All *hazards* of the top two severities to be appropriately mitigated or closed, and accepted as such by the relevant technical and operational airworthiness authorities.

b. Progress to be shown on the mitigation and closure of the remaining *hazards*.

c. For all 'Open' *hazards*, to consider whether any worst case credible scenario possible under SFP limitations may combine to affect continued safe flight and landing.

d. An initial *Safety Case Report* be submitted with the SFP application, to include:

(1) the status of the acquisition and modification project, with respect to the system integration and testing;

(2) the degree of SSP compliance against the SSPP and contractual requirements;

(3) the current Hazard Log;

(4) the level of risk associated with the anticipated flight test and subsequent additional operations, clearly documented (typically a Flight Test Hazard Analysis);

(5) a summary of what aspects of *System Safety* have not yet been addressed, or sufficiently mitigated by the SSP;

(6) a justification for the safety of the scope of flying to be conducted under the SFP; and

(7) a signed statement by the project integrator's Senior Design Engineer, describing the conditions, mitigations and limitations under which the aircraft is safe to fly, consistent with the SSP objectives, within the scope of the SFP.

Blank Page

SAFETY CASE REPORT (SCR) OUTLINE

1. The following outline is provided as an example of a typical SCR, and how it justifies an adequately safe weapon system.

2. The end aim for the SCR is to provide a well-reasoned summary document listing the activities undertaken to satisfy the goals of the SSP, and the artefacts that prove that your SSP maximised the probability of identifying, tracking, mitigating and accepting all risks for your weapon system.

Safety Case Report	
SC.1	**Introduction**
SC.1.1	Describe the weapon system
SC.2	**Overview**
SC.2.1	Describe Objectives of the SCR
SC.2.2	Outline the SCR
SC.2.3	Summarise the assessment of the safety achievements against the System Safety goals of the program
SC.3	**System Description**
SC.3.1	Describe system's purpose and intended use
SC.3.2	Provide a historical summary of weapon system development
SC.3.3	Provide a detailed description of weapon system components
SC.3.4	Identify any changes in CRE between previously certified systems and new systems
SC.4	**System Operation**
SC.4.1	Describe operational, testing and maintenance activities which may be hazardous to system or personnel
SC.4.2	Describe essential safety features for operations, test and maintenance
SC.4.3	Describe anticipated operational environment throughout entire life cycle from design to disposal
SC.4.4	Describe special support facilities or equipment
SC.5	**System Safety Engineering**
SC.5.1	Summarise safety criteria/methodologies used to classify hazards
SC.5.2	Describe how all hazards were analysed from a hardware, software and human causal factors perspective, and how the SSP maximised the possibility of identifying all potential hazards from system design, integration, operation, maintenance and disposal.
SC.5.3	Describe and list the analyses and tests performed to identify, evaluate and verify hazards and hazardous materials' mitigation to adequate levels
SC.5.4	Review significant hazards: hazards of the Catastrophic and Critical/Hazardous severities, and all other hazards with a residual risk greater than 'Acceptable'
SC.5.5	Justify the safety of the weapon system with respect to all identified hazards, new systems, legacy systems and interfaces between systems
SC.6	**Conclusions/Recommendations**
SC.6.1	Assess results of safety program justifying the safety of the system with respect to the residual risk, making a subjective overall residual risk assessment
SC.6.2	Provide recommendations for all hazards with a residual risk greater than 'Acceptable'
SC.6.3	Sign a confirmation that all identified hazards have been controlled sufficiently, and that system is adequately safe to operate
SC.7	**Appendices**
SC.7.1	As required

Blank Page

CDRL-9 AIRCRAFT-LEVEL FUNCTIONAL HAZARD ASSESSMENT (AFHA) AND SYSTEM-LEVEL FUNCTIONAL HAZARD ASSESSMENT (SFHA)

AIRCRAFT-LEVEL FUNCTIONAL HAZARD ASSESSMENT (AFHA)

Description/Purpose

1. A Functional Hazard Assessment is defined as a systematic, comprehensive qualitative examination of functions to identify and classify failure conditions of those functions according to severity. A FHA is usually performed at two levels. The Aircraft-level FHA is a high level, qualitative assessment of the basic functions of the aircraft as defined at the beginning of aircraft development. An AFHA should identify and classify the failure conditions associated with the aircraft-level functions. The classification of these failure conditions establishes some of the safety requirements that an aircraft must meet. The goal of conducting the AFHA is to clearly identify each failure condition along with the rationale for its severity classification. The output of both the AFHA and SFHA is the starting point for the generation and allocation of direct and derived safety requirements.

Preparation Instructions

2. The following documents are referenced herein:

a. SAE ARP 4761.

b. Joint Software System Safety Committee Software System Safety Handbook.

Content

3. The content of the AFHA shall integrate hardware, software and human factor aspects of the System Safety Program into the assessment, and comply with:

a. the requirements specified in SAE ARP 4761, and

b. guidance in the Software System Safety Handbook.

4. The report shall include definition of the failure condition criticality and design requirements that are to be satisfied for each function. Failure severity classifications shall be Catastrophic, Hazardous, Major and Minor.

5. Because the AFHA is an analysis of the aircraft functions at the highest level, most of these functions will be the same for most aircraft types, and may include:

a. providing attitude control,

b. providing ground directional control,

c. providing adequate lift,

d. providing adequate thrust,

e. providing flight critical information (which includes fault monitoring),

f. providing fire and explosion protection,

g. maintaining a habitable environment,

h. maintaining a safe external environment on the ground,

i. providing adequate crash survivability,

j. maintaining structural integrity,

k. providing adequate stowage of cargo,

l. providing adequate range (which includes in-flight refuelling),

m. providing for a safe landing,

n. providing adequate self-defence mechanisms, and

o. providing adequate offensive mechanisms.

6. The functional failures determined to be applicable to the *aircraft system* shall be analysed in terms of announced failures and unannounced failures for the following cases:

a. failure to provide the function when required,

b. provision of the function when not required, and

c. incorrect provision of the function.

7. Each subsequent ECP to the contract shall propose an update to the AFHA if the ECP proposes modifications that affect the AFHA.

SYSTEM-LEVEL FUNCTIONAL HAZARD ASSESSMENT (SFHA)

Description/Purpose

1. The System-level FHA is a qualitative assessment which is iterative in nature and becomes more defined as the system design evolves. It considers a failure or combination of system failures that affect an aircraft function. Assessment of any particular hardware, software or human factor issue is not the goal of the SFHA. However, if separate systems use similar architectures or identical complex components and introduce additional system level failure conditions involving integrated multiple functions, then the FHA should be modified to identify and classify these new failure conditions. After aircraft functions have been allocated to systems by the design process, each system should be re-examined using the SFHA process. The output of both the AFHA and SFHA is the starting point for the generation and allocation of direct and derived safety requirements.

2. The AFHA is one of the inputs to the SFHA, proving the list of functions and failures to be considered.

Preparation Instructions

3. The following documents are referenced herein:

a. SAE ARP 4761.

b. Joint Software System Safety Committee Software System Safety Handbook.

Content

4. The content of the SFHA shall integrate hardware, software and human factor aspects of the System Safety Program into the assessment, and comply with:

a. the requirements specified in SAE ARP 4761, and

b. guidance in the Software System Safety Handbook.

5. The functional failures determined to be applicable to the *aircraft system* shall be analysed in terms of announced failures and unannounced failures for the following cases:

a. failure to provide the function when required,

b. provision of the function when not required, and

c. incorrect provision of the function.

6. The report shall include definition of the failure condition criticality and design requirements that are to be satisfied for each function. Failure severity classifications shall be Catastrophic, Hazardous, Major and Minor. A system's severity classification shall be at least as severe as its most severe hazard.

7. The SFHA shall establish the hardware criticality and software developmental assurance levels of the system.

8. In each ECP proposed subsequent to contract signature, the Contractor shall propose the amendment of SFHAs already generated.

Blank Page

CDRL-10 PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA) AND SYSTEM SAFETY ASSESSMENT (SSA)

PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA)

Description/Purpose

1. The PSSA process is a systematic examination of proposed system architectures (for each system) to determine how failures can lead to the functional hazards identified by the System-level Functional Hazard Analysis (SFHA), and how the SFHA requirements can be met.

2. While the PSSA process is iterative with design, and the PSSA develops into the System Safety Analysis (SSA), once the design is fixed, unless significant changes to the design are undertaken, only the SSAs are updated. The decision to conduct a PSSA is dependent upon the design architecture, complexity, severity and consequence of the failure conditions, and type of functions performed by the system. The difference between the PSSA and the SSA is that the PSSA is a method to evaluate proposed architectures and derive system safety requirements for each; whereas the SSA is a verification that the implemented design meets both the qualitative and quatitative safety requirements defined in the AFHA, SFHA and PSSA.

3. The PSSA is a top-down approach and used to complete the failure conditions list and the corresponding safety requirements. It is also used to demonstrate how the system will meet the qualitative and quantitative requirements for the various hazards identified. The PSSA process identifies mitigation strategies, taking into account fail safe concepts and architectural attributes which may be needed to meet the safety objectives of the system and aircraft. It should identify and capture all derived system safety requirements. The PSSA outputs should be used as inputs to the SSA and other documents, including, but not limited to, system requirements, hardware requirements and software requirements.

4. The PSSA has two main inputs: the System-level Functional Hazard Analysis (SFHA) and the aircraft Fault Tree Analysis.

Preparation Instructions

5. The following documents are referenced herein:

a. SAE ARP 4761, and

b. Joint Software System Safety Committee Software System Safety Handbook.

Content

6. The content of the PSSA shall integrate hardware, software and human factor aspects of the System Safety Program into the assessment, and comply with:

a. the requirements specified in SAE ARP 4761, and

b. guidance in the Software System Safety Handbook.

7. The report shall include definition of the failure condition criticality and design requirements that are to be satisfied for each function and shall be structured to retain traceability. Failure severity classifications shall be Catastrophic, Hazardous, Major and Minor.

8. In each ECP proposed subsequent to contract signature, the ECPSSR shall propose the amendment of PSSAs already generated.

SYSTEM SAFETY ASSESSMENT (SSA)

Description/Purpose

1. The SSA is a systematic, comprehensive evaluation of the implemented system to show that relevant safety requirements are met. The analysis process is similar to the activities of the PSSA, but different in scope. The difference between the PSSA and the SSA is that the PSSA is a method to evaluate proposed architectures and derive system safety requirements for each; whereas the SSA is a verification that the implemented design meets both the qualitative and quatitative safety requirements defined in the AFHA, SFHA and PSSA.

2. The SSA integrates the results of the various analyses to verify the safety of the overall system. It is a bottom-up approach for verifying that design safety requirements and objectives have been met.

Preparation Instructions

3. The following documents are referenced herein:

a. SAE ARP 4761, and

b. Joint Software System Safety Committee Software System Safety Handbook.

Content

4. The content of the SSA shall integrate hardware, software and human factor aspects of the System Safety Program into the assessment, and comply with:

a. the requirements specified in SAE ARP 4761, and

b. guidance in the Software System Safety Handbook.

5. The report shall include definition of the failure condition criticality and design requirements that are to be satisfied for each function and shall be structured to retain traceability. Failure severity classifications shall be Catastrophic, Hazardous, Major and Minor.

6. The SSAs shall document all hazards for that system, but discuss in detail at least system Catastrophic and Hazardous hazards. Major hazards shall be discussed in detail if in a particular combination these hazards could cause a Catastrophic or Hazardous condition or if the Major hazard is complex in nature or function.

7. In each ECP subsequent to contract signature the ECPSSR shall propose the generation or update of SSAs.

8. The SSA’s Fault Tree Analysis shall identify hardware, software and human causal factors, and shall extend at least to the point where there are no single point failures leading to the top level event and at least two independent actions must be undertaken to reach the top level event. All mitigating actions shall be identified within the SSAs, and shall be easily traceable and identifiable on the Fault Trees.

9. The SSAs shall also include verification that the hardware, software and human factors’ safety requirements are traceable from their origin through to implemented design.

10. FMECA and FMEA results shall also be incorporated into the SSA for all Catastrophic and Hazardous hazards, and for Major hazards only as required.

CDRL-11 COMMON CAUSE ANALYSIS (CCA)

Description/Purpose

1. A degree of independence between functions, systems or items will be required to satisfy safety requirements. CCA provides the verification of this independence. CCA identifies individual failure modes or external events which can lead to a Catastrophic or Hazardous/Critical failure condition and provides appropriate mitigation.

2. CCA is subdivided into three separate sub-analyses:

a. Zonal Safety Analysis (ZSA). A ZSA is performed in every zone of the aircraft. Its objective is to ensure that equipment meets safety requirements with respect to:

(1) *Basic Installation.* That basic installation is checked against appropriate design and installation requirements.

(2) *Interference Between Systems*. The effects of failures of equipment should be considered with respect to their impact on other systems and structures falling within their physical sphere of influence.

(3) *Maintenance Errors.* Installation and maintenance errors and their effects on the system and aircraft should be considered.

b. Particular Risk Analysis (PRA). Particular risks are defined as those events or influences which are outside the system(s) and item(s) concerned, but which may violate failure independence claims. Each should be examined to determine the simultaneous or cascading effects of each risk. Typical risks include, but are not limited to:

(1) fire;

(2) high energy device separation;

(3) leaking fluids;

(4) hail, ice and snow;

(5) bird strike;

(6) tire tread separation;

(7) wheel rim release;

(8) lightning;

(9) high intensity radiated fields; and

(10) flailing shafts.

c. Common Mode Analysis (CMA). A CMA verifies that ANDed events in Fault Tree Analyses or Dependence Diagrams and Markov Analyses are independent in the actual implementation. The effects of design, manufacturing, maintenance errors and failures of system components which defeat their independence need to be analysed. Consideration should be given to the independence of functions and their respective monitors. Items with identical hardware and/or software could be susceptible to generic faults which could cause malfunctions in multiple items. Typical Common Mode faults include, but are not limited to:

(1) hardware error and failure;

(2) software error;

(3) production and repair flaws;

(4) situation dependent stress (eg abnormal flight conditions or abnormal system configurations);

(5) installation error;

(6) requirements error;

(7) environmental factors;

(8) cascading faults; and

(9) common external source faults.

Preparation Instructions

3. The following documents are referenced herein:

a. SAE ARP 4761.

b. Joint Software System Safety Committee Software System Safety Handbook.

Content

4. The content of the CCA shall integrate hardware, software and human factor aspects of the System Safety Program into the assessment, and comply with:

a. the requirements specified in SAE ARP 4761, and

b. guidance in the Software System Safety Handbook.

5. The report shall include definition of the failure condition criticality and design requirements that are to be satisfied for each function and shall be structured to retain traceability. Failure severity classifications shall be Catastrophic, Hazardous/Critical, Major/Marginal and Minor/Negligible.

6. As much as possible, the CCA shall be included as a sub-part of other analysis or assessment reports.

CDRL-12 HEALTH HAZARD ASSESSMENT REPORT

NOTE

CDRL may not be required if an OH&S report is also required.

Description/Purpose

1. This CDRL documents a Health Hazard Assessment (HHA) to identify health hazards, evaluate proposed hazardous materials, and propose protective measures to reduce the associated hazard risks to an acceptable level.

2. Should weapon system design solutions or subsequent ECPs incorporate hazardous material, as defined by xxxx, the Contractor shall perform a HHA to identify and determine quantities of the potentially hazardous materials or physical agents. The HHA shall also analyse how these materials and physical agents are used in the system and for its logistical support, and provide a description as to why alternative non-hazardous materials are not suitable.

Preparation Instructions

3. The following documents are referenced herein:

a. MIL-STD-882C, Task 207 ‘Health Hazard Assessment’.

b. DI-SAFT-80106B, ‘Health Hazard Assessment Report’.

Content

4. The content of the Health Hazard Assessment Report shall comply with the requirements specified in Task 207 of MIL-STD-882C and DI-SAFT-80106B, and integrate hardware, software and human factor aspects of the System Safety Program into the report.

Blank Page

CDRL-13 OPERATING AND SUPPORT HAZARD ANALYSIS REPORT

Description/Purpose

1. This CDRL documents an Operating and Support Hazard Analysis (O&SHA), to evaluate activities for hazards or risks introduced into the system by operational and support procedures and to evaluate adequacy of operational and support procedures used to eliminate, control, or abate other identified hazards or risks.

2. The O&SHA shall examine and mitigate proposed weapon system operating and maintenance issues which could contribute to failure conditions and/or hazards identified in other analyses. In each ECP proposed subsequent to contract signature, the Contractor shall propose the amendment of any O&SHA already generated.

Preparation Instructions

3. The following documents are referenced herein:

a. MIL-STD-882C, Task 206 ‘Operating and Support Hazard Analysis’.

b. DI-SAFT-80101B, ‘System Safety Hazard Analysis Report’.

Content

4. The content of the Operating and Support Hazard Analysis Report shall comply with the requirements specified in Task 206 of MIL-STD-882C and DI-SAFT-80101B, and integrate hardware, software and human factor aspects of the System Safety Program into the report.

Blank Page

CDRL-14 SAFETY REQUIREMENTS/CRITERIA ANALYSIS

Description/Purpose

1. This CDRL documents the safety design requirements and design criteria for a system under development.

2. The Safety Requirements/Criteria Analysis (SR/CA) relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level. The SR/CA uses the Preliminary Hazard List (Task 201) or the Preliminary Hazard Analysis (Task 202) as a basis, if available. The SRCA is also used to incorporate design requirements that are safety related but not tied to a specific hazard. In each ECP proposed subsequent to contract signature, the Contractor shall propose the amendment of any SR/CA already generated.

Preparation Instructions

3. The following documents are referenced herein:

a. MIL-STD-882C, Task 203 ‘Safety requirements/Criteria Analysis.

b. DI-SAFT-80101B, ‘System Safety Hazard Analysis Report’.

Content

4. The content of the SR/CA Report shall comply with the requirements specified in Task 203 of MIL-STD-882C and DI-SAFT-80101B, and integrate hardware, software and human factor aspects of the System Safety Program into the report.

Blank Page

CDRL-15 PRELIMINARY HAZARD ANALYSIS

Description/Purpose

1. This CDRL documents safety critical areas, providing an initial assessment of hazards, and the identification of requisite hazard controls and follow-on actions.

2. The Preliminary Hazard Analysis (PHA) provides an initial risk assessment of a concept or system. Based on the best available data, including incident and accident data (if applicable) from similar systems and other lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to acceptable levels shall be included. In each ECP proposed subsequent to contract signature, the Contractor shall propose the amendment of any PHA already generated.

Preparation Instructions

3. The following documents are referenced herein:

a. MIL-STD-882C, Task 202 ‘Preliminary Hazard Analysis’.

b. DI-SAFT-80101B, ‘System Safety Hazard Analysis Report’.

Content

4. The content of the PHA Report shall comply with the requirements specified in Task 202 of MIL-STD-882C and DI-SAFT--80101B, and integrate hardware, software and human factor aspects of the System Safety Program into the report.

Blank Page

MIL-STD-882 BASED SYSTEM SAFETY PROGRAM WEAPON SYSTEM SPECIFICATION

1. The following System Safety requirements should be considered for inclusion in the Project Specification. Early consultation with SCI-DGTA is crucial for the establishment of an SSP which is tailored to be commensurate to the scope of work expected.

2. Any standards called out below are TAR-preferred standards only, and therefore alternative standards can be proposed to fulfil the same requirements. The onus is on the Contractor to show equivalence.

3. The final set of clauses used for the Specification and Statement of Work will form part of the aircraft's airworthiness certification basis.

SYSTEM SAFETY PROGRAM

The *[Project Name]* shall establish a System Safety Program that complies with MIL-STD-882C to prove acceptably safe operation for the intended roles, configurations and operating environments of the ADF. The System Safety Program scope and acceptable safety levels shall be as defined in the *[Project Name]* Statement of Work. Alternate standards and requirements that provide an equivalent level of safety for the ADF intended roles, configurations and operating environments can be proposed, but the onus shall be on the contractor to prove equivalence.

NOTE

Commonwealth recognition of previous System Safety work may be based on acceptance by another government-based Airworthiness Authority, provided the basis of acceptance is relevant to the ADF's intended roles, configuration and operating environments. System Safety work that has not been accepted by another government-based Airworthiness Authority shall be presented to the Commonwealth and shall meet either the System Safety requirements defined in this specification, or an alternate basis shown by the contractor and agreed by the Commonwealth to provide an equivalent level of safety and performance.

Blank Page

FAR/JAR BASED SYSTEM SAFETY PROGRAM WEAPON SYSTEM SPECIFICATION

1. The following System Safety requirements should be considered for inclusion in the Project Specification. Early consultation with SCI-DGTA is crucial for the establishment of an SSP which is tailored to be commensurate to the scope of work expected.

2. Any standards called out below are TAR-preferred standards only, and therefore alternative standards can be proposed to fulfil the same requirements. The onus is on the Contractor to show equivalence.

3. The final set of clauses used for the Specification and Statement of Work will form part of the aircraft's airworthiness certification basis.

SYSTEM SAFETY PROGRAM

The *[Project Name]* shall establish a System Safety Program that complies with the System Safety requirements of all applicable Federal Aviation Regulations (FARs) to prove acceptably safe operation for the intended roles, configurations and operating environments of the ADF. The System Safety Program scope and acceptable safety levels shall be as defined in the *[Project Name]* Statement of Work. Alternate standards and requirements that provide an equivalent level of safety for the ADF intended roles, configurations and operating environments can be proposed, but the onus shall be on the contractor to prove equivalence.

Where reference is made in this specification to Federal Airworthiness requirements, either generically or specifically (eg FAR 25), that reference shall also be deemed to invoke all other applicable Federal Aviation Administration Advisory Circulars, Notices, Orders and Technical Standard Orders.

NOTE

Commonwealth recognition of previous System Safety work may be based on acceptance by another government-based Airworthiness Authority, provided the basis of acceptance is relevant to the ADF's intended roles, configuration and operating environments. System Safety work that has not been accepted by another government-based Airworthiness Authority shall be presented to the Commonwealth and shall meet either the System Safety requirements defined in this specification, or an alternate basis shown by the contractor and agreed by the Commonwealth to provide an equivalent level of safety and performance.

Blank Page

IN-SERVICE SYSTEM SAFETY PROGRAM (ISSSP) GUIDANCE

1. The following guidance is provided for the establishment and sustainment of In-Service System Safety Programs (ISSSPs) for legacy weapon systems that may or may not have had SSP requirements during original development, or where their original SSP documentation has not kept pace with aircraft configuration updates.

2. The principles of a SSP espoused in the main body of this Chapter are equally applicable to legacy weapon systems, although their application needs to be tailored to be commensurate to the scope of design changes and assessments undertaken at the SPO.

ISSSP TERMS OF REFERENCE

3. The overarching Terms Of Reference (TOR) for any ISSSP should be:

a. to value add,

b. to maximise use of the existing SPO Engineering Management System (EMS) and procedures,

c. to optimise use of existing System Safety related data, and

d. to minimise the impact on SPO resources.

THE ISSSP

ISSSP Scope

4. As a minimum, the scope of ISSSPs includes:

a. the generation of an ISSSP Plan (ISSSPP) to detail the value-added system safety methodologies to be applied to all SPO technical activities;

b. reliability monitoring of safety critical systems/items;

c. undertaking hazard analysis of weapon system design changes and assessments commensurate to risk, and accepting identified risks within a formal framework; and

d. presenting results of key System Safety activities to the annual Airworthiness Board (AwB).

ISSSPP Content

5. ISSSPP considerations should mirror applicable content of project SSPPs described in earlier Annexes of this Chapter. ISSSP methodologies should be tailored to ensure coverage of hardware, software and human factors' considerations by all SPO sections involved in design or design assessments. An example ISSSPP is provided at appendix 1.

6. Additional considerations for ISSSPP content include:

a. outlining all ISSSP activities and their timing, and

b. the definition of the exact documents which constitute the System Safety Document Baseline (SDBL) for the aircraft system.

ISSSP Execution

7. In executing the ISSSP and establishing the optimum effort required, the following guidance is provided:

a. The implementation of the ISSSP through the existing SPO EMS processes (such as EMERALD) is likely to be least time consuming. Typically many ISSSP requirements are already being considered

and/or reported by the EMS, but are not recognised as such. Where required, a slight modification of how specific data is presented will assist.

b. Typically SPOs already possess a Standing Instruction (SI) process and a SI on 'Judgement of Significance (JOS)'. A new ISSSPP SI complementing this and describing the extent of the ISSSP, the flexible ISSSP safety assessment processes, and HRI definition and use to assist with the JOS determinations would provide enough guidance for an effective ISSSP. This process can improve the efficiency of JOS determinations by reducing undue conservatism.

c. Document an assessment's or design change's tailored system safety approach only when 'significant'. The system safety approach would then describe the safety methodology, and residual risk acceptance criteria to be applied based on the HRI, and justify the type of hazard analyses to be completed.

d. Define the analysis techniques to be applied dependent on complexity and design change significance.

e. Generate tailored Safety Case Reports as part of the design acceptance rigour only for significant ECPs and projects.

f. Document design change or assessment hazards through a separate Hazard Log form on EMERALD. This will ensure its use during the extant EMS process and specifically document all hazards and their HRIs (pre and post-mitigation), to allow for data manipulation and tracking of individual mitigations. A standard Hazard Log data entry format would also assist in ensuring that all necessary considerations are applied to the change or assessment. A sample data entry format could be:

Unique Hazard Identifier:
Hazard Description:
Initial HRI:
Phase that Hazard is Identified for: [Design, Integration, Operation, Maintenance, Disposal]
Potential Contributory Causes to Hazard:
HARDWARE –
SOFTWARE –
HUMAN FACTORS –
Potential Mitigating Solutions (Short-term):
HARDWARE –
SOFTWARE –
HUMAN FACTORS –
Post Mitigation HRI (Short Term):
Potential Mitigating Solutions (Long-term):
HARDWARE –
SOFTWARE –
HUMAN FACTORS –
Post Mitigation HRI (Long Term):
Status of Mitigations:
HARDWARE –
SOFTWARE –
HUMAN FACTORS –

g. Create a Safety Critical Items/Systems (SCIS) List.

(1) A list of weapon system SCIS can be created from the Technical Maintenance Plan. Any of these SCIS that exhibit significant negative Mean Time Between Failure (MTBF) trending from the originally designed/predicted MTBF need to be assessed for risk and mitigated. Typically, differences considered significant would be of an order of magnitude or more, or an approximate 50% reduction, depending on the MTBF figure. Predicted MTBFs would have been used by the aircraft manufacturers to introduce an inherent level of safety in the design. This is the information they would have used to determine redundancies required and to justify sufficient risk mitigation for SCIS.

(2) Should originally designed/predicted MTBF data not be available, or item/system architecture changed significantly from original design, determining whether original design safety margins

are being retained is more difficult. However, platform flying hours and comparisons against previous years' in-service MTBF data will also assist in identifying negative trends and infer design safety levels, albeit with a lower level of confidence. For these cases, difference margins will need to be smaller, and the more years' worth of data is available, the better the long-term comparisons.

(3) AAP 7001.038-2 Section 3 Chapter 2 contains the definition of safety critical items. As an additional confidence check, a true SCIS is one whereby loss of the function provided by that item/system could, in a worst credible representative environment, directly (ie without additional events occurring) affect the aircraft's ability for continued safe flight and landing for its SOI. Most SCIS lists could therefore be expected to contain the following systems:

(a) powerplant,

(b) undercarriage,

(c) hydraulic system,

(d) navigation system,

(e) fuel system, and

(f) flight controls.

h. The appointment of a SPO System Safety Manager and deputy will ensure that workload is evenly distributed and no more demanding than a significant secondary duty. Typically, these individuals are senior SPO personnel, thus allowing them to provide as-required mentor services.

i. System Safety training provided both at ISSSP commencement and cyclically thereafter is crucial to program acceptance and viability. Training is most effective when tailored with an in-service focus, including topical SPO case studies.

j. Research the availability of existing System Safety Data for the weapon system's configuration. If this data exists it will significantly simplify the ISSSP through:

(1) an existing reference to qualitative or quantitative information on potential hazards already associated with specific systems or LRUs;

(2) already identifying a methodology for the analysis of specific systems or LRUs;

(3) the provision of existing interfaces to other systems; and

(4) the provision of a more holistic 'system' picture to assist with residual risk acceptance.

k. Determine the timing for a validation of the predicted MTBFs provided in the design phase of the *aircraft system*, as discussed in the body of this Chapter. Typically, validation of predicted MTBF can only occur when the original design is sufficiently robust and an adequate sample size exists (generally 4-7 years after introduction into service).

l. Establish close liaisons with the Force Element Group's operational Subject Matter Experts (SMEs) and Squadron and/or Wing Aviation Safety Officers (ASOs). Typically these individuals are capable of providing valuable insights and advice about technical options under consideration. ASOs are also typically trained in aviation risk management and crew resource management, and are therefore current with topical safety issues and HRI mitigation, albeit from an operational airworthiness perspective. This feedback can be provided through Configuration Control Boards (CCBs) and/or System Safety Working Groups, as necessary.

m. Establish an effective System Safety Working Group by generating a Charter and agreeing on how best to implement ISSSP goals. Discussions typically expected at SSWGs could be alternately embedded within design reviews and CCB agendas.

n. Include ISSSP checklists into design change/assessment processes to assist in the identification and consideration of both internal and external interfaces for hardware, software and human hazard causal factors during design, integration, operation, maintenance and disposal.

Appendix

1. Example In-Service System Safety Program Plan (SSPP) for XXSPO.

EXAMPLE IN-SERVICE SYSTEM SAFETY PROGRAM PLAN (SSPP) FOR XXSPO

SI (LOG) XX-XX

INTRODUCTION

1. This SI (LOG) xx-xx contains the System Safety Program Plan (SSPP) for the in-service xxxx weapon system. It presents an engineering risk management process to assess the type's level of safety and to provide assurance that it remains acceptable whilst the aircraft is in service. These goals are achieved by requiring:

a. reliability monitoring of safety-critical items/systems, and

b. undertaking hazard analyses of design assessments and design changes.

2. Inherent System Safety levels associated with the xxxx weapon system can be inferred by considering the reliability of its safety critical systems. By monitoring their failure rates, trends can be detected and mitigated in a timely manner.

3. Safety may however also be impacted by unusual circumstances or by proposed designs. Hazards with unacceptable risks may be inadvertently introduced. By undertaking hazard analyses commensurate to significance and accepting risk within a formal framework, a level of safety can be assured.

4. The following System Safety activities will directly support the technical airworthiness of the xxxx weapon system and hence a summary of key results is to be presented at the annual Airworthiness Board (AwB).

5. This SSPP fits within the broader engineering and logistics framework supporting the continued airworthiness of the in-service xxxx weapon system. Higher level guidance to this SSPP is provided by AAP 7001.054 Section 2 Chapter 1 'System Safety Engineering'.

AIM

6. The aim of this instruction is to define the System Safety Management and Engineering activities required to establish and maintain an acceptable level of safety for the in-service xxxx weapon system.

AUTHORITY

7. This instruction is issued under the authority of Officer Commanding XXSPO.

SCOPE

8. This SSPP applies to the in-service engineering activities relevant to the xxxx weapon system. It is the responsibility of the XXSPO CENGR to ensure that the intent of this plan is implemented within the organisation.

9. XXSPO is required to:

a. undertake reliability monitoring of safety-critical items/systems for significant negative trending;

b. undertake hazard analyses commensurate to significance for design assessments and changes to the xxxx weapon system, and accept identified risks within a formal framework; and

c. present key System Safety results to the xxxx annual AwB.

DEFINITIONS

10. Relevant definitions are provided in the attached Annex 'Application of System Safety Management and Engineering Activities to XXSPO'.

INSTRUCTION

11. XXSPO System Safety Engineer. The XXSPO System Safety Engineer (SSE) recognises the importance of System Safety, in particular the need to provide guidance and continuity to XXSPO personnel. OIC XXX is appointed as the XXSPO SSE. The responsibilities of this position include:

a. development of XXSPO System Safety policy and processes, and

b. providing training and guidance to staff on System Safety Engineering processes and methodologies.

12. Design Assessments or Changes. Hazard analyses commensurate to the inherent risk shall be undertaken for all design assessments or changes to the xxxx weapon system, in accordance with annex A to this SI. For the purposes of this SI, design assessments and changes include design proposals and evaluations, modifications, deviations, waivers, technical substitutions, publication amendments and Maintenance Interval Extension Requests. Hazard analyses are to account for the aircraft's operating environment or changes to that environment.

13. Design changes also include changes to the software or firmware of the xxxx weapon system. Additional guidance on the management of software changes is provided AAP 7001.054 Sect 2 Chap 7 'Software for Airborne and Related Systems'. Where software modifications to the xxxx weapon system are required, any Statements of Work shall adhere to the policy guidance outlined in the AAP 7001.054.

14. Hazards for significant design changes and assessments are to be recorded in a Hazard Log. The hazards shall be mitigated and accepted within the Hazard Risk Index (HRI) framework shown at annex A. Further, for significant ECPs, a Safety Case Report (SCR) shall be produced for the design change, capturing the results of the hazard analyses and justifying the overall safety of the design change.

15. Safety-Critical Items/Systems MTBF Evaluation. MTBF monitoring of safety-critical items/systems shall be undertaken for significant negative trending evaluation. These trends will be initially assessed for validity of data, and then for potential causal factors and mitigation.

16. Airworthiness Board Presentation. A key System Safety aspects presentation is to be made to the xxxx weapon system AwB. This presentation shall include:

a. an introduction (outlining the purpose of the ISSSP);

b. an overview of the ISSSP;

c. a summary of Hazard Logs for Significant design assessments and changes processed during the preceding year; and

d. safety-critical items/systems with significant negative trending and mitigations implemented.

17. System Safety Training. In order to fulfil the requirements of this SSPP, all XXSPO Design Engineers require formal System Safety training. The main training is provided by the System Safety courses sponsored by SCI-DGTA, including requested periodical continuation training. Additional System Safety techniques training is provided on an as-required basis. The requirement for all training is included in the XXSPO training database.

18. System Safety Process at XXSPO. Procedures for implementing this SSPP policy are documented in the attached annex 'Application of System Safety Management and Engineering Activities at XXSPO'.

APPLICATION OF SYSTEM SAFETY MANAGEMENT AND ENGINEERING ACTIVITIES AT XXSPO

INTRODUCTION

1. All xxxx weapon system design changes and assessments must be analysed for hazards. The role of System Safety is to provide a framework within which those hazards are identified, quantified and mitigated or accepted.

AIM

2. To detail the process of applying System Safety Management and Engineering concepts to the analysis and control of design assessments and changes at XXSPO.

SCOPE

3. This instruction applies to all design assessments and changes managed by XXSPO.

DEFINITIONS

4. **Hazard**. From MIL–STD–882C, ‘Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.’

5. **Hazard Risk Index (HRI)**. From MIL–STD–882C, ‘A program-specific numerical priority assigned to hazards, pre and post-mitigation, based on their risk level (combination of hazard severity and hazard probability). The acceptance of a hazards’ HRI is commensurately assigned to program and vendor management, dependent on risk’.

INSTRUCTION

6. The process flow chart at appendix 1 details design assessment and change processes, and their integration with System Safety, noting that only ECP design changes are required to go through CCBs and Safety Review Boards.

7. EMERALD is used for logging and controlling all hazards.

8. SAE ARP4761 (Guidelines & Methods for Performing the Safety Assessment Process on Civil Airborne Systems and Equipment) provides guidance on the conduct of System Safety activities required by this instruction.

9. **Preliminary Hazard Analysis (PHA).** The DE judging significance is required to compile a comprehensive list of hazards that are associated with the assessment or change. SAE ARP4761 Appendix A (FHA - Functional Hazard Assessment) provides the process required to develop a comprehensive list of hazards and associated safety requirements. For complex design changes, the use of Fault Tree Analysis to support the FHA is highly recommended (refer SAE ARP4761 Annex D).

10. When compiling the list of hazards, DEs are to consider:

a. changes in role, configuration and environment and departures from the certified baseline. Hazards associated with departures from the certified baseline should address:

(1) the aircraft’s legacy systems,

(2) new and modified systems,

(3) the interface between new and legacy systems, and

(4) complex system interactions.

b. modes of failure including reasonable human errors as well as single point and common mode failures;

c. contribution of hardware and software (including software developed by sub-contractors) events, faults and occurrences (such as improper timing) on the safety of the sub-system;

d. possible independent, dependent and simultaneous hazardous events including higher level system failures, failures of safety devices, common cause failures and events, and higher level system interactions that could create a hazard or result in an increased risk;

e. health hazards, including:

(1) chemical hazards;

(2) physical hazards;

(3) ergonomic hazards; or

(4) other hazardous materials that may be formed by the introduction of the system, or by the manufacture, test or operation of the system.

f. susceptibility to external events including:

(1) fire;

(2) humidity/moisture/water/seaspray/hail/ice/snow;

(3) lightning;

(4) dust;

(5) bird strike;

(6) tyre/wheel disintegration;

(7) leaking fluids;

(8) depressurisation; and

(9) crash landing/impact/shock/vibration.

11. Once all credible hardware, software and human factor hazards are identified for the design, integration, operation, maintenance and disposal of the design change or assessment, DEs are to assign a Hazard Risk Index (HRI) in accordance with appendix 2. For the purpose of the Judgement Of Significance (JOS), DEs will not necessarily be required to derive quantitative probabilities. Rather, the determination of probability shall be through a combination of experience and qualitative analysis of the system under examination.

12. On completion of the PHA, the significance of the design change is re-assessed. The DE judging significance is required to record a summary of the PHA results in the EMERALD ‘Judgement Of Significance’ comment field (including hazards with a HRI of 15-20). The record is to include hazard description, failure mode, severity and probability assessment and HRI. For extensive PHAs, a separate document may be created, linked to the EMERALD task and referenced in the JOS decision. For ECP’s, the PHA is presented at the PDR.

13. Where the highest HRI makes the design change significant, all hazards with a HRI of 10 or lower are to be entered on EMERALD as a Hazard Log Logistics Process. Any new hazards with a HRI of 10 or lower identified during further proceedings are also to be entered on EMERALD.

14. **System Safety Analysis Plan (SSAP).** For significant design changes or assessments, the DE is required to prepare a System Safety Analysis Plan (SSAP) which will form the basis for mitigating or accepting hazards, identifying and justifying the analyses to be conducted, and the verification methods required for the specific design

change or assessment. Appendix 3 details the criteria for determining whether hazards require further analyses. Techniques to be considered for analysing hazards include:

a. Fault Tree Analysis (FTA);

b. Failure Mode Effects Analysis (FMEA);

c. Markov Analysis; and

d. Dependence Diagrams.

15. Depending on the complexity of the system under study, it may be appropriate to use a combination of techniques. For instance, complex systems may first be described using FTA, and FMEAs then used to validate the FTA or define probabilities for specific failure conditions.

16. Hazard Mitigation. All hazards that have an assigned HRI of less than 15 have to be mitigated or accepted by the appropriate Commonwealth engineering authority. Specifically, the level of engineering authority required for accepting residual risks is to be commensurate with the residual HRI. Hazard mitigation is an iterative process that culminates when the residual risk has been reduced to an acceptable level.

17. When conducting a hazard analysis, the following hierarchy for risk mitigation shall be considered:

a. elimination of hazards through design improvement;

b. incorporation of safety devices;

c. provision of warning devices; and

d. development of procedures and training to avoid the hazard.

18. Hazards are considered to be mitigated and the residual risks acceptable when the calculated HRI is greater than 14. All actions taken to mitigate and accept hazards are to be recorded on EMERALD by the DE, either directly or through linked documents.

19. Safety Case Report (SCR). For ECPs, prior to Design Acceptance, the ECP Coordinator shall prepare a Safety Case Report (SCR) including a justifiable argument for the safety of the design change. The SCR should also include:

a. an overview of the hardware, software and human factors' hazards identified for the design, integration, operation, maintenance and disposal phases;

b. a summary of any analyses undertaken and mitigation of the hazards identified therein;

c. a summary of any residual risks and their recommendations; and

d. completed Hazard Logs as an enclosure (EMERALD Report).

20. Contracted Design Changes. Where a design change has been outsourced, the AEO status of the contractor shall be considered. Where the contactor does not have AEO status, the contractor shall be responsible for preparing the PHA in consultation with the coordinating DE. The DE will then be responsible for managing the process on EMERALD as per the process in appendix 1. Where the contractor holds AEO status, the DE raising the Statement of Work shall ensure that the contractor adheres to the minimum processes outlined in this SI. Development of the Statement of Work will include consideration of the requirements in AAP 7001.054 Section 2 Chapter 1, commensurately tailored to meet the scope of the design task. In all cases however, the contractor shall provide the following deliverables on completion of the design change:

a. a completed Hazard Log (electronic format), including the following fields:

(1) a short title capturing the nature of the hazard;

(2) a summary description of the hazard;

(3) probability of the hazards prior to mitigation;

(4) severity of the hazards prior to mitigation;

(5) the Hazard Risk Indices (HRI) prior to mitigation;

(6) mitigation strategies implemented;

(7) probability of the hazards post mitigation;

(8) severity of the hazards post mitigation;

(9) the hazards' HRIs post mitigation;

(10) status of the hazards (Open or Closed); and

(11) a record of safety analyses' approval (name and title).

b. a Safety Case Report, and

c. where the design change includes software changes, the DE is to consider the deliverable requirements of AAP 7001.054 Section 2 Chapter 7 for software safety assurance.

21. System Safety Management and Engineering Training. Formal System Safety Management and Engineering training is highly desirable for all XXSPO personnel to hold Design Engineer EA. Training is desirable for LOGENG and TD staff. The main training is provided by System Safety courses sponsored by SCI-DGTA, including requested periodical System Safety continuation training. Additional System Safety techniques training is provided on an as-required basis. The requirement for all training is included in the XXSPO training database.

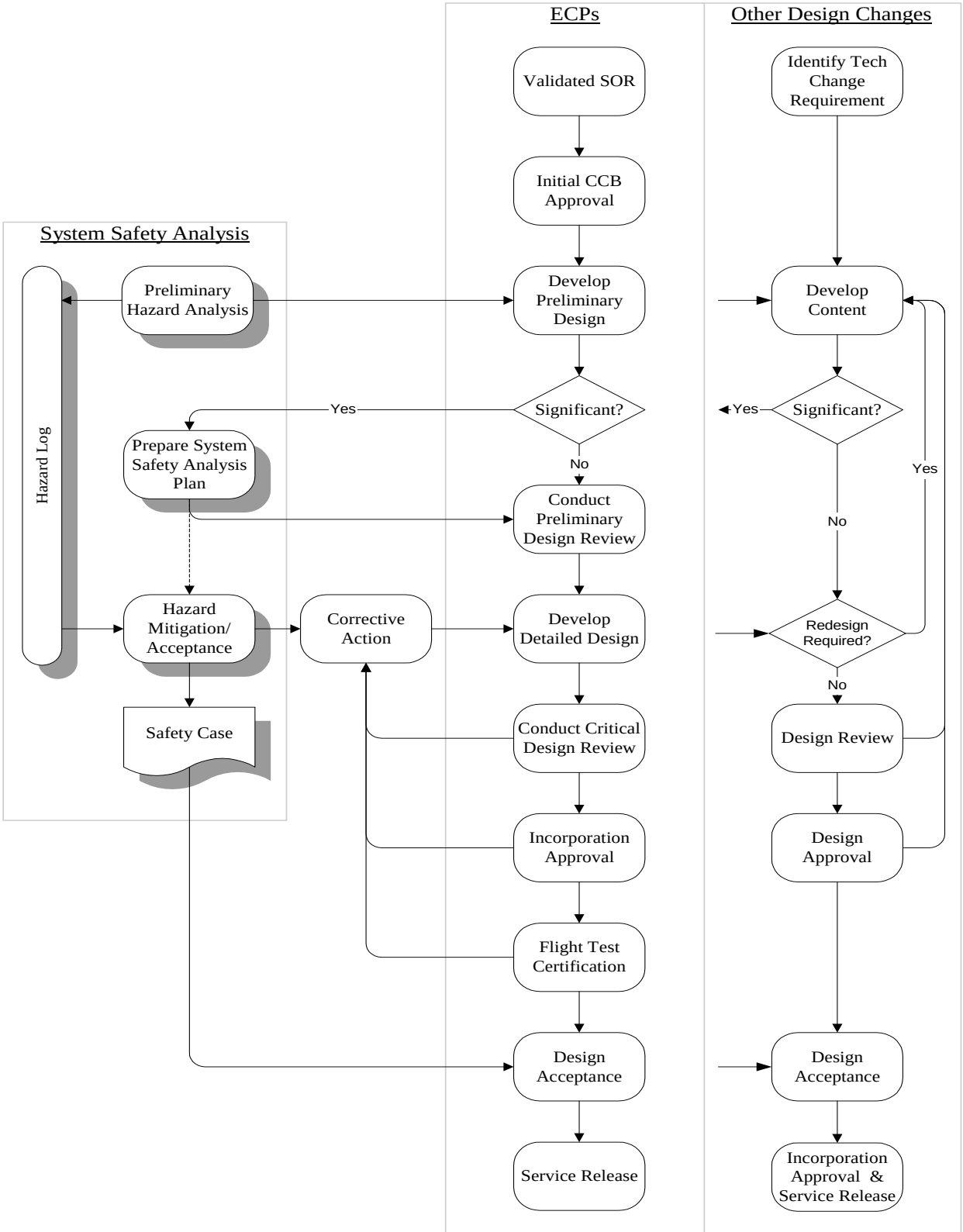
22. References. AAP 7001.054 Section 2 Chapter 1 provides further guidance on relevant standards and the application of system safety engineering to aerospace design changes or assessments. Section 2 Chapter 7 discusses safety assurance processes for software systems.

Appendices:

1. System Safety Design Change Process
2. Risk Acceptance Framework
3. Hazard Analysis Requirements

Appendix 1 To Annex A To
SI (LOG) XX-XX

SYSTEM SAFETY DESIGN CHANGE PROCESS



Appendix 2 To Annex A To
SI (LOG) XX-XX

RISK ACCEPTANCE FRAMEWORK

1. The following definitions of Severity shall be adopted when describing risk.

Hazard Severity Categories	
Category	**Description**
Catastrophic	Death, permanent total disability, aircraft loss, or severe environmental damage.
Critical	Severe injury, major occupational illness, major aircraft or systems damage, or major environmental damage.
Marginal	Minor injury, minor occupational illness, minor aircraft or systems damage, or minor environmental damage.
Negligible	Less than minor injury or occupational illness, less than minor aircraft or system damage or less than minor environmental damage.

2. The following definitions of Probability shall be adopted when describing risk.

Hazard Probability Categories			
Category	**Qualitative Description**		**Quantitative Description**
	Per Aircraft	**Entire XX Fleet**	**Per Flight**
Frequent	Likely to occur frequently.	Continuously experienced.	$p > 10^{-2}$
Probable	Will occur several times in the life of an item.	Will occur frequently.	$10^{-2} > p > 10^{-4}$
Occasional	Likely to occur some time in the life of an item.	Will occur several times.	$10^{-4} > p > 10^{-6}$
Remote	Unlikely but possible to occur in the life of an item.	Unlikely but can reasonably be expected to occur.	$10^{-6} > p > 10^{-8}$
Improbable	So unlikely, it can be assumed occurrence may not be experienced.	Unlikely to occur, but possible.	$p < 10^{-8}$

3. Authority for closing hazards shall be determined from the Hazard Risk Index (HRI) matrix below.

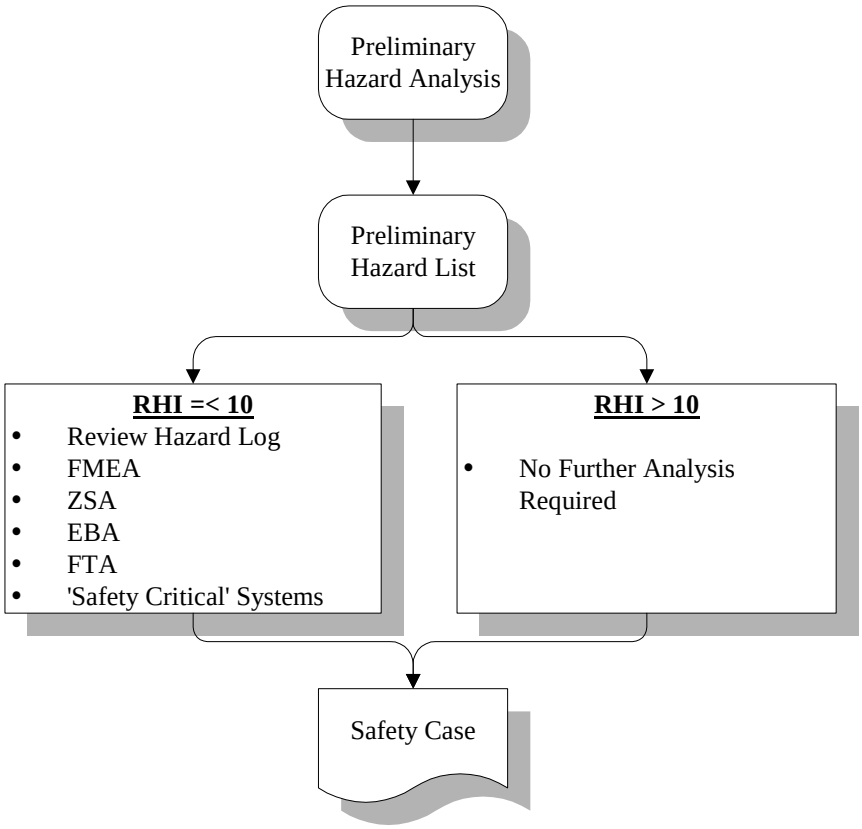
	Severity			
Likelihood	**Catastrophic**	**Critical**	**Marginal**	**Negligible**
Frequent $p > 10^{-2}$	1	3	6	10
Probable $10^{-2} > p > 10^{-4}$	2	5	9	14
Occasional $10^{-4} > p > 10^{-6}$	4	8	13	17
Remote $10^{-6} > p > 10^{-8}$	7	12	16	19
Improbable $p < 10^{-8}$	11	15	18	20

HRI	**Significance**	**Risk Acceptance and Authority**
1 - 6	N/A	Unacceptable
7 - 10	Significant	Requires mitigation, with acceptance by DAR and OAAR
11 - 14	Non-Significant	Requires mitigation, with acceptance by DE
15 - 20	Non-Significant	LOGENG or DE can accept

Appendix 3 To Annex A To
SI (LOG) XX-XX

HAZARD ANALYSIS REQUIREMENTS

1. The criteria for determining whether further System Safety analyses are required is detailed below.



FMEA - Failure Mode Effects Analysis
ZSA - Zonal Safety Analysis
EBA - Energy/Barrier Analysis
FTA - Fault Tree Analysis

Blank Page

COMMONWEALTH-LEVEL
SYSTEM SAFETY PROGRAM PLAN OUTLINE

1. The following provides a sample outline of a Commonwealth-level SSPP, for both a completely new acquisition, or an update to a legacy aircraft. This plan is particularly useful for identifying higher-level Commonwealth SSP aims, SSP requirements and in collating Commonwealth-only SSP processes.

2. Titles and content below requires tailoring to Project Office (PO) SSPP aims. Additional guidance or clarification can be sought from SCI3-DGTA.

SECTION	TITLE	DESCRIPTION
1.0	**INTRODUCTION**	
1.1	**General**	• Extent of SSP expected • Traceability expected • Legacy equipment integration to the SSP • SSPP role
1.2	**Purpose and Scope**	• Expected coverage of SSP tasks and responsibilities • Documents subordinate to Commonwealth-level SSPP • Documents to which the Commonwealth-level SSPP is subordinate
1.3	**Objective**	• SSP objectives for the project or in-service
1.4	**Applicable Documents**	
1.5	**Definitions, Abbreviations and Acronyms**	
2.0	**PO SSP MANAGEMENT**	
2.1	**Safety Management Overview**	
2.1.1	Safety References	
2.1.2	General	• Effect of the safety references on the development of the SSP
2.2	**System Safety Certification Basis**	• The original civil and military System Safety certification basis and when attained • Description of legacy systems' and COTS integration into the SSP
2.2.1	System Safety Baseline	• What documents are expected to constitute the aircraft type's System Safety Baseline
2.2.2	Updates to the System Safety Baseline	• Circumstances under which updates to the System Safety Baseline are expected
2.3	**Requirements Of The Contractor SSP**	• Expected scope of the Contractor SSP and how this will be conveyed to the Contractor • Interface of Contractor's SSP to sub-contractors and vendors
2.3.1	Contractor SSPP	• Expected coverage of Contractor's SSPP • System Safety Standards and guidance to be applied • Expected updates to the Contractor's SSPP • where the System Safety responsibility boundaries lie between ARDU, ASCENG, JALO, EOC, PO and the Contractor, for projects involving flight test, stores or explosive ordnance
2.4	**PO Authority And Responsibility**	• Overall PO authority and responsibility • Scope of authority and responsibility of the PO SSM • How the PO SSM expects to implement a program to achieve CoA SSP objectives • where the System Safety responsibility boundaries lie between ARDU, ASCENG, JALO, EOC, and the PO, for projects involving flight test, stores or explosive ordnance
2.5	**PO SSM Qualifications**	• Recommended qualifications and training requirements of

SECTION	TITLE	DESCRIPTION
		the PO SSM commensurate to PO SSP requirements and Contractor experience
2.6	**SSM Integration**	• Safety management activities that will ensure that the SSP is an integrated effort between hardware, software and human factors disciplines applied to design, integration, operation, maintenance and disposal of the aircraft system
2.7	**System Safety Interfaces**	• Intra and inter-CoA interfaces expected and roles and functions of those interfaces to allow the conduct of the SSP • PO expectations of the interfacing personnel • ASCENG, JALO, EOC, ARDU, DGTA interfaces to the PO and the Contractor • Responsibility for the conduct of the T&E hazard assessment
2.7.1	General	
2.7.2	System Safety Interfaces Within the PO	
2.7.3	System Safety Interfaces to Other Project Phases and Other Projects	
2.7.4	System Safety Interfaces to Command Aviation Safety Officers	
2.7.5	System Safety Interfaces to Unit Aviation Safety Officers	
2.8	**PO Safety Activities**	• System Safety Tasks and their aims
2.8.1	PO Executives' Meetings	• Expected System Safety aims, inputs and outputs
2.8.2	Project Management Reviews	• Expected System Safety aims, inputs and outputs
2.8.3	System Safety Groups and Working Groups	• Expected System Safety aims, inputs and outputs • Reference to the SSG/SSWG Charter
2.8.4	Type Certification Working Groups	• Expected System Safety aims, inputs and outputs
2.8.5	Flight Test Readiness Review	• Expected System Safety aims, inputs and outputs
2.8.6	Safety Review Boards	• Expected System Safety aims, inputs and outputs
2.8.7	Contractor Input to CoA Flight Test Safety	• Expected System Safety aims, inputs and outputs
2.8.8	Review of Safety-Related DRs and STRs	• Expected System Safety aims, inputs and outputs
2.8.9	System Safety Input to Reviews	• Expected System Safety aims, inputs and outputs
2.8.9.1	System Safety Reports	• Expected System Safety aims, inputs and outputs
2.8.9.1.1	ECP System Safety Reports	• Expected System Safety aims, inputs and outputs
2.8.9.1.2	Waiver/Deviation System Safety Reports	• Expected System Safety aims, inputs and outputs
2.8.9.2	Preliminary Design Reviews	• Expected System Safety aims, inputs and outputs
2.8.9.3	Critical Design Reviews	• Expected System Safety aims, inputs and outputs
2.8.9.4	Technical Publication and Modification Order Reviews	• Expected System Safety aims, inputs and outputs
2.8.9.5	Safety-Critical DR and STR Reviews	• Expected System Safety aims, inputs and outputs
3.0	**SYSTEM SAFETY REQUIREMENTS**	
3.1	**System Design Criteria**	• How and where System Safety Design criteria will be generated, and what processes these will feed into
3.2	**Historical Data Use**	• What safety requirements are expected from historical 'lessons learned' databases
3.3	**Design Precedence**	• Expected System Safety hazard mitigation design order of precedence
4.0	**SAFETY ASSESSMENT TECHNIQUES**	• How a systematically integrated SSP and tasks will be achieved to account for hardware, software and human factors considerations in equipment design, integration,

SECTION	TITLE	DESCRIPTION
		operation, maintenance and disposal
4.1	**Hardware Safety Risk Assessment**	
4.1.1	Failure Condition Severity Definitions	
4.1.2	Probability Definitions	• Qualitative and quantitative definitions
4.1.3	Probability and Severity Relationship	• Hazard Risk Index (HRI) matrix provided, with residual risk acceptance levels defined
4.2	**Software Safety Risk Assessment**	
4.2.1	Software Safety Assurance	• What assurance guidance will be used and how this will be applied to increase confidence in the software
4.2.2	Software System Safety	• What software system safety guidance will be used and how it will be applied to increase confidence in the software
4.2.2.1	Software Hazard Criticality Matrix	• Provision of the Software Hazard Criticality Matrix and how this will interface to the HRI
4.3	**Human Factors' Safety Risk Assessment**	
4.3.1	Human Factors' Analysis and Interface with Human Engineering Program (HEP)	• What System Safety input and requirements will the HEP provide • How will the HEP provide input to all System Safety activities and how will this input be included into integrated safety analyses and assessments
4.4	**Compliance Assessment Methodology**	• System Safety tasks expected of the contractor, and how they will value-add to the PO SSP aims
4.4.1	Compliance finding process	• How the PO expects to conduct compliance findings against the certification basis and what artefacts it expects to provide that evidence
4.4.1.1	A/C Level Functional Hazard Assessment (FHA) ***or equivalent military safety tasks***	
4.4.1.2	System-Level FHA (SFHA)	
4.4.1.3	Preliminary System Safety Assessment (PSSA)	
4.4.1.4	System Safety Assessment (SSA)	
4.4.1.5	Health Hazard Assessment (HHA)	
4.4.1.6	Hazard Log/Database	
4.4.1.7	Safety case Report	
4.5	**Safety Critical Items/Systems**	• Definition of Safety-critical items/systems • List of safety-critical items/systems (if possible) • Differences in handling safety-critical items/systems
4.6	**Verification Techniques**	• Process and actions by which incorporation of mitigations will be verified, and assessed as being adequate against their mitigation requirements
4.7	**Closed Loop Hazard Tracking System**	• Expected purpose and functioning of closed loop hazard tracking system
4.8	**Flight Operations And Test Safety**	• Expected System Safety aims, inputs and outputs
4.8.1	Contractor Flight Test Safety Activities	
4.8.2	Commonwealth Flight Test Safety Activities	
5.0	**SYSTEM SAFETY ACTIVITIES**	
5.1	**System Safety Data**	
5.1.1	Contractor-Required Safety Deliverable Data Schedule	
5.2	**System Safety Audits**	• If audits of the contractor and sub-contractors are expected,

SECTION	TITLE	DESCRIPTION
		what are the System Safety aims, inputs and outputs • Strategy for amalgamating System Safety audits with other CoA audits of the contractor and sub-contractors
5.3	**Contractor Support – Incidents, Accidents And Investigations**	• What is the scope and effort expected of the Contractor for aircraft incidents, accidents and investigations, both pre-delivery and post-delivery of each airframe
5.4	**PO – Incident/Accident Handling**	• PO procedures
5.4.1	Incoming For-Information Incidents and Accidents	• PO procedures for handling for-information incident and accident sources of data which may have an effect on the PO platform as well
5.4.2	PO Incident s and Accidents – Disposition	• PO procedures for implementing and tracking the implementation of incident and accident recommendations
5.5	**PO Acceptance Of Residual Risk**	• How the PO is expecting to ensure that all hazards are accepted by the CoA • For hazards which have specifically remained above the 'Acceptable' risk line after mitigation, how the PO will ensure that CoA management levels commensurate to the risk will accept this risk
5.6	**PO Safety Sign-Off**	• Expected minimum System Safety aims, inputs and outputs
5.6.1	Safety Sign-Off Prior to design T&E	• Minimum System Safety activities expected prior to initial and on-going ground and flight tests • Additional risks expected if this level of disclosure is not attained
5.6.2	Safety Sign-Off Prior to Commonwealth Design Acceptance	• System Safety aims, inputs and outputs • Safety Case Report usage for these aims
5.6.3	Safety Sign-Off Prior to OT&E	• Minimum System Safety activities expected prior to OT&E
5.7	**Safety Training**	• Expected Safety training for all Commonwealth and Contractor staff involved with the new or updated weapon system
Annexes		
A	**RECOMMENDED PO SSM QUALIFICATIONS**	
B	**PO SSWG CHARTER**	

Appendix:

1. Typical SSPP Compliance Finding Activities

TYPICAL SSPP COMPLIANCE FINDING ACTIVITIES

1. The following provides an example of the typical compliance finding activities required to establish confidence in a SSPP.

Table 1–G1–1 Typical Compliance Finding Activity Requirements

Requirement	Activity	Aim
Always required	Review of SSPP, Safety assessments or analyses, SCRs, and Hazard Log	• To ensure SSP DIDs are complied with. • To ensure FPOs are being achieved.
For systems whose criticality is Hazardous/Critical or above	Review of Design	• To determine at a system architectural level if the design, when implemented, is likely to provide an adequate level of safety in its intended application., and that Commonwealth endorsement has been provided. • To better understand new or novel design features for determining safety requirements.
	Review of Defect Reports, Deficiency Reports and System Trouble Reports	• To validate that all test results and analyses are supported by demonstrated product stability and appropriate performance and mitigation during development activities. • To provide a basis for continued airworthiness management.
	Witnessing of Qualification Testing	• To ensure that test results are valid and applicable. • To provide independence for test activities that are subjective rather than quantitative.
	Review of Safety Case Report	• To establish that the implemented design provides the required level of safety. • To determine possible operating restrictions or limitations. • To ensure Commonwealth acceptance of residual risk at the correct management level.
For systems whose criticality is Catastrophic	Witnessing of Developmental Testing	• To ensure that test results are valid and applicable. • To provide independence for test activities that are subjective rather than quantitative.
	Review of Test Plans/Procedures	• To ensure that the test program includes System Safety qualification requirements to support a System Safety compliance finding.
	Review of Test Results	• To make System Safety compliance findings for relevant aspects of the SSP.
	Review of Safety Case Report	• To establish that the implemented design provides the required level of safety. • To determine possible operating restrictions or limitations. • To ensure Commonwealth acceptance of residual risk at the correct management level.

Blank Page

SAMPLE CBD ENTRIES FOR MILITARY AND COMMERCIAL-BASED SYSTEM SAFETY PROGRAMS

1. The following tables provide sample CBD entries for military and commercial-based SSPs. Additional tailoring guidance or clarification can be sought from SCI3-DGTA.

Table 1–H–1 Sample System Safety CBD Table for Military System Safety Programs

Airworthiness Requirement	Revision Status	Description	Compliance Finding Activity	Compliance Finding Agency	Compliance Evidence
(Prior Certification) MIL-STD-882C	-	System Safety Program Requirements	S	NAVAIR (USN)	System Safety Program Plan, Safety Compliance Report
(New Development) MIL-STD-882C	-	System Safety Program Requirements: for Software changes for A-A Missile integration	I, T, A	NAVAIR (USN)	System Safety Program Plan, Safety Compliance Report
(New Development) MIL-STD-882C	-	System Safety Program Requirements: for A-A Missile integration	I, T, A	AIR NNNN PO	System Safety Program Plan, Safety Case Report
Specification Clause yy.yy	5	System Safety Program	I, T, A	AIR NNNN PO	System Safety Program Plan, Safety Case Report

Table 1H–2 Sample System Safety CBD Table for Commercial System Safety Programs

Airworthiness Requirement	Revision Status	Description	Compliance Finding Activity	Compliance Finding Agency	Compliance Evidence
(Prior Certification) FAR 25.1309	1 Jan 95	Equipment, Systems and Installations	S	FAA	System Safety Assessment Reports for each system, Type Certification Data Sheets
(New Development) FAR 25.1309	1 Jan 01	Equipment, Systems and Installations: In-flight refuelling system	I, T, A	FAA	System Safety Assessment Reports for each system, Type Certification Data Sheets
(New Development) FAR 25.1309	1 Jan 01	Equipment, Systems and Installations: Countermeasures Dispensing System	I, T, A	AIR NNNN PO	System Safety Program Plan, System Safety Assessment Report, Safety Case Report
Specification Clause yy.yy	7	System Safety Program	I, T, A	AIR NNNN PO	System Safety Program Plan, Safety Case Report

For Compliance Finding Column: I – Inspect, T – Test, A – Analyse

Blank Page

EXAMPLE SYSTEM SAFETY WORKING GROUP CHARTER

1. System Safety Working Groups (SSWGs) are typically organised to achieve the following aims:

a. To allow different internal and external Subject Matter Experts (both technical and operational) to discuss subjective safety issues and their adequate mitigation options.

b. To review SSP status, including results of technical or operational risk assessments of relevance.

c. To summarise hazard analyses including identified problems, status of resolution, and residual risk.

d. To develop and/or validate system safety requirements and criteria applicable to the SSP.

e. To identify safety program deficiencies and provide recommendations for corrective actions or prevention of re-occurrence.

f. To plan and coordinate support for design change acceptance.

g. To provide Commonwealth management with consensus recommendations on hazards and safety issues.

2. The following provides a sample In-Service System Safety Program Charter, and tailoring is required to suit either individual SPO or Project Offices' SSP aims.

XXX WEAPON SYSTEM SSWG CHARTER

Purpose. The xxx System Safety Working Group (SSWG) is an advisory group to the OC xxxSPO, and is an aid in the implementation of the xxx SSP throughout the weapon system's life cycle. SSWG member and adviser lists are attached.

The xxx SSWG will serve the following functions:

a. Reviews SSP effort for compliance with system safety criteria, and recommend action to accept or correct deficiencies.

b. Reviews procedural data for safety impact and recommend appropriate action.

c. Reviews and recommend action on any safety deficiencies identified by other organisations.

d. Reviews safety aspects of proposed significant design changes, including review of hazard analyses' and assessments' residual risk for acceptance.

e. Assigns action items and tracks them until resolution is complete.

f. Reviews hazards and their hardware, software and human factor causes, identified as part of Engineering Change Proposals, Deficiency Reports, System Trouble Reports, Deviations, and Waivers across Weapon System design, integration, operation, maintenance and disposal.

g. Performs other system safety tasks as assigned by OC xxxSPO.

To carry out these functions, the SSWG will draw upon the consensus expertise of its members and advisers.

Authority. In accordance with AAP 7001.054 Section 2 Chapter 1, the SSWG provides safety surveillance, coordination and recommendations. All SSWG decisions will be provided as recommendations to OC xxxSPO.

SSWG Attendees. The following describes SSWG constituents:

a. Members

(1) The membership for the SSWG will include representatives of the organisations listed in the attachment, reflecting all weapon system stakeholder representatives. Members may be added or deleted from this list as deemed necessary by OC xxxSPO.

(2) Member organisations are selected because of their close association with safety considerations in design, integration, operation, maintenance and disposal of the weapon system. Member participation in the SSWG is essential to provide stakeholder input (or awareness) on issues that will impact throughout the life cycle of the system.

(3) Member responsibilities:

(a) Submit agenda items when informed of an upcoming SSWG meeting.

(b) Be prepared for discussion of, and action, on agenda items.

(c) Attend all SSWG meetings or send a knowledgeable alternate.

(d) Provide their own organisation's official position on matters addressed by the SSWG.

(e) Respond to action items assigned by the chairman, by the due date.

(f) Familiarise themselves with the applicable SSP and safety documents.

b. Advisers

(1) Advisers include organisations that provide specialist technological knowledge. Advisers to the xxx SSWG will include, but are not limited to, organisations listed in the attachment. Additional advisers may attend, as deemed necessary by the chairman.

(2) Adviser responsibilities:

(a) Respond to action items assigned by the chairman, by the due date.

(b) Study issues assigned to them and provide professional opinions and recommendations.

(c) Act as a System Safety liaison between their respective organisations and the xxx SSWG.

Administration. The SSWG will be administered through the following mechanisms:

a. The SSWG will be officially chaired by the xxxSPO System Safety Manager (SSM). The SSM may delegate the SPO Deputy SSM to chair the meeting in their place. The chairperson will assign all action items. The chairperson has the final approval authority for the SSWG Minutes.

b. Meetings will be held as required, but at least once a year. SSWG Members and advisers will be notified of the SSWG date approximately thirty days prior.

c. The xxxSPO SSM will be responsible for notifying members and advisers of upcoming SSWG meetings and for providing them with an agenda with adequate time to prepare on issues to be discussed. A sample agenda is attached.

d. SSWG presentations will contain the necessary background, current status, and recommended solutions. A hard copy of the briefing material presented will be provided to the SSM for inclusion in the Minutes.

e. In the event of disagreement on recommendations, a minority report may be included in the Minutes at the discretion of the dissenting party/ies, for consideration by OC xxxSPO in making a final decision.

Annex:

A. Member and Advisor List for xxxSSWG

Annex A to
xxx SPO SSWG Charter

MEMBERSHIP AND ADVISOR LIST FOR XXX SSWG

MEMBERS

OC xxxSPO
xxxSPO CENGR
xxxSPO SSM
xxxSPO Avionics/Aeronautical Flight Commander
xxxSPO Design Engineers
xxxSPO DR/STR Manager
FEG Operational Representative
Wing Operational Representative/ Aviation Safety Officer
Squadron Operational Representative/ Aviation Safety Officer
Capability Systems Division Representative
Contractor SSM

ADVISORS

ASCENG
DGTA
Training Command Representative
Air Command Representative
Other Service Representatives
Contractor Engineering Specialists
DSTO Representative
AVMED Representative

Appendix:

1. Sample System Safety Working Group Agenda

Blank Page

SAMPLE SYSTEM SAFETY WORKING GROUP AGENDA

XXXSPO SSWG #1 AGENDA – 12-14 JULY 03

0900-1700 HRS ROOM C BUILDING L474 RAAF WILLIAMS

SSWG #1 Objectives

1. Baselining of xxx Weapon System, System Safety effort: Where we are and where we want to go.

2. Status of System Safety efforts.

3. Review of significant design assessment hazard mitigations for acceptance

	AGENDA ITEM	SPEAKER
1.	Opening Remarks and Introductions	xxxSPO SSM
2.	Previous Action Item Review	Individual Actionees
3.	SSP requirements and related PO Safety efforts	xxxSPO SSM
4.	Latest Design Assessment/Change Schedule	xxxSPO CENGR
5.	Hazard analysis progress and completion status for significant designs and assessments	xxxSPO CENGR
6.	Presentation of hazards from the hazard tracking database for each significant assessment or change for acceptance	Individual SPO DEs
7.	Review of Safety-Related DRs and STRs for closure plans and the existence of short term mitigations	SPO DR/STR Manager
8.	Safety-related changes processed since xxxx: - Status of safety-related Publication Improvement Requests - Status of safety-related publication amendments - Status of safety-related Flight Manual updates - Status of safety-related aircraft operating limitations - Status of Safety Critical Items/Systems who display negative reliability trends	xxxSPO CENGR & FEG Representative
9.	Discussion on xxx ASOR, MASOR and accident report recommendations for SSP implications	xxxSPO CENGR
10.	Safety implications from Trade Studies	xxxSPO CENGR
11.	Other Business	All
12.	Review of open Action Items	xxxSPO SSM
13.	Meeting Close and next SSWG date	xxxSPO SSM

Blank Page

SECTION 2

CHAPTER 2

ELECTROMAGNETIC ENVIRONMENTAL EFFECTS IN AIRBORNE SYSTEMS

INTRODUCTION

1. Aircraft Electromagnetic Environmental Effects (E^3) are the impact of the total electromagnetic environment (EME) upon the operational capability of an aircraft. E^3 phenomena encompasses both natural and man-made influences on the aircraft including lightning, precipitation static (p-static), electrostatic discharge (ESD), emanations security (EMSEC – formerly known as TEMPEST), Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC). With the trend towards lower operating voltages and the upward trend in emitted power levels, modern electronic equipment is becoming increasingly susceptible to EM energy.

2. E^3 considerations must be applied during the requirements definition, specification, design, development and test and evaluation phases of acquisitions, as well as the in-service support, modification and maintenance phases of an aircraft's lifecycle. Acquisitions and modifications that do not consider E^3 issues as part of their design and production activities may increase the risk of compromising mission capability, or at worst technical airworthiness.

3. This chapter details a number of E^3 concepts and provides guidance to Project Offices (POs) and SPOs on required E^3 activities for acquisitions, modifications and in-service support of ADF aircraft.

GENERIC APPROACH TO E^3 DESIGN

4. Many aircraft sub-systems and equipment are susceptible to the effects of electromagnetic energy. Whenever an aircraft sub-system or equipment is procured or modified, measures must be taken to ensure that the product does not suffer in performance when operating in its intended EME, or that the E^3 control measures already in place are not compromised. A generic approach to E^3 design can be loosely broken into five steps:

a. Establish the EME in which the system is to operate. The EME is the composite of all EM energy present in the operating environment of the aircraft, both man made and natural phenomena (lightning, p-static etc.). The operating EMEs for a civilian passenger aircraft and a military fighter aircraft will differ markedly. The passenger aircraft will be designed to operate in a relatively benign EME consisting of ATC radars, radio transmitters, natural phenomena etc. In addition to this EME, the fighter aircraft will need to contend with high-power airborne, land-based and maritime radars (both friendly and hostile), communication links and possibly a hostile electronic attack environment. All of this EM energy will have an impact on the ability of onboard equipment to function correctly.

The role of the aircraft will determine how the operating EME is defined. This definition process should occur in the concept stage of a project, prior to any acquisition or modification activities, and should be maintained and upgraded as appropriate throughout the life of a system.

b. Identify aircraft safety of flight (SOF) and mission critical (MC) equipment. A clear delineation between SOF, MC and other aircraft sub-systems is required. Aircraft E^3 validation must ensure that SOF sub-systems are capable of withstanding the platform's operational EME. MC sub-systems should also be capable of withstanding the same EME, although some compromises may be assessed by the project authority as acceptable (refer to Section 2 Chapter 1 for information on 'missionised hazards').

c. Establish the effects of the EME on aircraft systems. Aircraft fuselages and equipment casings offer varying degrees of protection to the sensitive internal components from the total EME. This environment is a combination of the induced external EME (EM energy admitted through aircraft apertures), and the emissions of the equipment within the fuselage, and should be used to define the fundamental EMI/EMC design criteria for equipment and equipment installations.

d. Design the system and equipment protection. The design of sub-systems and equipment should assure immunity to the effects of the operational EME levels, including clearance within the relevant margins (as

discussed later in this chapter). The key requirement is to allow the SOF equipment (and MC equipment, as required) to perform their intended functions without direct or indirect interference from the external EME.

e. **Verify the protection adequacy**. Two commonly utilised practices for assuring EMI/EMC performance are 'intrasystem' and 'intersystem' qualification. Intrasystem qualification uses testing and/or analysis to establish that onboard aircraft systems are compatible with each other. Intersystem qualification uses testing and/or analysis to establish that the aircraft is capable of performing SOF and MC functions whilst being exposed to the defined operational external EME.

5. The next part of this chapter provides a framework for addressing these five generic steps through the aircraft acquisition and modification processes.

GUIDANCE FOR ACQUISITIONS AND MODIFICATIONS

6. The information below defines the ADF preferred approach to E^3 design and verification activities for aircraft acquisitions and minor/major modifications. It introduces each of the topics involved in scoping and implementing E^3 considerations for new acquisitions and modifications.

7. In the context of this chapter, 'major modifications' are those that make significant electrical or electronic changes to an aircraft, particularly those that alter the layout and/or performance characteristics of wiring and SOF/MC equipment. While minor modifications may not have an impact on SOF/MC equipment, they still have the potential to introduce EMI problems. Hence the 'building block' approach should also be applied for minor modifications.

Building Block Approach to E^3 Assurance

8. In broad terms, assurance of the E^3 aspects of a design should be based on an incremental or 'building block' approach. Each 'building block' functions to provide an increased level of assurance in the design and integration effort, and consists of either design activities or verification activities. This distinction is important, as historically POs and contractors have tended to focus resources on verification activities that may have been better directed towards addressing key E^3 aspects of the design. For the ADF in particular it is important to put reasonable effort into the design activities because there are no accredited E^3 test facilities in Australia capable of performing electromagnetic vulnerability (ie. intersystem) testing of entire aircraft.

9. For in-country modifications, applying the 'building block' approach to EMC mitigates the risks associated with the lack of in-country electromagnetic vulnerability (EMV) test facilities, while maintaining an appropriate level of confidence in the E^3 integrity provided by design and integration activities. For overseas acquisitions or major modifications, the 'building block' approach provides a means by which POs can ensure that vendor E^3 programs achieve an appropriate balance of design and verification activities. The five building blocks are as follows:

a. equipment level qualification,

b. design/integration principles and practices,

c. installation practices,

d. verification of intrasystem compatibility, and

e. verification of intersystem compatibility.

10. By applying resources to ensuring the first three building blocks (E^3 design and installation aspects) are adequately addressed for the scope of the modification or acquisition, reliance on E^3 verification activities (intra- and intersystem testing) is significantly diminished. While intra- and intersystem testing are a useful check of a design, these methods of testing are resource-intensive, only a limited number of test points can be carried out in a reasonable timeframe and favourable results from one aircraft may not translate to other aircraft in the fleet. In addition, simulating an aircraft's operational EME in terms of modulations and power levels is extremely difficult using commercial equipment.

11. Predictive EMI software tools are not to be used as a substitute or alternative for testing. A DSTO research task, sponsored by DGTA, has shown these tools to be unsuitable for validation of the E^3 performance of aircraft systems.

12. An acquisition or major modification Statement of Work (SOW) should emphasise the importance of a contractor applying sound E^3 design and integration principles and good installation practices complemented by appropriate equipment qualification. Source/victim assessment is intended only as a limited confidence check to verify the absence of gross EMC problems. Intersystem testing, whilst providing some quantitative data to support establishment of an aircraft's electromagnetic vulnerability (EMV), is an expensive and time-consuming place in the development cycle to be correcting EMC problems which should have been mitigated during system design and integration. Thus the bulk of the ADF's effort should be spent ensuring that the equipment level qualification, system design, integration and installation aspects are satisfactory. A final check via intrasystem testing (and intersystem testing if deemed necessary) should be used to ensure that no system level problems result from the changes.

13. The material in the following sections should be considered in the context of the above building block approach, to ensure that the effort put into obtaining E^3 assurance is directed appropriately. Annex A provides guidance on E^3 requirements that should typically be reflected in a SOR for ADF aircraft acquisition and modification programs.

Equipment Level Qualification

14. Prior to determining the appropriate qualification levels for equipment, an analysis of the platform's operational EME, and criticality of onboard systems (SOF/MC/other) should be conducted. For a platform operating in a harsh EME, the SOF (and applicable MC) systems should be qualified to a rigorous (ie. military) standard.

15. For modification activities, or an acquisition altering the configuration of an NAA-certified civilian aircraft, the applicability of the E^3 standard(s) used for previous certification of the SOF, MC and other equipment should be analysed for applicability against new equipment. If the standards used for the existing certification are adequate for the defined EME, there is little to be gained from qualifying equipment to a more stringent standard. Given the high cost of designing and testing items to military standards, and the relatively benign operating EMEs of some ADF platforms, qualification of items to less stringent civilian standards may be perfectly acceptable.

16. Many older ADF platforms were procured against previous revisions of existing standards or against superseded standards. Qualification of new equipment against the latest revision of a military standard is DGTA's preferred approach, unless the use of a superseded revision or standard can be justified. For platforms that will be operating in harsh EMEs, or for equipment that requires higher levels of assurance (eg. SOF systems), a higher qualification level will usually be appropriate. POs/SPOs will thus need to give appropriate consideration to qualification levels for each equipment type depending on the item criticality and defined EME for the platform.

17. Ensuring correct application of standards to equipment. Many equipment level standards have multiple categories and/or limits applicable to tests (eg. different limits applied for rotary and fixed wing aircraft or a unique set of tests required for air launched missiles etc.). When specifying compliance to a standard or procuring COTS/MOTS equipment already compliant to a standard, the PO/SPO needs to ensure that the appropriate test categories and other requirements from the standard are suited to the item and its intended application/parent system. Test reports should be made available by contractors/equipment OEMs to allow PO/SPO engineers to confirm that the standard has been applied correctly. If the equipment has been tested incorrectly against the standard, the PO/SPO should only accept the equipment for service following additional testing to confirm compliance to the applicable requirements from the standard.

18. If there is doubt regarding the validity of a test report, a contractor/OEM has provided inadequate analysis of any failures, an unacceptable standard was used or the accreditation/credentials of the test facility are dubious, retesting should be considered. This early stage in the integration process permits potential shortfalls or problems to be examined or resolved at a much lower cost than later in the program. Additionally, fault-finding and problem resolution at the equipment level is far simpler than at the aircraft level (eg. during source/victim testing).

19. Failure against the selected standard. If equipment does fail individual tests of the selected standard, the shortfalls need to be carefully evaluated before declaring the item unsuitable or attempting a re-design. Aspects such as the frequency range(s) in which the failure occurred should be analysed, along with the level of emission/susceptibility shortfall against the standard. Should the difference be of an acceptably small amount or the frequency ranges of the failure not align with the emission/vulnerability characteristics of other systems in the aircraft, the item may be acceptable. POs/SPOs will need to carefully consider the ramifications of accepting the item, including the possible effect on future modifications. A tailored source/victim analysis, and Systems Safety assessment (if applicable), should be carried out to determine whether additional design activities are required to mitigate the non-compliance. Details of any equipment limitations/deficiencies are to be recorded by the PO/SPO and

passed to the in-service manager of the aircraft for use in the management of in-service EMI/EMC issues and future modifications of the platform.

20. During aircraft modifications, contractors may propose the use of equipment that is not qualified to a standard recognised by the ADF. If an analysis shows that the standard is not acceptable, the ADF may request that the item be tested to a higher standard to provide assurance that it will not introduce any EMI/EMC problems. This testing should be carried out by a qualified EMI test house (Australian facilities should be NATA-accredited for the selected test standard). Annex B contains guidance on the content and application of a number of E^3 standards that are recognised by the ADF.

Design, Integration and Installation Principles & Practices

21. Once compliance with the equipment level standards has been verified, a large number of items (including LRUs, wiring, equipment racks, antennas) must often be integrated and installed successfully into the aircraft, while ensuring EMC between all items.

22. **Electromagnetic interference (EMI).** For EMI to exist there must be three elements present:

a. a source to generate the energy,

b. a victim that is affected by the energy, and

c. a coupling path for the energy to be transferred from the source to the victim.

EMI can transfer from the source to the victim via two means, either a radiated path or a conducted path. Radiated EMI propagates through free-space from source to victim (eg. an antenna, cable or other item can receive radiated energy and transfer it to the victim). Conducted EMI is coupled directly from the source to the victim via wiring or metallic structure.

23. Elimination of EMI can be achieved by removing any of the three elements (source, victim or coupling path). Removing either the source or victim equipment from an aircraft is usually unacceptable, therefore efforts will be directed towards eliminating the coupling path, reducing the effect of undesirable emissions from equipment or reducing the susceptibility of victim equipment. The paragraphs below detail a number of design techniques that assist with achieving EMC between items within an aircraft.

24. **Equipment location.** As physical space is often at a premium in aircraft, options for suitable equipment locations can be limited. Regardless, sites for system installation must be assessed for any potential EMI from existing conducting or radiating sources. Strategies to minimise any possible interference should be introduced, for example, selecting a location where EMI is at a minimum or by using shielding. The EMI/EMC ratings of adjacent equipment should also be verified to ensure that the new equipment does not introduce any emissions which will result in EMI/EMC problems.

25. **Bonding.** Bonding controls voltages by providing low impedance paths for current flow. Good electrical bonding practices are an essential element of successful E^3 system design, and have solved many EMI/EMC issues such as p-static problems, susceptibility of electronics to the external EME, and lightning vulnerability. Electrical bonding within the system should provide good electrical continuity across external interfaces on electrical and electronic equipment, both within the equipment and between the equipment and aircraft structure to assist in the control of EMI/EMC. Bonding levels will vary depending on the materials, but 2.5mΩ is commonly used for metallic interfaces. Higher values may be justified for certain metals or composites – refer to AAP 7045.002-1 and MIL-STD-464A for more detailed information.

26. While the aim of bonding is to obtain good electrical contact between materials, this can lead to corrosion in the case of dissimilar metals. Additional corrosion control measures therefore need to be incorporated in aircraft maintenance practices and personnel should be made aware of this requirement to ensure that material bonding remains effective. MIL-STD-464A appendix A provides further information on electrical bonding.

27. **E^3 wiring practices.** AAP 7045.002-1 (ADF Aircraft Wiring and Bonding Manual) is the primary wiring installation manual for all ADF aircraft. Included in this publication are ADF requirements for wire labelling, including a category for applying an EMI/EMC criticality to individual wires. The application of EMI/EMC criticalities to wiring not only assists in fault-finding activities, it assists with conflict avoidance in future wire-routing activities. As this is one of the main causes of EMI/EMC problems, care should be exercised when deciding on the

routing of cables. For example, wiring for analogue signals, digital signals, DC power and AC power should be grounded separately to minimise potential E^3 problems.

28. The appropriate wire type EMI 'hardness' needs to be applied at the sub-system level (eg. airframe wire, shielded wire, twisted pair, through to wires with EMI attenuating coatings or fibre optic) dependent on:

a. the sub-system criticality,

b. the sensitivity of the equipment,

c. the physical location of the wire with respect to other sub-systems/equipment, and

d. the severity of the potential coupling characteristics from the external EME.

29. Antenna installations. Antenna bonding is important to ensure adequate system performance is achieved while providing sufficient low impedance paths for p-static, lightning and other RF sources. A poorly bonded antenna can severely reduce the effective range of a transmitter, even down to as low as a few hundred metres. In addition, reflected power via standing waves can cause damage to the transmitter. Antenna bonding also encompasses the cabling to the transceiver, by ensuring it has been correctly grounded. MIL-STD-464A appendix A contains guidance on antenna installations.

30. Shock and fault protection. Bonding of all exposed electrically conductive items subject to fault condition potentials should be provided to control shock hazard voltages and allow proper operation of circuit protection devices. MIL-STD-464A appendix A contains further information on this topic.

31. Lightning. Lightning strikes on or near aircraft can lead to severe damage to the airframe or avionics components due to the high currents involved. Aircraft typically have lightning discharge paths to permit the dissipation of charge build-up caused by lightning strikes. Maintenance units should take care to ensure that these discharge paths are maintained adequately. POs/SPOs undertaking modifications must take into account the existing lightning protective measures (and incorporate new measures if applicable) to ensure that there are no safety hazards introduced. Guidance on lightning aspects is provided in annex C to this chapter.

32. Margins. Margins are applied during system design to account for variability in system hardware and uncertainties from verification activities. The application of margins provides confidence that electromagnetic and electrical stresses induced internal to the system are below interference thresholds by at least the margin when the aircraft is subjected to its worst-case operational EME. Margins should be selected appropriate to the system (SOF, MC, ordnance etc.) and/or standard being applied and should not be waived for SOF systems or ordnance. For more information refer to MIL-STD-464A appendix A para A5.1.

33. Hazards of electromagnetic radiation to personnel (HERP). EM radiation has been proven to have an adverse biological effect on personnel. RF exposure guidelines have been generated by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) to protect both occupational and non-occupational personnel from the effects of RF exposure. Department of Defence compliance with these guidelines is a requirement and the policy is promulgated in the Defence Safety Manual (volume 1 part 4 chapter 2). SPOs and POs should ensure that new equipment, or modifications to existing equipment, are able to meet the requirements of the HERP policy.

34. Hazards of electromagnetic radiation to fuel (HERF). Fuel vapours can be ignited by an arc induced by a strong RF field. Aircraft and all associated equipment (including vehicles, earthing leads, hand-held radios etc.) should be designed and employed to ensure that fuels are not inadvertently ignited by radiation from onboard emitters or the external EME. MIL-STD-464A appendix A paragraph A.5.8.2, USAF Technical Order 31Z-10-4 and USN NAVSEA OP 3565 should be consulted for matters relating to HERF. Note that HERF is limited to ignition via sparks caused by RF energy, not electrostatic discharge, p-static or lightning.

35. Hazards of electromagnetic radiation to ordnance (HERO). Electro-explosive devices (EEDs) can be actuated or ‘dudded’ due to RF energy from the external EME, which may result in safety hazards or performance degradation of the explosive ordnance. EEDs should possess an adequate Maximum No-Fire Stimulus that will allow the EED to meet all performance requirements during its life cycle (storage, transport, handling and operation). Engineering staff from Guided Weapons and Explosive Ordnance Branch, AOSG–ASCENG and/or Directorate of Ordnance Safety should be consulted as appropriate for aircraft acquisition and modification activities with HERO implications.

36. Lifecycle hardness/maintenance. The E^3 protective measures on an aircraft naturally degrade over time through fatigue, corrosion and material breakdown. As such, these features should be easily accessible, maintainable and able to be surveyed to gauge condition (or, if not possible, survive the lifetime of the system without maintenance or inspection). Maintenance personnel should be trained on E^3 protective measures incorporated into the aircraft to ensure that the measures are maintained appropriately throughout the aircraft's lifecycle. The DGTA-sponsored 'E^3 Management Course for Maintainers' contains material on E^3 protective measures as well as other aspects relevant to maintenance personnel. MIL-STD-464A appendix A contains further guidance.

37. Electrostatic charge control. P-static arcing can result in the generation of broadband interference that may affect receiver sub-systems. This phenomenon will only manifest itself when the aircraft is airborne, with increasing probability when subjected to dust, ice, rain, snow or clouds. If the charge dissipation sub-system of the aircraft has been maintained appropriately, the probability of p-static related arcing is minimal.

38. All modifications that alter the exterior of an aircraft (such as a new panels or antennas) should be subject to p-static testing. Where p-static testing has not previously been performed on an ADF aircraft type, approval should be sought from the relevant SPO prior to testing. The ADF has a number of p-static test sets and SCI-DGTA personnel have had involvement in p-static testing on several ADF aircraft types. Units should contact SCI-DGTA if assistance with p-static testing is required. MIL-STD-464A provides further guidance on p-static.

Verification of Intrasystem Compatibility

39. Intrasystem EMC refers to the electromagnetic compatibility of aircraft sub-systems and equipment with each other. The most common intrasystem problems involve antenna-connected sub-systems, receivers, and microprocessor clock harmonics radiating from cabling. However, when appropriate controls are implemented in the aircraft design, such as EMI/EMC hardening, EMI/EMC equipment qualification and good grounding and bonding practices, intrasystem EMC problems are minimised.

40. Source/victim testing is the most common intrasystem verification method used in Commonwealth projects and provides some confidence that systems are compatible. While some intrasystem testing will usually be required, it is manpower intensive and it is not feasible to conduct a 100 percent check of all systems in all modes. A risk-based approach should be adopted during the development of the source/victim matrix to cull unnecessary source/victim combinations from the test plan. For example, justification for culling may be that there is no conducted or radiated coupling path where the systems are able to affect one another or that the systems and their harmonics operate in different areas of the frequency spectrum. Prior to testing, a list of existing E^3 problems and faults should be compiled to ensure that corresponding test fails are not attributed to the new modification. Annex D provides a detailed process for establishing source/victim test matrices, while MIL-STD-464A provides additional guidance on achieving sub-system compatibility.

Verification of Intersystem Compatibility

41. Intersystem EMC describes the ability of the aircraft to withstand its worst-case operational EME. Verification of an aircraft's ability to withstand its expected EME is very difficult due to the large range of possible emitters that an aircraft may encounter, the modulations of these emitters, high power levels and movement of the aircraft relative to the emitters. The most effective method currently available is to expose an aircraft in an anechoic or reverberation chamber to EM radiation that is representative of the expected EME while operating and monitoring the aircraft systems for interference.

42. Intersystem testing should only be considered for major modifications that make significant changes to aircraft systems and/or wiring, and therefore E^3 analysis in isolation does not provide sufficient assurance that SOF systems are still immune to the operational EME. In all cases, sound E^3 design and installation strategies, as well as previous qualification (and intrasystem testing to a limited extent) are relied on to retain the aircraft E^3 immunity. The decision to perform intersystem testing is best determined on a case-by-case basis via a risk-based assessment. There is currently no comprehensive in-country intersystem test capability in Australia so the ADF is restricted to overseas testing. This results in significant cost to the PO/SPO and requires long lead times to coordinate. If required, intersystem testing should therefore be planned early in the project/modification process, taking into consideration an aircraft and personnel being absent from their unit for several months. Annex E provides guidance in establishing the requirement for intersystem testing.

43. Low level swept coupling and bulk current injection (LLSC/BCI). While not a substitute for chamber testing, LLSC/BCI can be used to provide some confidence in system operation at low frequencies (usually 0.5 – 400MHz). LLSC/BCI involves determining a transfer function between the external field and the currents in a

particular LRU/wire bundle. This transfer function can then be extrapolated to determine the value of current to be injected into the LRU wiring. The use of this technique is popular in the UK, but still in its infancy in Australia. As such, programs that propose the use of LLSC/BCI should be assessed on the following criteria before using this testing technique:

a. the competence of the people, processes and data within the organisation involved with the testing;

b. the accreditation credentials of the facility/equipment used to perform the testing;

c. the quality, content and repeatability of the test procedures for the aircraft type in question; and

d. the application of appropriate margins.

PROJECT E^3 MANAGEMENT

44. For acquisitions and modifications, contractors (and the Commonwealth when acting as the design integrator) should have a program in place to manage E^3 strategies and ensure the inclusion of preventative and protective measures in their design. This will commonly be referred to as the E^3 Control Program (E^3CP), although contractors may use other names to describe these activities. Depending on the likely impact of E^3 issues on the acquisition/modification, the Commonwealth may need to obtain detailed information on the contractor's proposed E^3CP in order to provide the required level of oversight of the program.

45. Usually, little oversight will be required for acquisitions as the ADF generally buys aircraft from large, reputable companies with established skills in the E^3 technology area. For some projects, the Commonwealth will sign an agreement with a recognised National Airworthiness Authority (NAA) to perform certification activities on the Commonwealth's behalf. In this case there will usually be little need for the Commonwealth to provide detailed oversight of the E^3 program as the NAA will perform this role. For modification projects, the level of risk will vary depending on the organisation that has primary responsibility for the design. If a third party (non-OEM) contractor is performing the modification, a high level of oversight will probably be required as the company is unlikely to be familiar with the original E^3 design aspects of the aircraft, nor have access to OEM E^3 design data. In cases where the Commonwealth is acting as the design integrator, the risk will generally be considered high due to Commonwealth staff not regularly undertaking complex aircraft modifications. In this case, a detailed plan should be prepared and reviewed by a third party (eg. SCI-DGTA).

E^3 Control Program Plan

46. Where detailed information on the E^3 design strategies is required, contractors (or the PO/SPO when acting as the design integrator) should generate an E^3CP Plan (E^3CPP). The E^3CPP is used to detail the proposed E^3CP and demonstrate how the E^3CP will be implemented and managed throughout the project/modification. The review authority is then able to ensure that the organisation is conducting all necessary activities and applying sufficient rigour to the E^3 aspects of the design.

47. Once the E^3CP has been established, the E^3CPP should be updated on a regular basis to reflect any developments or changes in the program. As such, the E^3CPP should be treated as a living design document throughout the acquisition/modification activity rather than a deliverable item provided by the OEM/contractor at the beginning of the project. Annex F outlines the requirements that should be addressed in an E^3CPP.

E^3 Control Advisory Board (E^3CAB)

48. For projects requiring significant Commonwealth oversight, an E^3CAB may be set up to monitor the E^3CP, provide a means of expediting solutions to problems and establish high level coordination between agencies. An E^3CAB consists of specialist representatives from the contractor, sub-contractor (if applicable), the Commonwealth and any other relevant agencies. The role, responsibilities and composition of the E^3CAB should be defined in the contract and also detailed in the E^3CPP.

Plan for E^3 Aspects of Certification

49. For projects of low technical risk (eg. an acquisition from a large and well established manufacturer, modification by an OEM or a highly competent third-party contractor with access to OEM design data), POs/SPOs will usually not need detailed design information to ensure that the E^3 aspects are being carried out satisfactorily. In this case a Plan for E^3 Aspects of Certification (PE^3AC) (which contains considerably less data than an E^3CPP) may be

more appropriate. The aim of the PE^{3}AC is to demonstrate at a high level, through reference to processes, design documentation, test reports etc., that the E^3 aspects of the design will meet the requirements in the CBD and SOR. Additionally, the PE^{3}AC should provide information that can be passed on to the in-service managers to assist with managing E^3 aspects of future modifications or E^3 issues that may arise during the aircraft's life. Refer to annex G for PE^{3}AC requirements.

Contractor Documentation

50. The PO/SPO will need to determine how much contractor-produced E^3 documentation (eg. design documents, test plans/reports etc.) is to be procured during the project. This will primarily depend on the level of Commonwealth oversight being provided, however documents describing important aspects such as the design philosophies employed, performance, shortfalls etc. may provide the project and in-service managers with information that will significantly benefit future modification or management activities. Consideration should therefore be given to which documents will provide the project with the necessary information to manage the E^3 aspects effectively, as well as providing the necessary information for future management activities.

IN-SERVICE E^3 MANAGEMENT

51. An aircraft's E^3 integrity may be compromised over time due to wear and tear, and minor modifications. SPOs and maintenance units should therefore focus attention on maintaining the E^3 protective measures of the aircraft during its in-service life to ensure continued satisfactory performance. This can be achieved by maintaining an ongoing awareness of the protective measures through attending the E^3 Management training courses sponsored by DGTA, and actively ensuring the preservation of these measures during maintenance and modification activities.

52. E^3 Management Plan (E^{3}MP). To assist with this activity, SPOs may wish to create and maintain an E^3 Management Plan (E^{3}MP) to provide a collection of information and guidance to support the through-life management of E^3 issues associated with a specific aircraft type. An E^{3}MP should detail the E^3 design/mitigation strategies incorporated in the aircraft, specific guidance for conducting modifications and maintenance, details of any equipment emission/susceptibility non-compliances, other known aircraft E^3 issues, E^3 test history and results, and so on.

53. Reporting and rectifying EMI problems. Over the life of an aircraft, unresolved E^3 issues can lead to significant degradation of onboard systems and hinder fault-finding activities. Reporting and recording of E^3 problems in a single location (eg. a database maintained by the SPO) will assist in identifying fleet-wide issues, prioritising E^3 problems and promulgating appropriate rectification actions. Reporting of EMI problems must be accurate to give the best chance of replication by maintenance personnel, so all relevant parameters such as atmospheric conditions, system modes and aircraft configuration should be recorded.

ASSOCIATED ISSUES

54. Emanations security (EMSEC – also known as TEMPEST). If an aircraft acquisition or modification affects secure voice facilities, sub-systems that process any information above Restricted level or invalidates previous EMSEC qualifications, EMSEC testing may be required. 462SQN Detachment Laverton produces an 'Emanations Security Bulletin' specifically relating to aircraft design requirements. This bulletin provides guidance to POs/SPOs on design, testing and certification of EMSEC related aspects of aircraft acquisitions/modifications and is available on request from 462SQN Det Laverton. The Commonwealth has specific EMSEC design requirements, therefore if alternate standards are proposed by a contractor, POs/SPOs should check with 462SQN Det Laverton to ensure that Commonwealth requirements continue to be met.

55. Electromagnetic pulse (EMP). While the ADF has not historically required aircraft to be protected against EMP, POs for new acquisitions should establish whether EMP protection is a capability requirement. Some ADF aircraft may already incorporate EMP protection and the appropriate authority should decide whether to retain this protection.

56. Emission control (EMCON). EMCON is the effective management of all electromagnetic emissions to prevent premature disclosure of the presence, location and composition of own forces. Depending on role, some ADF aircraft types may need EMCON functionality to comply with emission policies during operations. Advice and requirements on EMCON should be sought from the relevant FEG. MIL-STD-464A Appendix A contains further information on this topic.

57. EM spectrum compatibility. All radiating equipment onboard aircraft need to comply with ADF and civilian (both national and international) regulations for the use of the electromagnetic spectrum. The Spectrum and

Communications Regulation (SCR) organisation within Chief Information Officer Group (see paragraph 61.f) are able to advise SPOs/POs on spectrum usage issues.

58. Portable electronic devices (PEDs). Refer to Section 2 Chapter 18 of this manual for information on PEDs.

59. Role equipment. Refer to Section 2 Chapter 14 of this manual for information on Role Equipment.

60. Simulators and system support facilities. Any simulators, procedural trainers, systems engineering/software support facilities etc. will generally comply with domestic E^3 standards. The E^3 standards and processes in this chapter are unlikely to be relevant to these systems.

ADO E^3 POINTS OF CONTACT

61. The following Defence organisations possess expertise in various disciplines of E^3 and are available to provide advice:

a. Systems Certification and Integrity (DGTA). Primary point of contact is SCI2A on 03 9256 3551 or DGTA.E3enquiries@defence.gov.au. SCI-DGTA provides centralised expertise for airborne E^3 including establishing design and testing requirements and provision of specialist E^3 advice. In addition, SCI sponsors two courses (E^3 Management for Designers and E^3 Management for Maintainers) to improve the level of E^3 knowledge in Defence and related organisations. Refer to the DGTA website for further information.

b. 462SQN Det Laverton. Primary point of contact is the TEMPEST Standards Officer on 03 9256 4144. 462SQN Det Laverton (formerly IOSQN) are the ADF centre of expertise for aircraft-related EMSEC/TEMPEST issues and testing, and also sponsor the Emanations Security Bulletin.

c. Guided Weapons and Explosive Ordnance Branch. Centre of expertise for the in-service management and acquisition of aircraft EO systems. Points of contact are CENGR of the SPO (in-service systems) on 02 4737 0905 and CENGR Guided Weapons Acquisition on 02 6265 7443.

d. Aircraft Stores Compatibility Engineering Agency (AOSG). ASCENG are the ADF centre of expertise for aircraft stores clearance issues. Point of contact is Director ASCENG on 08 8393 2208.

e. Directorate of Ordnance Safety (Joint Logistics Command). DOS provide assurance that EO is safe and suitable for service, and are the technical regulatory authority for storage and transport of EO.

f. Spectrum and Communications Regulation (Chief Information Officer Group). SCR are responsible for the coordination of Defence spectrum management and communications regulation and can be contacted at spectrum.planners@defence.gov.au.

g. Air Operations Division (AOD) – DSTO. AOD has a small cell of personnel employed on E^3 research and technology tasks related to topical E^3 issues. In some cases, DSTO may be available for assistance with E^3 investigative tasks, however SCI2-DGTA (as the DSTO research task sponsor) should be contacted in the first instance.

Annexes:

A. E^3 Statement of Work and Specification Requirements

B. E^3 Standards and References

C. Aircraft Lightning Immunity Guidance

D. Intrasystem Testing

E. Establishing the Requirement for Intersystem Testing

F. E^3 Control Program Plan Requirements

G. Plan for E^3 Aspects of Certification Requirements

Blank Page

E^3 SOW AND SPECIFICATION REQUIREMENTS

1. The Commonwealth must ensure that acquisition and modification projects satisfactorily address E^3 issues. The following paragraphs provide guidance to POs/SPOs on the E^3 items that should be placed into a SOR. While the requirements/standards suggested below are those preferred by DGTA based on past experience, alternative standards suggested by OEMs/contractors may be suitable and an assessment should be carried out by the PO/SPO (with SCI-DGTA assistance, if necessary) to determine whether the alternative is suitable.

2. Equipment-level standards. The role and operating environment of the aircraft should be assessed to determine an appropriate equipment level standard. 'Military' aircraft equipment (especially SOF and MC systems) should be tested to MIL-STD-461E, while systems other than SOF/MC items should also meet the requirements of this MIL-STD, or an acceptable alternative standard. 'Civil' aircraft equipment may be tested against a less-stringent civilian E^3 standard such as RTCA DO-160E. When specifying an equipment level standard, the appropriate test types and limit lines for the equipment application should be taken into account (if required, contact SCI-DGTA for more information).

3. The PO/SPO should request a copy of the test report from the manufacturer/contractor, along with an analysis of any non-compliance with the chosen standard. This report will provide assurance that the appropriate tests were carried out and correct limit lines used for the end application. Advice should be sought on any non-compliance with the test standard to determine whether the item is suitable or requires modification to achieve EMC.

4. Design/integration/installation requirements. Any unique Commonwealth requirements relating to the E^3 aspects of design, integration or installation should be addressed in the SOW. Refer to chapter 2 for further information on requirements relating to the following design/integration/installation items:

a. Bonding. Requirements should be drawn from AAP 7045.002-1 in conjunction with MIL-STD-464A;

b. Wiring. Requirements should be drawn from AAP 7045.002-1 in conjunction with MIL-STD-464A;

c. Antenna installation/placement. Requirements from MIL-STD-464A should be used for all acquisition and modification activities;

d. Lightning. Refer to annex C for assistance in determining lightning-related requirements. Where possible, MIL-STD-464A should be specified for military aircraft;

e. Hazards of Electromagnetic Radiation to Personnel (HERP). Refer to SAFETYMAN volume 1 part 4 chapter 2, noting that the requirements of the ARPANSA standard contained in SAFETYMAN are mandated by law;

f. Hazards of Electromagnetic Radiation to Fuel (HERF). Requirements should be drawn from MIL-STD-464A;

g. Hazards of Electromagnetic Radiation to Ordnance (HERO). Where applicable, Guided Weapons and Explosive Ordnance Branch, AOSG–ASCENG and/or Directorate of Ordnance Safety are the authorities for provision of guidance and requirements on all aspects of EO;

h. P-static. MIL-STD-464A contains comprehensive p-static guidance and requirements for all modifications and acquisitions. In addition, POs/SPOs should determine whether p-static testing is required following a modification;

i. Electromagnetic Pulse. The requirement for EMP protection in a new platform, or maintenance of existing EMP protective measures, should be included in the contract. Refer to MIL-STD-464A for specific requirements if applicable;

j. Emission control (EMCON). Operational requirements for EMCON are to be determined by FEGs. POs/SPOs undertaking modifications to existing aircraft should ensure that the characteristics of the existing EMCON system are retained, while requirements for aircraft acquisitions can be obtained from MIL-STD-464A;

k. Emanations security (EMSEC)/TEMPEST. The 462SQN EMSEC Bulletin contains all necessary requirements for ADF aircraft. Assistance from 462SQN Det Laverton staff should be sought when generating requirements; and

l. Life cycle hardness requirements. Existing E^3 protective measures should be retained where possible. Additional measures installed or those for new aircraft acquisitions should be in accordance with MIL-STD-464A.

5. E^3 Control Advisory Board (E^3CAB). If the acquisition/modification is deemed to be of sufficient risk, the Commonwealth may request the contractor to establish and manage an E^3CAB to monitor the E^3 Control Program, and manage and coordinate E^3 problems to their resolution. Membership of the E^3CAB should comprise both contractor and Commonwealth personnel.

6. Intrasystem qualification. Given the value and relative ease of performing an intrasystem test program, POs/SPOs should specify the requirement to verify intrasystem EMC of the platform in the contract. MIL-STD-464A contains a section on intrasystem EMC aspects that will assist in generating contract requirements.

7. The type of project (acquisition, minor modification, major modification) and organisation responsible (OEM/third-party contractor) will dictate the amount of involvement the PO/SPO will have in defining and formulating the intrasystem test program in the contract. For cases where the Commonwealth needs to provide specific requirements for intrasystem qualification, refer to annex D for further guidance.

8. Electromagnetic environment (EME)/intersystem qualification. For new aircraft acquisitions, it is important to define the operating EME for the platform. This EME will depend on the role and operating environment of the aircraft and will determine the level of E^3 protection that must be designed into the systems and installation. For modification activities, the original EME should be maintained and used as the basis for the design unless there is a requirement to update it based on an aircraft role or environment change. Where a modification is sufficiently extensive or affects SOF systems, intersystem testing at an appropriate facility may need to be specified. This test program should use an appropriate EME and test applicable aircraft systems. Refer to annex E for further guidance.

9. For ‘military’ aircraft operating in a harsh EME (eg. fighter, naval helicopter), the most appropriate EME table from MIL-STD-464A should be selected for use as follows (refer to the standard for more information on each environment):

a. Table 1A –EME for deck operations on ships;

b. Table 1B – EME for shipboard operations in the main beam of transmitters;

c. Table 1E – EME for Army rotary wing aircraft; or

d. Table 1F – EME for fixed wing aircraft, excluding shipboard operations.

10. For ‘civil’ aircraft in ADF service (eg. training aircraft), a ‘civilian’ EME (eg. from EUROCAE ED-107) will often be most appropriate. Alternatively, a DSTO-generated EME based on real-world emitter data may be specified for use (contact SCI-DGTA in the first instance to discuss this option). The latter option may be most useful if an aircraft manufacturer has specified a unique EME for their aircraft and the PO needs to assess whether it will meet ADF requirements. If the Commonwealth has specific additional requirements, these test points could be factored into the OEM’s test program to meet any shortfalls.

11. In the past, some POs/SPOs have not received a test report following overseas test programs, making it extremely difficult to obtain information on test fails and to formulate a plan to remedy them. POs/SPOs should thus specify the requirement for a test report, including precisely what level of information is required in the document (such as details of test fails, thresholds and frequencies at which the failure occurred, interpretation of the failure etc.).

12. Documentation deliverables. Commonwealth documentation requirements should also be included in the SOW. The amount and level of documentation required under the contract will depend on the level of risk of the acquisition/modification. As a result, the following document types may need to be delivered/maintained throughout the project:

a. E^3 Control Program Plan (E^3CPP) – should be maintained as a living design document for projects where Commonwealth oversight/input into the E^3 control program is required (see chapter 2 and annex F for details);

b. Plan for E^3 Aspects of Certification (PE^3AC) – should be delivered for low-risk projects (see chapter 2 and annex G for details);

c. test reports – as discussed in the equipment and system level test sections above, disclosure of the E^3 performance of the aircraft/systems is important in determining whether the proposed product satisfactorily meets Commonwealth requirements; and

d. E^3 maintenance requirements – information on new/modified E^3 protective measures should be included in maintenance publications to assist in maintaining the EMC of the aircraft.

Blank Page

E^3 STANDARDS AND REFERENCES

1. There are a number of E^3-specific standards and references published by various international organisations. The US DoD standards (MIL-STD-461 for equipment and MIL-STD-464 for system level) are recognised by DGTA as the most appropriate standards for ADF aircraft which operate in a hostile EME. Where justified, a less stringent standard such as RTCA DO-160 may be used (eg. in the case of an ADF aircraft conducting operations similar to civil aircraft). Note, however that the E^3 principles and processes outlined in MIL-STD-464 should still be observed where possible.

2. The standards listed below are issued by a number of major organisations with E^3 experience (US DoD, UK MoD, FAA etc.). Even if these standards are not specified for use during an acquisition/modification, they contain excellent guidance and reference material that may assist with understanding E^3 issues, or solving problems. Where an OEM/contractor proposes a standard other than those listed below, a comparison between this and the DGTA-preferred standard should be performed. Contact SCI-DGTA if assistance is required with such a comparison.

UK Military Standards

3. DEF STAN 00-970 – Design and Airworthiness Requirements for Service Aircraft. This is a generic standard that addresses most E^3 requirements by reference to DEF STAN 59-41, although both documents are incomplete and lack verification requirements. As a result DEF STAN 00-970 E^3 requirements alone are not considered an adequate basis for certification of ADF aircraft and their sub-systems.

US Military Standards

4. MIL-STD-464A – Electromagnetic Environmental Effects, Requirements for Systems. This is a comprehensive E^3 standard for complete systems (ie. aircraft). This standard establishes requirements, verification criteria, and contractor tasks for E^3 protection of airborne, ground and support systems. MIL-STD-464A covers virtually all requirements for a complete E^3 Control Program with the exception of unique ADF requirements such as HERP and EMSEC/TEMPEST testing. While MIL-STD-464A provides extensive management guidance for achieving overall system electromagnetic compatibility, it also provides scope for customers to tailor the guidance to their own requirements.

5. MIL-STD-461E – Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment. This document establishes requirements for the control of electromagnetic emission and susceptibility characteristics of electronic, electrical, and electromechanical sub-systems and equipment. MIL-STD-461E individually assesses conducted emissions, radiated emissions, conducted susceptibility and radiated susceptibility of equipment. Note that testing to MIL-STD-461E is limited to aircraft sub-systems/equipment only, not aircraft-level testing. Tests within MIL-STD-461 are applied depending on the higher level system that the equipment will be fitted to (eg. fixed wing land-based, rotary wing, air launched weapon). The appropriate set of tests should be specified for the equipment, as well as selection of the appropriate limit line for each test.

Civilian standards

6. RTCA DO-160E – Environmental Conditions and Test Procedures for Airborne Equipment. Sections 15 to 23 of this standard detail specific requirements for demonstrating equipment EMC compliance. The standard is similar in intent to MIL-STD-461E, but is not as rigorous in some areas. DO-160E provides the opportunity to apply minimal immunity requirements to some aircraft systems, which may result in MC equipment being afforded little protection from EMI. Where this standard is proposed for use by contractors, POs/SPOs should be aware of the test "Category" applied to each piece of equipment, and ensure that this is satisfactory depending on the system criticality and application. Information on making this determination is contained within the standard, and SCI-DGTA is available to provide assistance if necessary.

7. FAR/JAR Documents. The requirement for control of E^3 is recognised in FARs/JARs, including reference to RTCA/DO-160E. The requirements, however, lack sufficient detail for military purposes and have only recently been supported by relevant advisory circulars setting out compliance demonstration guidance. In addition, the FAR/JAR requirements do not address any of the military unique requirements of E^3, such as ordnance and the harsher EMEs likely to be encountered by military aircraft. While the different aspects of E^3 control requirements are mentioned, the actual compliance methodology, limits for testing and analysis methodology are not well addressed. As such,

application of FAR/JAR requirements should only be considered in cases where the aircraft has been certified to FAR/JAR regulations and will adopt a strictly ‘civil’ role (eg. the ADF’s VIP fleet).

AIRCRAFT LIGHTNING IMMUNITY GUIDANCE

1. Lightning strikes on ADF aircraft are a common occurrence and have the potential to cause damage to the exterior of an aircraft as well as internal equipment. Effects such as burning, eroding, blasting and structural deformation are known as the direct (or physical) effects of lightning. The internal (or indirect/electromagnetic) effects can include damage to onboard systems from the fields associated with lightning and the interaction of these fields with structures and equipment within the aircraft. Indirect effects can also occur from a lightning strike near the aircraft. Aircraft are designed and fitted with numerous lightning protective measures, and provided that these are maintained appropriately, safety hazards due to lightning strikes are minimised. This annex provides guidance to SPOs on ensuring that the effectiveness of lightning protection measures are retained following aircraft modifications.

LIGHTNING QUALIFICATION

2. New aircraft acquired by the ADF will usually have lightning protection designed and tested to an appropriate standard. Once aircraft are in service, SPOs will mainly be concerned with two aspects of lightning protection – ensuring that the lightning discharge path remains effective following any design changes to the platform, and that new equipment has adequate protection from the indirect effects of lightning. For more complex modifications where zoning and modelling activities are required, the standards listed at the end of this annex can be used for guidance. In addition, SCI-DGTA is also able to provide assistance and can call upon DSTO resources for complex activities if required.

3. Lightning qualification activities need to be approached from a hazard analysis standpoint, that considers the physical characteristics of the aircraft, and the criticality of failure of the items affected.

Protection from direct effects

4. The direct effects of lightning can cause burning, eroding, blasting and structural deformation of aircraft. Depending on the zoning characteristics of the fuselage, equipment in some areas can be subject to the full power of a lightning strike, and this can represent a flight safety issue for fuel systems and ordnance. Qualification of direct effect protection of aircraft is thus an important consideration.

5. Any modification to an aircraft's structure has the potential to alter its lightning protection features. Modification projects should focus on maintaining the original qualification level of the aircraft (and hence the protective measures installed). As part of the modification process, contractors/SPOs should examine whether the affected area contains lightning protection features or is part of the lightning discharge path. If so, the designer should ensure that the replacement/modified item will have the same protection properties and/or current carrying capacity to adequately maintain the aircraft's immunity.

6. **Lightning strike zones.** The surface of an aircraft can be divided into a set of lightning strike zones which represent the areas likely to experience the various types of lighting currents and components of the lighting environment. An awareness of the lightning strike zones will be most important for those modification activities involving equipment at the extremities of an aircraft, which are those most vulnerable to lightning strike (eg. installation of new antenna or CMDS system close to the nose of aircraft). Refer to the standards section below for a list of applicable documents on zoning.

7. **Lightning discharge path.** In order to effectively dissipate currents from lightning strikes, most aircraft have a low-impedance lightning discharge path. This path runs from the extremities (nose, outer wing/rotor blade areas etc.) of the aircraft (the most likely area of the airframe for lightning strikes) to the rear of the aircraft, leading the induced currents away from fuel and ordnance systems. Organisations undertaking airframe modifications must be mindful to preserve the lightning discharge path (eg. adequate bonding must be implemented; new composite panels within the discharge path must contain sufficient conductive material to carry the expected currents). Further, maintenance personnel need to ensure the ongoing effectiveness of the lightning discharge path as part of routine maintenance (and maintaining the overall E^3 protective measures of the aircraft). Lightning has the potential to also cause damage to the discharge path following a strike. As a result, maintenance personnel should perform an inspection of the lightning discharge path following a lightning strike event and repair any damage to ensure that it remains effective for future lightning strikes.

Protection from indirect effects

8. Even if lightning strikes do not directly contact the aircraft electrical wiring and internal structure, strikes to the aircraft are capable of inducing voltage and current surges into internal areas. This also holds true for the changing electromagnetic field produced by a nearby lightning flash that does not directly strike the aircraft. Damage to SOF avionics subsystems from the indirect effects of lightning are of greatest concern, followed by avionic sub-systems that have externally mounted fixtures such as air data probes, heaters, actuators and antennas. Ideally, aircraft internal equipment will be appropriately EMI hardened to withstand the effects of lightning strikes. Additionally, internal equipment relies on shielding and protection from airframe components. Any changes to external panels or other parts of the aircraft structure should take into account the level of protection offered to internal equipment in order to ensure that existing protection features are not degraded.

9. Specifying an appropriate equipment-level E^3 standard (eg. MIL-STD-461, DO-160) will normally provide assurance that equipment will be able to withstand the indirect effects of lightning, providing that key conducted susceptibility tests are not tailored. Engineers should initially assume that the full extent of indirect lightning testing will be needed on any internal equipment or fixtures. This requirement should then be diluted on the basis of:

a. the assigned criticality (ie. SOF, fuel systems, MC or other);

b. the installation location on the aircraft and the assigned lightning strike zone;

c. the physical location and type of earthing sub-system employed;

d. the properties of the surrounding areas to installation location; and

e. previous qualification of the sub-system, and the appropriateness of the test standard.

10. If uncertainty exists as to the risk posed by the indirect effects of lightning, a full analysis should be carried out to aid in determining the level of testing required.

LIGHTNING-RELATED STANDARDS

11. Aircraft manufacturers will normally specify lightning standards for new aircraft. For modification projects, SPOs should specify the continuing use of this original lightning standard unless it is unsuitable for the change being undertaken or has been superseded by a more applicable standard. Where the original lightning design standards for aircraft or equipment are unknown, the following paragraphs provide some guidance.

12. MIL-STD-461E. Requirements CS114, 115 and 116 from MIL-STD-461E are often used as a de-facto standard for lightning indirect effects testing of equipment. When equipment is tested to MIL-STD-461E, these tests should be specified in order to ensure that the item is able to withstand indirect effects.

13. MIL-STD-464A. This standard provides guidance on requirements relating to the direct and indirect effects of lightning and draws on a combination of military and civil aircraft documents. It is sufficiently comprehensive to use as a standalone document to satisfy all lightning requirements for ADF aircraft.

14. Civil standards. While the standards listed above should be sufficient for most ADF acquisitions and modifications, the following provide additional information on the approach, tools and processes used for the certification of civil aircraft.

a. RTCA/DO-160E (Environmental conditions and test procedures for airborne equipment). Section 22 of DO-160E contains equipment testing requirements for the indirect effects of lightning, while Section 23 contains tests to determine the ability of externally mounted equipment to withstand the direct effects of a lightning strike. Note that DO-160E Section 22 is more stringent than the corresponding MIL-STD-461E test, as it requires up to three times as much current to be induced into the equipment to meet the pass criteria.

b. FAA AC 20-136A (Protection of aircraft electrical/electronic systems against the indirect effects of lightning). This AC contains information and approaches for the protection of aircraft systems and a means of demonstrating compliance with FARs 23, 25, 27 and 29.

c. **FAA AC 20-53B (Protection of aircraft fuel systems against fuel vapour ignition caused by lightning).** The AC and its user manual (DOT/FAA/CT-83/3) provide guidance for the protection of fuel sub-systems from both the direct and indirect effects of lightning. Both traditional metal and composite construction techniques are addressed by the AC.

d. **FAA-endorsed SAE lightning standards.** The following related standards are referenced in a number of FAA ACs and may be used to demonstrate compliance to the FARs. These standards define lightning threats to aircraft, along with the tests required to support the lightning protection aspects of aircraft certification:

(1) SAE ARP 5412 (Aircraft lightning environment and related test waveforms),

(2) SAE ARP 5413 (Certification of aircraft electrical/electronic systems for the indirect effects of lightning),

(3) SAE ARP 5414 (Aircraft lightning zoning), and

(4) SAE ARP 5415 (User's manual for certification of aircraft electrical/electronic systems for the indirect effects of lightning).

e. **SAE ARP 5577 (Aircraft Lightning Direct Effects Certification).** SAE ARP 5577 provides guidance for complying with regulations relating to the direct effects of lightning for conventional aircraft design, as well as those with composite structures or other new technologies. This standard applies to both initial designs and modifications. While not referenced in FAA documents, the information within may provide valuable reference material for modifications.

Blank Page

INTRASYSTEM TESTING

1. Intrasystem (or source/victim) testing is carried out to check the E^3 compatibility between aircraft systems following the integration of new equipment. Given the emphasis and effort that should have been put into the first three building block steps (equipment level qualification and application of design/integration/installation principles), this testing should be considered as a confidence check in the EMC of the aircraft to ensure that nothing has been missed in the prior steps. The extent of intrasystem testing that needs to be carried out will depend on the systems being modified and is usually more comprehensive where SOF systems are involved.

2. The scope of intrasystem testing should include checks that:

a. modifications do not affect existing SOF/MC systems,

b. existing systems do not affect the modification, and

c. the modification does not permit coupling of existing systems to each other, particularly SOF/MC systems.

3. The aim of this annex is to provide POs/SPOs with information to assist with generating and/or reviewing intrasystem test matrices and plans. This advice should be read in conjunction with chapter 2 to ascertain the context and extent of source/victim testing required.

4. Comprehensive intrasystem testing is very manpower intensive and time consuming. POs/SPOs must determine how much intrasystem testing they can afford to carry out given the limited time available in the project schedule. A balance must be struck between obtaining a satisfactory level of assurance that SOF systems are not affected by changes (beyond that provided by the design analyses) and testing every operating mode/frequency of every system onboard the aircraft. Given the differences between all fleet aircraft, intrasystem testing (which is normally carried out on only one aircraft) can not be regarded as a comprehensive means of checking for problems.

5. Prior to intrasystem testing, PO/SPO staff should perform a confidence check of the first three E^3 building-block steps as described in chapter 2. If these steps were carried out satisfactorily, the level of source/victim testing can be tailored with a high degree of confidence. Alternatively, if these initial building block steps were not performed well, the PO/SPO/contractor should revisit these areas rather than attempt to obtain confidence in the modification by performing an extensive intrasystem testing program over many weeks or months.

GENERATING SOURCE/VICTIM TEST MATRICES

6. Modern aircraft have a large number of electronic systems, which can result in very large source/victim matrices if all systems are included for testing. Projects will rarely have sufficient time to test every source/victim combination, hence a risk-based approach must be taken when generating a test matrix. The aim should be to minimise the duration of the test program while ensuring an adequate level of safety.

7. The process described in the paragraphs below can be used to generate an intrasystem test matrix appropriate to the extent of the modification and available timeframe. When generating the intrasystem test plan, the number and order of test points should be generated to ensure that (in priority order):

a. the safety of the aircraft has not been adversely affected (SOF systems),

b. MC systems still operate effectively,

c. the modification does not introduce any problems into non-SOF/MC aircraft systems and is not a victim of existing systems itself, and

d. no other EMC problems have been introduced into the remaining systems.

8. Initially, a complete listing of all aircraft systems should be compiled and placed into a matrix, each as both a source and a victim. With the priorities from paragraph 7 in mind, the number of test combinations in the matrix can be progressively reduced by assessing the risk of not carrying out each source/victim pair.

9. If there is no clear coupling path (either conducted or radiated) between two systems in the source/victim matrix, this test combination can be removed. A similar approach can be taken for any source/victim combinations that operate in different parts of the frequency spectrum (including related harmonics) or at field levels that are unlikely to result in interference problems. Likewise, if a source/victim combination is unlikely to ever occur during aircraft operation, it should be removed from the matrix.

10. For complicated source/victim matrices, 'active' and 'passive' classifications may be applied to systems in order to streamline testing. In general terms, an 'active' source/victim will have its functionality comprehensively exercised against other systems, while a 'passive' source/victim may be run collectively with other systems and observed for abnormalities in its operation. This methodology will reduce the number of test points that need to be carried out while exercising all necessary systems. An example of a source/victim matrix is included at appendix 1.

11. Testing considerations. Each of the remaining source/victim combinations should then be sequentially tested against each other, and observed for any signs of electromagnetic interference. For systems with many operating modes, such as radios, multiple test points will need to be determined for each applicable source/victim combination. To ensure adequate testing coverage of such systems, technical and/or operational personnel as appropriate should be consulted to determine important or frequently-used operating modes. Given the large tuneable range of radio systems, it should be established with operators whether any part of the spectrum or discrete frequencies for each radio system are used exclusively, or alternatively whether any parts of the spectrum are avoided or not used at all. Unless there are existing EMI problems with radios, testing large frequency ranges should be avoided unless there is a belief that the modification is likely to cause interference or to have permitted coupling to a radio system. Where applicable, focus should also be placed on testing frequencies that are harmonics of other onboard systems to check for unwanted coupling. Emergency frequencies should also be given priority for testing.

12. Baseline testing. If the opportunity arises, and the resources are available, performing a baseline intrasystem test on an unmodified aircraft will provide an excellent reference. This is particularly the case if the Commonwealth needs to hand over an aircraft to a contractor for modification. Providing a copy of the baseline to the contractor may assist in determining whether E^3 problems following a modification are attributable to the changes, or whether they were pre-existing problems.

13. Production testing. In some cases, contractors may have a program in place to carry out production testing of new or modified aircraft as they are manufactured or modified. This testing can be used as a tool to identify shortfalls with production methods and provides a greater level of confidence in the intrasystem compatibility of the aircraft fleet. Production testing will involve only a small subset of all tests carried out during the initial intrasystem test program, and will usually target the SOF systems. POs/SPOs should determine whether the contractor has a production testing program in place for their program, and if not consider whether one is required.

Appendix:

1. Example of F/A-18 (Dual and Single Seat) source/victim matrix

EXAMPLES OF A F/A-18 (DUAL AND SINGLE SEAT) RAAF SOURCE VICTIM TEST MATRIX

SOURCES: Aircraft Safety of Flight and Mission Critical Equipment

LEGEND

- SOURCE SUBSYSTEMS FOR F/A-18A EMC TESTING
- QUALIFIED BY DESKTOP AUDIT
- 81WG SAFETY OF FLIGHT SUBSYSTEM
- ACTIVE SOURCE - ACTIVE VICTIM
- ACTIVE SOURCE - PASSIVE VICTIM
- TEST NOT APPLICABLE

VICTIMS: Aircraft Safety of Flight & Identified Mission Critical Equipment

SOF SUBSYSTEM

- Amplifier Control, Intercom (ACI)
- Communication System Control (CSC)
- COMM 1 (VHF/UHF), ARC-210
- COMM 2 (VHF/UHF), /ARC-210
- Comm 1 Transmit Switch (aft cockpit)
- Comm 2 Transmit Switch (aft cockpit)
- Landing Gear Down Tone of VHF/UHF Radio
- Air Data Computer (ADC)
- CIT, APX-111(V)
- Embedded GPS INS (EGI), AN/ASN-174
- Magnetic Azimuth Detector (MAD)
- VOR/ILS, AN/ARN-514
- TACAN
- EEDs, BRU-32/33 and LAU-116 (CCU-44/45)
- Stores Management System (SMS), AYQ-9
- SUU-20/5003 B/A
- Head Up Display (HUD), AN/AVQ-28
- Horizontal Indicator (HI)
- Digital Display Indicator (DDI)
- Digital Display Repeater Indicator (DDRI), (aft cockpit)
- Up Front Control (UFC)
- Up Front Control Panel (UFC), (aft cockpit)
- Seat/Canopy
- Seat (aft cockpit)
- Standby Instruments (aft cockpit)
- Standby Instruments
- Caution Lights
- Caution Lights (aft cockpit)
- Warning/Advisory Lights
- Warning/Advisory Lights (aft cockpit)
- Mission Computer 1 & 2 (MC), XN-8+
- External Probe Heaters
- Anti-skid/Brakes
- Arresting Hook
- Flight Control System (FCS)
- Flaps
- Rudder Trim
- Speed Brake
- Landing Gear
- Nose Wheel Steering (NWS)
- Wing Fold System
- Electrical Generators/Electrical System
- Environmental Control System (ECS)
- Avionics Undercool Warning
- Bleed Air Leakage Detect System
- Fire Detection
- Fuel System
- Engine Performance Indicator (EPI)
- Engines/APU

- Radar (APG-73)
- Enhanced Interference Blanking Unit (EIBU)
- Jammer, ALQ-126B

Crash Data Recorder
ICS Panel (aft cockpit)
HF Radio, RT-1448/ARC-200
HF Encryption, KY-75
VHF/UHF Encryption, KY-75
Automatic Direction Finding (ADF)
KIV-8
Radar Altimeter (RADALT)
Forward Looking Infrared (FLIR) AN/AAR-38A
M61A1 Gun
Radar (APG-73)
Countermeasures Dispenser (ALE-39)
Jammer, ALQ-126B
Enhanced Interence Blanking Unit (EIBU)
Radar Warning Receiver (RWR) AN?ALR-67(
Video Recording System
Control Panel Video Recorder
Memory Unit (MU), ASQ-194
Nose Wheel Well DDI (NWWDDI)
Maintenance Signal Data Recorder Set (MSD
External Lights
Internal Lights
Inflight Refueling Probe
Cockpit Video Recording System
Wind Shield Rain Removal/Anti-Ice

Blank Page

ESTABLISHING THE REQUIREMENT FOR INTERSYSTEM TESTING

1. Intersystem EMC relates to the ability of an aircraft to operate successfully in its worst-case operational EME. Intersystem testing involves radiating the aircraft with EM radiation from varying aspects to replicate the aircraft's operational EME. Attempting to test the full EME is difficult due to the limitations of the test equipment in trying to replicate power levels, modulations, pulse densities etc. Hence, as with intrasystem testing, intersystem testing provides a limited 'check' (rather than complete confidence) of an aircraft's compatibility. As per the building-block approach described in chapter 2, the emphasis should be placed on equipment level testing, sound design/installation strategies and some intrasystem testing in order to provide confidence in the EMC of the aircraft.

2. There is currently no comprehensive E^3 intersystem testing facility in Australia and the only option available to POs/SPOs for this type of testing is to choose from a number of overseas facilities. Intersystem testing is thus very expensive (costing millions of dollars per test program) and requires aircraft, personnel and other resources to be deployed from Australia for extended periods of time, therefore this testing is rarely conducted on ADF aircraft. The decision to perform intersystem testing should be made on a case-by-case basis using a risk-based assessment of the aircraft design or applicable changes.

3. When to perform intersystem testing. There are four common cases where the resources required for intersystem testing may be justified:

a. where additional intersystem testing is required (beyond that carried out by the OEM) during the acquisition of an aircraft;

b. for large scale modifications, especially if SOF systems are affected;

c. there is a requirement to employ an aircraft in an EME that is significantly more harsh than its original qualification (or the qualification EME is unknown); and

d. periodic retesting over the service life of an aircraft to either provide confidence that the E^3 protective measures remain effective, or the EME immunity of the aircraft is questionable.

4. To obtain the most benefit from testing, the operating EME of the aircraft should be well defined and understood so that appropriate test parameters can be generated. Prior to undertaking intersystem testing, the selected EME should also be reviewed to ensure continued relevance to the aircraft's configuration, role and operating environment. Some ADF aircraft will have been qualified to an EME from a standard, OEM document or other source, while older aircraft may not have been qualified against an EME (or this EME may have become outdated). In the latter case a revised EME will be required if testing is to be carried out.

5. If an EME derived from a standard or other source is inappropriate, or an aircraft has a unique EME, DSTO may be able to provide assistance. Under a DGTA-sponsored research task, DSTO have generated a number of EMEs for various ADF aircraft types based on commercially available emitter data. For enquiries on these DSTO-generated EMEs contact SCI-DGTA in the first instance.

6. In addition to the EME determination, POs/SPOs must also be aware of the aircraft systems that require testing. As with intrasystem testing, the focus should be on ensuring the ongoing safety of the aircraft by testing SOF and, where appropriate, MC systems.

7. Acquisition testing. The ADF will normally acquire aircraft that are able to meet EME requirements, and the testing carried out by the manufacturer will usually adequately demonstrate compliance. In some cases though, this testing may not be adequate due to the ADF requirement to operate the aircraft in a different EME (eg. Army troop-lift helicopter operating from Navy ship) or a significant modification (eg. civilian airliner conversion to AEW&C platform). In such cases, the PO may need to include additional intersystem test requirements in the contract. The extent of the shortfall in EME testing will determine whether a small number of test points can be added to the initial test program (eg. addition of several Navy ship emitter parameters) or whether a more extensive program will need to be undertaken (eg. complete requalification of the aircraft due to significant structural and SOF system modifications).

8. Complex/SOF system modification. Major changes to an aircraft's configuration have the ability to introduce E^3 problems. For example – changes to SOF/MC systems may have an impact on the ongoing safe operation of the

aircraft, changing structural components may alter the E^3 protection provided for some aircraft systems, and significant wiring changes have the potential to introduce unwanted coupling paths.

9. Where large scale modifications are carried out (particularly those affecting SOF systems), requalification of the aircraft's intersystem EMC may be required. The PO/SPO should carry out an analysis of the changes and determine which systems are affected (either directly or indirectly) and the likely effects on the aircraft EME immunity. As part of this analysis, an examination of the equipment qualification, design/installation techniques and intrasystem test results should be undertaken to gauge the likely impact on EME immunity from the changes.

10. Compliance with existing design/installation/protection techniques should also be examined. Continuing to use these techniques should ensure that the aircraft's immunity is maintained following the modification. However, if the EME immunity of an aircraft (particularly older aircraft) is unknown and/or the E^3 protective measures have not been well maintained, it may be difficult to confirm continued immunity via analysis. Contact SCI-DGTA if assistance is required.

11. Change of EME. Intersystem testing may be required if a significant change to the operating EME of an aircraft is planned (eg. embarkation of a previously-unqualified Army helicopter on a Navy ship). If this EME is beyond the original qualification EME of the aircraft (or the original qualification EME is unknown, particularly for an older aircraft) there may be uncertainty as to whether the aircraft will be able to operate safely.

12. Periodic testing. Many years of aircraft operation, minor modifications, maintenance actions and general wear may have an effect on the EME immunity of an aircraft. If modifications have been carried out in accordance with existing E^3 installation and protection techniques, and these protective measures have been adequately maintained, there should be little impact on the EME immunity of the aircraft. In cases where an aircraft type's immunity is in question, analysis and inspection should be carried out to check the state of the E^3 design features of the aircraft, whether past modifications were carried out in accordance with existing E^3 practices, whether equipment meets appropriate E^3 standards etc. Targeted source/victim testing may also assist in solving problems. Should none of these measures provide adequate confidence in the EME immunity, intersystem testing may be warranted.

13. Post-testing. Intersystem test facilities are in high demand and once test programs are completed, there is usually no provision for the test organisation to provide assistance in interpreting or resolving problems discovered during testing (unless specialist assistance is specifically included in a contract). POs/SPOs (or contractors) should therefore be prepared to interpret the results in the test report and make a decision on whether the problem is sufficiently serious to require aircraft modification or whether a workaround can be formulated. The PO/SPO must ensure that sufficient detail is provided in the test report to support this decision.

E^3 CONTROL PROGRAM PLAN REQUIREMENTS

1. As discussed in chapter 2, there may be cases where a PO/SPO will require detailed disclosure of a contractor's E^3 Control Program (E^3CP), or to generate such information when acting as a design integrator. The E^3CP consists of all design, testing, integration and installation activities relating to E^3 aspects of the acquisition/modification and is disclosed through the E^3 Control Program Plan (E^3CPP). This document provides a means for contractors and the Commonwealth to establish the requirements of the E^3CP early in the design stages, and should be updated as the design matures to reflect the final state of the acquisition/modification design.

2. This annex describes the information that should be detailed in the E^3CPP, including management policies, design philosophies and the technical approach to be used by the contractor/PO/SPO. Information and guidance from the main body of this chapter should also be referred to when compiling the E^3CPP. For modifications, the plan should detail all activities related to the new equipment as well as the interface to the existing systems. In addition, any information relevant to the existing equipment E^3 qualifications or design philosophies should also be included. The E^3CPP should be broken into two major sections: 'Management Requirements' and 'Technical Requirements' as detailed below.

E^3CPP MANAGEMENT REQUIREMENTS

3. The Management Requirements section of the E^3CPP should provide an outline of the plan, followed by a clear description of the proposed management framework for the E^3CP. The following topics should be addressed as a minimum:

a. **Document overview and use.** This paragraph should summarise the purpose and contents of the E^3CPP and describe any security or privacy considerations associated with its use;

b. **Scope.** This section should fully identify the items to which the E^3CP applies and extent of the program;

c. **Applicable documents.** All applicable/referenced documents used in the E^3CP should be listed, including standards, contractor documents etc. This listing should include the title, revision status and issue date for each document;

d. **Definitions, acronyms and abbreviations.** Definitions, acronyms and abbreviations used in the E^3CPP should be listed as appropriate;

e. **Management.** The E^3CPP should describe the management aspects of the Program, including the following:

(1) the companies, departments and all sub-contractors involved in the E^3CP, including the relationships between each;

(2) details and relevant experience of the key personnel that will be involved in the E^3 Program, including the E^3 Control Program manager and Design Engineers;

(3) identification of the responsibilities and authorities for planning, implementing and managing the E^3 aspects of the design; and

(4) details on the interface between the contractor and the Commonwealth on E^3 issues (eg. Commonwealth design requests, documentation to be supplied, design review feedback etc.).

f. **E^3 Control Advisory Board (E^3CAB).** Details such as the role, responsibilities and composition of the E^3CAB should be listed in the E^3CPP (see chapter 2 for further details on the E^3CAB).

E^{3}CPP TECHNICAL REQUIREMENTS

4. The Technical Requirements section of the E^{3}CPP should provide a detailed technical plan on how the E^3 airworthiness requirements of the acquisition/modification are to be met. The areas addressed should include at least the following, along with any other items deemed relevant:

a. **Electromagnetic environment (EME).** Provide details of the selected EME, including how it was derived (from an E^3 standard, OEM-derived, DSTO analysis etc.);

b. **Aircraft equipment.** An outline of the equipment and items covered under this plan should be provided, along with a basic outline of the company philosophy on E^3 control practices:

(1) **Criticality categories.** The E^{3}CPP should provide a list of all new equipment and sub-systems, along with a brief description of function, and should assign each a criticality category based on a systems safety assessment (eg. category I for SOF, category II for MC and category III for all other sub-systems). This list should be provided to the Commonwealth for acceptance prior to commencement of any system integration or testing;

(2) **Sub-system location.** The E^{3}CPP should describe the proposed layout of equipment to be installed or relocated. In particular, justification for the equipment locations, and how EMI/EMC problems will be minimised or mitigated as a result of the proposed locations, should be provided;

(3) **Equipment level qualifications.** The E^{3}CPP should define the established E^3 requirements for each of the new equipment and sub-systems, based on their assigned criticality. The reasons for use of the selected test standard (eg. MIL-STD-461E, RTCA/DO-160E), including details of all tailoring, test categories, additional testing requirements and waivers, should be provided;

(4) **Margins.** For systems classified as either SOF, MC or ordnance, safety margins should be applied to account for equipment and aircraft manufacturing and installation tolerances. Reasoning should be provided for the margin values selected; and

(5) **Developmental items.** The process used to design, test, integrate and install any developmental items in the aircraft should be detailed.

c. **Design concept.** The E^{3}CPP should describe the overall aircraft design concepts that have been implemented to address E^3 requirements. This section should include an appraisal of the identified E^3 risks, along with specific information on the E^3 mitigation strategies incorporated during design and development. These design concepts should be transferred into maintenance procedures/publications to ensure that EMI mitigation features of the design are adequately maintained throughout the aircraft life. The following should be included in the E^{3}CPP:

(1) **Electrical bonding.** The E^{3}CPP should detail the bonding and grounding provisions to be implemented to demonstrate compliance with E^3 requirements (power current return paths, shock hazards, antenna performance, electrostatic charge control, external grounds etc.);

(2) **Shielding.** Details of all shielding used for circuits, wiring, joints etc. should be provided, in addition to information on natural shielding provided by the airframe and other aircraft components;

(3) **Corrosion control.** The E^{3}CPP should detail the system corrosion control plans and how they will assist with meeting E^3 requirements;

(4) **Wiring.** The E^{3}CPP should detail the E^3 design approach for electrical cabling installation, including wiring categorisation, shielding techniques, labeling, shield terminations, wire routing and wire separation;

(5) **Antenna installations.** If antennas are to be installed, details on function, design, bonding and intended location should be provided. This section should be populated when new antennas are to

be installed or existing antennas are to be moved and should contain a justification on the selected physical locations, along with test results that demonstrate the suitability of the proposed antenna locations from an EMC and performance perspective;

(6) **Lightning.** The E^{3}CPP should detail the contractor's design criteria and philosophy as to how they intend to protect against the direct and indirect effects of lightning strikes, addressing zoning, standards applied, protection measures, details of proposed testing etc.;

(7) **Electrostatic charge and precipitation static (p-static) control.** The design techniques used to prevent p-static problems with the aircraft should be provided. If p-static testing is proposed, test plans, test procedures/preparations, facilities, approval processes and risk mitigation activities should be detailed;

(8) **Shock and fault protection.** Information on shock and fault protection measures should be provided;

(9) **Electromagnetic radiation hazards (EMRADHAZ).** The E^{3}CPP should detail the approach taken for the control of radiation hazards to personnel, fuel and ordnance. The E^{3}CPP should identify any potential hazards and detail the measures proposed to mitigate these.

(i) **Hazards of electromagnetic radiation to personnel (HERP).** The E^{3}CPP should encompass the requirements relating to the mandated ARPANSA standard as detailed in chapter 2. Details of analyses performed to determine minimum safe distances from transmitters should be provided. For modifications that add intentional emitters, details of the verification activities to requalify aircraft safety distances should be given;

(ii) **Hazards of electromagnetic radiation to fuel (HERF).** Design techniques to avoid HERF issues should be provided; and

(iii) **Hazards of electromagnetic radiation to ordnance (HERO).** Where HERO aspects are applicable, POs/SPOs should check with GWEO, DOS and/or ASCENG-AOSG as applicable to ensure that the approach proposed by a contractor meets Commonwealth requirements. Where the Commonwealth is acting as the design integrator, these organisations should be consulted for assistance with the design.

(10) **EMSEC (TEMPEST).** If applicable to the acquisition/modification, details of EMSEC design and test considerations or requalification should be provided. POs/SPOs should ensure that any additional requirements recommended by 462SQN are also included in the Plan;

(11) **Emission control (EMCON).** If applicable, this section should detail how EMCON design and test requirements are to be met;

(12) **EMP.** If applicable, this section should detail how EMP design and test requirements are to be met;

(13) **EM spectrum compatibility.** Considerations of RF interoperability of aircraft systems and impact from external transmitters on aircraft receivers should be included if applicable;

(14) **Lifecycle hardness.** The E^{3}CPP should detail design features of the aircraft/modification that contribute to E^3 lifecycle hardness. This section should also include any maintenance or periodic testing activities required to maintain the E^3 protective measures for the life of the aircraft; and

(15) **New/unproven techniques.** Special and unproven E^3 control techniques should undergo validation before the applicable item is assembled and integrated. The E^{3}CPP should describe any special testing that will be conducted to demonstrate the compliance of the item with E^3 requirements and/or to investigate the effectiveness of the proposed technique. Test results should be included in the E^{3}CPP as they become available. Any use of E^3 software prediction tools as part of a system assessment should also be disclosed, noting the guidance in chapter 2 that software tools are not to be used as a substitute or alternative for testing.

d. **Testing.** The contractor will need to plan, define and perform tests and analyses to verify the compliance of the aircraft/modification with the E^3 requirements set out in the SOW. This section of the E^3CPP should detail the responsibilities for testing, test facilities to be utilised, scope of testing to be carried out and the physical configuration that the aircraft will be tested in (ie. prototype state or representative of production aircraft). The following items should be included in the E^3CPP as a minimum:

(1) **Test responsibilities.** Details should be provided of the agency and personnel (along with their qualifications) responsible for generating test procedures and conducting E^3 testing. Additionally, the level and amount of involvement of contractor personnel in testing at the selected facility should also be detailed (eg. contractor will witness or participate in tests);

(2) **Facilities.** The E^3CPP should detail the facilities that will be used for E^3 testing, including the resources available. Information should be provided on the type and capabilities of the facilities (eg. anechoic chamber, open area test site) and accreditations of the facilities (eg. NATA) to be utilised for all types of testing (eg. intersystem, intrasystem, sub-system and equipment qualifications). Additionally, any inability of the facilities to meet the EME or E^3 standard required for testing should be detailed, along with a plan for how the contractor is to demonstrate compliance with Commonwealth requirements;

(3) **Intrasystem EMC testing.** The E^3CPP should detail the approach to be used to ensure intrasystem electromagnetic compatibility, including the testing and/or analysis to be performed on systems to ensure compatibility. The E^3CPP should reference the intrasystem test plan and report;

(4) **Intersystem EMC testing.** The requirement for (and extent of) intersystem testing will depend on the type of acquisition or risk associated with a modification. The proposed scope and details of intersystem testing should be provided in this section of the E^3CPP. Alternatively, if testing is not proposed, details of the strategy to be employed to assure the continued immunity of the aircraft should be provided;

(5) **Lightning immunity testing.** New aircraft types will usually have lightning immunity testing carried out as part of their development, while the requirement for this testing to be carried out for modification projects will vary depending on the extent of the changes. Details of the proposed testing (or testing already carried out) should be provided in the E^3CPP. If testing is deemed to be unnecessary, details of the strategy to maintain the lightning immunity of the platform should be provided in the design area of the document;

(6) **P-static testing.** For modifications that involve the installation of antennas or changes to the exterior surfaces of aircraft, p-static testing should be carried out. Details of testing carried out or proposed by a contractor should be included;and

(7) **Other testing carried out.** Information should be provided on any other tests to be carried out (eg. EMSEC, EMCON etc.).

e. **Documentation requirements.** All documentation relevant to the E^3CPP should be referenced in the plan. Such documentation includes E^3 design documents, standards, test plans, test procedures, test reports etc. Refer to chapter 2 for further details.

PLAN FOR E^3 ASPECTS OF CERTIFICATION REQUIREMENTS

1. When the Commonwealth has a high level of confidence in the E^3 skills of a company, there will usually be no need to request detailed information on the E^3 design and management aspects of the project. In cases such as these, the PO/SPO will just need to ensure that they have sufficient information to carry out the compliance finding activities against the E^3 elements appearing in the certification basis. This can be achieved with a Plan for E^3 Aspects of Certification (PE^3AC) rather than the more detailed E^3 Control Program Plan.

2. Where possible the PE^3AC should make reference to the contractor's processes, design and test documents rather than including large amounts of information on how the contractor is conducting their E^3 management activities. This will ensure that the documentation burden on the contractor is maintained at an appropriate level and that the Plan continues to be useful to the Commonwealth. The information recommended for inclusion in a PE^3AC is described below.

3. **Scope.** This section should include:

a. an overview of the E^3 aspects of the aircraft acquisition/modification;

b. details of the focus areas of the design (eg. equipment compatibility, RADHAZ, TEMPEST, lightning protection etc.);

c. the platform's operational EME;

d. company philosophies on systems classification (SOF/MC/other);

e. a list of related plans/documents (eg. E^3 standards, design documents, test plans, maintenance publications, test reports); and

f. for modifications, provide details of E^3 standard(s) used for previous aircraft certification and reference the original E^3 design principles employed (eg. by reference to acquisition project E^3 documentation or company design processes/documents).

4. **E^3 standards.** Provide an outline of the proposed standards (and tailoring, if applicable) to be used for equipment level qualification, equipment design/installation/integration (ie. bonding, p-static, wiring, RADHAZ etc.) and system testing.

5. **E^3 design, installation and integration principles.** A brief outline of the E^3 design, installation and integration principles should be provided keeping detailed technical aspects to a minimum. Where a related document provides detailed information, or existing company design philosophies are to be used, these should be referenced to ensure that the PE^3AC does not become too lengthy or detailed.

6. **E^3 testing.** Briefly outline the details and extent of the testing to be carried out, including equipment level, intrasystem and, if applicable, intersystem testing. Also include coverage of other testing to be performed if applicable (EMCON, TEMPEST, p-static etc.). The testing organisation and their accreditation/qualification details should be included in the PE^3AC. Where possible provide a reference to the test plan(s) as a source of more detailed information.

7. **Test results.** A summary of test results (or reference to test reports and other relevant documentation) should be provided. The PE^3AC should list details of any test non-compliances and the corresponding fixes, mitigations, workarounds etc. recommended by the company.

Blank Page

SECTION 2

CHAPTER 3

GENERAL AVIONICS SYSTEMS

INTRODUCTION

1. This chapter provides general avionics systems requirements for ADF aircraft to supplement common civilian and military standards. In addition, where state aircraft are required to interface with civilian aircraft and Air Traffic Management (ATM) systems, current and likely future functional requirements are included.

COMMUNICATION, NAVIGATION AND SURVEILLANCE SYSTEMS

Background

2. While State aircraft are exempt under International Civil Aviation Organisation (ICAO) rules from complying with civil aviation requirements, it will now become increasingly more difficult (in some cases state aircraft will not be exempt) for civilian air traffic authorities to cater for ADF aircraft if they are not capable of similar CNS performance to civil aircraft. This may result in ADF aircraft being subjected to civilian airspace restrictions, for example non-optimal altitudes (restrictions or possible exclusion), sub-optimal routing and increased flight times. These restrictions may have financial, operational and political implications for the ADF.

3. DI(G) OPS 40-3 – *Implementation of Aviation Communication, Navigation and Surveillance and Air Traffic Management Initiatives in the Australian Defence Force* promulgates policy on the implementation of CNS/ATM capabilities/initiatives in the ADF. This Defence Instruction details the process for identifying the requirement for, and method of implementing, a CNS/ATM capability. ACPA-ADF Airworthiness Advisory Circular (AAC) 008 provides further guidance on the process for the operational approval of CNS systems. CNS/ATM requirements for ADF aircraft are influenced by operational requirements to operate in various airspaces and the need to interface with the civilian ATM environment. This latter requirement is now gaining prevalence, as a result of the rapidly expanding civil aviation industry and the consequent increase in complexity for the civilian ATM system. The need to install these systems in ADF aircraft is determined by capability managers and will be based upon an assessment of the suitability of available equipment and the operational ramifications of relying on alternate strategies (such as waivers and exemptions).

Communications Systems

4. This section presents a number of military and civilian standards acceptable for ADF communication systems and also highlights future considerations with respect to communication systems.

5. ***Communications Minimum Performance.*** Each of the standards below details performance standards and provide a means of assuring that the systems will satisfactorily perform its intended function:

a. HF Radio:

(1) MIL-STD-188-141B - *Interoperability and Performance Standards for Medium and High Frequency Radio Systems;*

(2) CASA CAO 103.22 Issue 2 - *Equipment Standards – HF Communications Transmitting and Receiving Equipment; and*

(3) RTCA/DO-163 - *Minimum Performance Standards – Airborne HF Radio Communications Transmitting and Receiving Equipment Operating within the Radio-Frequency Range of 1.5 to 30 MHz.*

b. VHF Radio:

(1) MIL-STD-188-242 Revision 85 - *Interoperability and Performance Standards for Tactical Single Channel Very High Frequency (VHF) Radio Equipment;*

(2) CASA CAO 103.24 - *Equipment Standards – VHF Communications Transmitting Equipment*;

(3) CASA CAO 103.25 - *Equipment Standards – VHF Communications Receiving Equipment*;

(4) FAA AC 20-67B - *Airborne VHF Communications Equipment Installations; and*

(5) RTCA/DO-186B - *Minimum Operational Performance Standards for Airborne Radio Communications Equipment*.

c. UHF Radio:

(1) MIL-STD-188-243 Revision 89 - Interoperability and Performance Standards for Tactical Single Channel Ultra High Frequency (UHF) Radio Communications.

6. When defining testing requirements for radio systems, FAA Order 6050.32, *Spectrum Management Regulations and Procedures Appendix 2* provides an extensive set of VHF and UHF performance formulas and graphs for a variety of transmitter/receiver heights and transmitter power outputs. CASA CAO 108.34 – *Specification Airborne Radio Systems Appendix 1* provides some guidance for flight test performance of VHF Communications systems.

7. VHF Channel Spacing. EASA has mandated the adoption of 8.33 kHz channel spacing for VHF communications in some European airspace (refer JAR AGM Section 1 Part 3 Leaflet 7). The reduced Channel separation allows an increased number of VHF channels to be used within the overall bandwidth allocated for aviation purposes. Aircraft without 8.33 kHz spacing VHF radios may be precluded from operating in some European airspace. As such, when acquiring new aircraft or radio systems, the Project Authority should establish whether operations in Europe may be required. If so, EUROCAE ED-23B - *Minimum Operational Performance Standards for Airborne VHF Rx-Tx operating in the Frequency range 117.975 – 136.975 MHz*, provides an acceptable standard for VHF communications which allow receivers and transmitters to be used in both a 25 kHz and a 8.33 kHz channel separation environment. There appears to be no move towards mandating this channel spacing elsewhere in the world, including the USA.

8. Spectrum Management. Special consideration must be given to spectrum management issues during the acquisition of communications equipment. The major issues to consider are safe operation of air systems with ground systems and the legality of operating on intended frequencies. As an example, during trials activity at Woomera ARDU staff determined that Kalkara command and flight termination systems operated on the same frequency as RAAF UHF hand held radios. Also, the legality of operating communication equipment on specific frequencies should be determined in accordance with ADFP 6.0.4 - *Radiofrequency Spectrum Management*. ADFP 6.0.4 is a compilation of policies, management requirements and engineering procedures for efficient and effective use of the RF spectrum within the ADF.

9. Future Civilian Communications Systems. While future civilian communications requirements have not been finalised, they will likely comprise a mixture of SATCOM, VHF and HF radios with digital datalink services to reduce voice transmissions. ICAO has agreed that the primary infrastructure for datalink implementation will be the Aeronautical Telecommunication Network (ATN) based on Internet architectures derived from the Open Systems Interconnection model.

Navigation Systems

10. An aircraft's navigation system may consist of a combination of discrete and integrated navigation components that provide aircrew with guidance information to support flight operations. Example navigation system components include GPS, INS, Doppler, VOR, ILS, TACAN and DME.

11. A navigation systems ability to provide a navigation solution with sufficient ***accuracy, integrity, availability and continuity of service*** is pivotal to safe and effective aircraft operation and mission success. Navigation error is considered to be a combination of Navigation System Error (NSE) and Flight Technical Error (FTE). The integration of navigation systems within aircraft should focus on the reduction of both NSE and FTE. Whereas NSE is generally addressed through the navigation system components and architecture, FTE is addressed through standardisation, reduction in aircrew workload and the implementation of flight automation (such as coupling to autopilot systems and flight sequencing using non-editable aeronautical databases).

12. The following paragraphs provide standards against which the adequacy of navigation systems can be assessed. This assessment needs to be done with cognisance of the aircraft's role - be it strategic or tactical, including the tracking accuracies required.

13. ***Required Navigation Performance (RNP).*** RNP describes the minimum navigation performance accuracy necessary for operation within a defined airspace. The genesis for RNP is ICAO Doc 9613-AN/937 - Appendix E *(Manual on RNP)*. The RNP types specify the navigation performance accuracy (expressed as "X" nautical miles both across-track and along track, eg. RNP 5) within a designated airspace. Although ADF aircraft can still use civilian airspace without having the requisite RNP endorsements, aircraft may be assigned sub-optimal routes, altitudes and flight times. The following CASA and FAA advisory material provide relevant guidance for RNP type approval for civilian aircraft, and therefore present useful comparative standards for ADF aircraft:

a. CASA AC 91U-2(0) – *Required Navigation Performance 10 (RNP10) Operational Authorisation*;

b. CASA AC 91U-3(0) – *Required Navigation Performance 4 (RNP 4) Operational Authorisation*;

c. CASA Civil Aviation Advisory Publication CAAP B-RNAV-1 - *Approval of Australian Operators and Aircraft to Operate under Instrument Flight Rules in European Airspace – (RNP(5) accuracy criteria)*; and

d. FAA Order 8400.12A R*equired Navigation Performance 10 (RNP 10) Operational Approval.*

14. ***Area Navigation (RNAV).*** RNAV is a method of navigation which permits aircraft operation on any desired flight path within the coverage of station-referenced navigation aids or within the limits of the capability of self-contained aids, or a combination of these aids. The following documents detail the minimum performance specifications for area navigation:

a. EUROCAE ED-75B - *Minimum Aviation System Performance Specification (MASPS) Required Navigation Performance for Area Navigation*;

b. RTCA/DO-236B - *Minimum Aviation System Performance Standards: Required Navigation Performance for Area Navigation*; and

c. FAA AC 90-45A - *Approval of Area Navigation Systems for use in the US National Aerospace.*

15. ***Basic Area Navigation (B-RNAV).*** B(asic)-RNAV defines European RNAV operations which satisfy a horizontal track keeping accuracy from a planned position equal to or better than +\- 5 NM for 95% of the flight time (i.e. RNP 5). The following publication and AC should be considered:

a. CASA Civil Aviation Advisory Publication CAAP B-RNAV-1 - *Approval of Australian Operators and Aircraft to Operate under Instrument Flight Rules in European Airspace Designated for Basic Area Navigation*, provides guidance material for the approval of operators of Australian registered civil aircraft and operators of foreign registered aircraft and whose principal place of business is in Australia, operating in Basic Area Navigation environment in the European region; and

b. FAA AC 90-96A – *Approval of U.S. Operators and Aircraft to Operate under IFR in European Airspace Designated for B-RNAV and Precision Area Navigation (P-RNAV).*

16. ***Inertial Navigation System (INS*).** The following standards present appropriate requirements for INS's in ADF aircraft:

a. SNU 84-1 - *Specification for USAF Standard Medium Accuracy Inertial Navigation Unit*; and

b. FAA AC 25-4 - *Inertial Navigation Systems*, provides guidance on the minimum performance criteria for the installed system.

17. ***Multi Sensor Navigation or Flight Management Systems.*** Reliance on discrete navigation aids can unnecessarily limit flight operations due to the difficulty in obtaining satisfactory performance in all four key navigation parameters (i.e. accuracy, integrity, availability and continuity of service) from a single navigation aid. Multi Sensor Navigation or Flight Management Systems that determine aircraft position by integrating data from

multiple navigation sensors can not only improve the accuracy, integrity, availability and continuity of the navigation solution, they can also reduce aircrew workload. The following minimum performance standards for civilian aircraft present useful comparative standards for ADF aircraft:

a. CASA AC 21-37(0) - *Airworthiness Approval of Navigation or Flight Management Systems Integrating Multiple Navigation Sensors*;

b. FAA AC No: 20-130A - *Airworthiness Approval of Navigation or Flight Management Systems Integrating Multiple Navigation Sensors*;

c. FAA TSO C115B - *Airborne Area Navigation Equipment Using Multi-Sensor Input*; and

d. RTCA/DO-187 - *Minimum Operational Performance Standards for Airborne Area Navigation Equipment Using Multiple-Sensor Inputs.*

18. ***Global Positioning System (GPS).*** Capability managers should be cognisant of DI(G) OPS 41-5 - *Global Positioning System in New Acquisitions* which details the role of the Navigation Warfare System Project Office (NAVWAR SPO) with respect to GPS procurements.

19. GPS equipment has the capability to provide accurate navigation for enroute, terminal and approach phases of flight. In order for these capabilities to be realised fully, GPS equipment must be integrated with aircraft systems and further, must utilise aeronautical databases from approved suppliers such as RAAF Aeronautical Information Services.

20. The majority of military GPS equipment will not be certified against civil standards as it is optimised for Navigation Warfare, incorporating a number of additional functions that are specifically excluded in civil GPS equipment. The requirements detailed in civil standards do however form an accepted baseline against which military GPS equipment can have equivalence, shown through analysis and risk mitigation. Equivalence needs to factor in:

a. satisfaction against the higher level operating parameters of accuracy, integrity, availability and continuity of service (with particular focus on integrity);

b. GPS integration with aircraft navigation systems and displays; and

c. aircrew procedures and proficiency.

21. Civil design standards for aviation approved GPS equipment are as follows:

a. CASA AC 21-36(0) – *Global Navigation Satellite System (GNSS) Equipment: Airworthiness Guidelines* (which replaced CASA CAAP 35-1(0)) details the GPS integration requirements (design, installation and testing) for all phases of flight with respect to VFR, IFR, RNP, RNAV and single/dual pilot operations. GPS installation on ADF aircraft should normally comply with the requirements of CASA AC 21-36 (0), excluding the specified requirement for the GPS to be FAA Technical Standard Order certified;

b. FAA AC 20-138A - *Airworthiness Approval of Global Navigation Satellite System (GNSS) Equipment* is referenced within CASA AC 21-36(0) and is seen as an equivalent document;

c. FAA TSO-C129a - *Airborne Supplemental Navigation Equipment Using the Global Positioning System (GPS)* which references RTCA/DO-208;

d. FAA TSO C145b - *Airborne Navigation Sensors using the Global Positioning System Augmented by the Satellite Based Augmentation System* which references RTCA/DO-229;

e. FAA TSO C146b – *Stand Alone Airborne Navigation Equipment Using the Global Positioning System Augmented by the Satellite Based Augmentation System* which references RTCA/DO-229;

f. RTCA/DO-208 - *Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)*; and

g. RTCA/DO-229 – *Minimum Operational Performance Standards for Global Positioning System / Wide Area Augmentation System Airborne Equipment.*

22. ***Reduced Vertical Separation Minimum (RVSM).*** RVSM describes the reduction of standard vertical separation between aircraft flying between Flight Levels 290 and 410, from 2,000ft to 1,000ft. Airspace or routes between these altitudes where a Vertical Separation Minimum of 1,000ft is applied is designated as RVSM airspace. ADF aircraft that are not RVSM compliant may be subjected to civilian airspace restrictions. The following documents provide guidance on RSVM:

a. CASA CAAP 181A-1(1) - *Reduced Vertical Separation Minimum (RVSM) Approvals*, provides appropriate guidance for civilian aircraft requiring RVSM approval, and is largely applicable to ADF aircraft;

b. FAA Order 8400.10 Volume 4 Chapter 1 Section 5 provides requirements for civilian aircraft and operators in RVSM airspace;

c. FAR Part 91 Appendix G – *Operations in Reduced Vertical Separation Minimum (RVSM) Airspace* or EASA Leaflet No 6 revision 1 - *Guidance Material on the Approval of Aircraft and Operations for Flight in Airspace above Flight Level 290 where a 300m (1000ft) Vertical Separation Minimum is applied*; and

d. FAA 91-RVSM (Change 2): *Guidance Material on the Approval Operators/Aircraft for RVSM Operations.*

23. ***VOR/ILS FM Immunity.*** The term 'FM Immunity' refers to a problem where commercial FM radio communications combine to create a negative effect on the VOR and ILS receivers in an aircraft, causing them to display inaccurate information (often without indication that the information is inaccurate). FM interference immunity performance provisions are detailed in ICAO Annex 10. Aviation authorities have two options: either use analysis to assess the impacts of FM broadcast changes and manage accordingly, or require the fitment of VOR/ILS systems that are immune to the problem. This latter approach has been mandated in the European region from January 2001, and therefore ADF aircraft operating in Europe must either have FM immune VOR/ILS systems fitted, or accept that they may be subject to significant restrictions, particularly on terminal area flight operations. Some European nations may even refuse entry to non-compliant State aircraft, or may only allow en-route access.

24. CASA is unlikely to mandate a similar approach in Australia (to date CASA have notified ICAO of non compliance with Annex 10 FM Immunity requirements), and therefore are not influencing the ADF's decision whether to fit FM immune VOR/ILS equipment. A reasonable approach is for ADF aircraft with a requirement to operate in Europe to be modified with FM immune VOR/ILS systems, while other ADF aircraft should have this capability incorporated on an opportunity basis. Acceptable equipment standards for complying with FM immunity performance requirements are as follows:

a. EUROCAE ED-22B - *Minimum Performance Standards for Airborne VOR Receiving Equipment* or RTCA/DO-196 - *Minimum Operating Performance Standards for Airborne VOR Receiving Equipment Operating within the Radio Frequency Range of 108 – 117.95 MHz*;

b. EUROCAE ED-23B - *Minimum Operating Performance Standards for Airborne VHF Rx-Tx Operating in the Frequency Range 117.975 – 136.975 MHz;* or RTCA/DO-186B - *Minimum Operating Performance Standards for Airborne Radio Communications Equipment*; and

c. EUROCAE ED-88 - *Minimum Operational Performance Specification for Multi Mode Receiver (MMR) including Instrument Landing System(ILS), Microwave Landing System (MLS) and Global Positioning System (GPS) used for Supplemental Means of Navigation* or RTCA/DO-195 - *Minimum Operating Performance Standards for Airborne ILS Localiser Receiving Equipment Operating within the Radio Frequency Range of 108 – 112 MHz.*

Surveillance Systems

25. The following paragraphs detail standards against which the adequacy of various surveillance systems can be assessed.

26. ***Airborne Collision Avoidance System (ACAS).*** DI(G) OPS 40-1 - *Airborne Collision Avoidance and Ground Proximity Warning Equipment for ADF Aircraft* provides policy for the fitment of ACAS (also known as TCAS - Traffic Alert and Collision Avoidance System) in ADF aircraft. The capability managers for each ADF aircraft should determine which type of TCAS (TCAS I or TCAS II) is required. The following documents prescribe minimum performance standards for both TCAS I and II systems. Note that if TCAS II is to be fitted, the fitment of Mode S transponder is mandatory:

a. FAA TSO-C118 - *Traffic Alert and Collision Avoidance System (TCAS) Airborne Equipment, TCAS I*;

b. RTCA/DO-197 - *Minimum Operational Performance Standards for an Active Traffic Alert and Collision Avoidance System I*;

c. FAA AC 20-131A – *Airworthiness Approval of Traffic Alert and Collision Avoidance Systems (TCAS II) and Mode S Transponders*;

d. FAA AC 20-151 – *Airworthiness Approval of Traffic Alert and Collision Avoidance Systems (TCAS II) Version 7.0 and Associated Mode S Transponders*;

e. FAA TSO-C119B, *Traffic Alert and Collision Avoidance System (TCAS) Airborne Equipment, TCAS II*; and

f. RTCA/DO-185A - *Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) Airborne Equipment.*

27. ***Ground Proximity Warning System (GPWS).*** DI(G) OPS 40-1 also provides policy for the fitment of GPWS (now also known by the acronym TAWS - Terrain Awareness and Warning System) in ADF aircraft. The capability managers for each ADF aircraft should determine which type of TAWS system is required – Class A or Class B. The following AC and TSO prescribe minimum performance standards for TAWS systems:

a. FAA AC 25-23 - *Airworthiness Criteria for the Installation Approval of a Terrain Awareness and Warning System (TAWS) for Part 25 Airplanes*; and

b. FAA TSO-C151B - *Terrain Awareness and Warning System.*

28. ***Identification Friend or Foe (IFF).*** The technical characteristics of military IFF systems are contained in NATO STANAG 4193 (for Mk XA and XII systems). If there is an operational requirement for fitment of Mode S (eg. TCAS II fitted), the following documents prescribe the minimum performance standards:

a. FAA TSO-C112 - *Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/mode S) Airborne Equipment*; and

b. RTCA/DO-181 - *Minimum Operational Performance Standards For Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S) Airborne Equipment.*

29. The ADF's IFF Replacement Project (JP 90) will replace the Mode 4 Mk-XII IFF capability with the next generation airborne combat identification system in ADF aircraft over the period 2015-2020. The Options Review Committee (ORC) agreed that Mode 5 Mk-XIIA will be the sole ADF solution based on current international activities and coalition interoperability requirements. New projects should endeavour to fit Mode 5 Mk-XIIA where possible.

30. ***Landing Gear Down Tones.*** All ADF fixed wing aircraft (including leased aircraft on the State register) fitted with retractable undercarriage require an independent secondary system that either confirms that the landing gear is down and locked, or warns the pilot that the aircraft is not correctly configured for landing. The decision to fit landing gear down tone devices to future ADF fixed wing aircraft will be made by the relevant Operational Airworthiness Authority. Factors to be taken into consideration include the functionality provided by the configuration monitoring system fitted to the aircraft, crew composition and the additional cost of fitting a landing gear down tone device.

31. ***Future Civilian Surveillance Systems.*** Future surveillance systems will provide aircraft identification and accurate positional information, and disseminate this information via air and/or ground-based communications systems. This is likely to be an evolutionary process, resulting in a reduction in aircraft dependence on ground based systems and controllers. Cornerstone to this approach is Automatic Dependent Surveillance – Broadcast (ADS-B),

which is an automated system for delivering navigational information via datalink between aircraft and ground stations. Project Offices should wherever possible specify a requirement for ADS-B compatible transponder equipment in new aircraft acquisitions. Equipment complying with the following standards is considered suitable for ADF aircraft:

a. CASA ATSO-C1004 - *Airborne Mode A/C Transponder Equipment with Extended Squitter Automatic Dependent Surveillance - Broadcast (ADS-B)*;

b. FAA TSO-C166 - *Extended Squitter Automatic Dependent Surveillance –Traffic Information Service - Broadcast (TIS-B) Equipment Operating on the Radio Frequency of 1090 Megahertz (MHz)*; and

c. RTCA/DO-260A Change 1 - *Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services (TIS-B).*

32. CASA has produced a draft Advisory Circular AC 21-45(0) - *Airworthiness Approval of Airborne Automatic Dependant Surveillance Broadcast Equipment* which defines the airborne component of the 1090 MHz Extended Squitter Automatic Dependant Surveillance Broadcast (ADS-B) data link use in Australia. Appendix A to this draft AC details related Australian and International documents.

INTEROPERABILITY

33. Several military standardisation bodies produce standards to facilitate the interoperability of equipment and systems amongst their member nations. Two such bodies are the Air and Space Interoperability Council (ASIC), and NATO. The ASIC produces ‘Air Standards’, and NATO produces ‘Standardisation Agreements’ (STANAGs). Standards produced by these bodies specify the minimum basic technical characteristics of equipment and systems to achieve interoperability, and should not be confused with more detailed equipment standards (eg. MIL-STDs) specifying requirements relating to equipment function and performance as well as interoperability. There is some overlap and commonality between the standards produced by the ASIC and NATO, since they have several member nations in common. Typically communications, navigation and surveillance equipment complying with the requirements of either NATO STANAGs or ASIC Air Standards will meet ADF interoperability requirements.

34. ***ASIC Air Standards.*** The ASIC is a body comprised of military representatives from Australia, USA, UK, Canada and New Zealand. Working Party 70 (WP 70) of the ASIC produces Air Standards covering the interoperability of mission avionics - in particular communications, navigation and identification systems (for example Air Standards 70/03 and 70/04 relate to VHF and UHF communications equipment respectively). Whilst equipment standards are typically consistent with the requirements of WP 70 (as they are produced by ASIC member countries), consideration should be given to applying the requirements of WP 70 standards to ensure that the most current interoperability requirements are met.

35. ***NATO STANAGs.*** STANAGs 4203, 4204 and 4205 specify interoperability requirements for HF, VHF and UHF radio equipment. STANAG 4193 (IFF equipment) and STANAG 4294 (NAVSTAR Global Positioning System) are very comprehensive, and equipment complying with these STANAGs will typically also meet all functional performance requirements necessary to assure airworthiness. For example, calling out STANAG 4193 as a requirement for IFF systems in a project specification is likely to be sufficient in itself, without the need to specify a particular equipment standard.

INSTRUMENTS AND DISPLAYS

General Layout and Functionality

36. In most circumstances, the requirements in both DEF STAN 00-970 and FAR/JARs cover the general layout and functionality of instruments and displays. Some requirements may need to be added by the Project Office for military instrument/display systems since these are not covered by FARs/JARs, and DEF STAN 00-970 (Part 1 Sections 1 and 6) only provides guidance. Human factors considerations (eg. cockpit ergonomics) are best assessed on a case-by-case basis; if the ADF has unique layout requirements additional clauses may be needed (refer Section 2 Chapter 13).

Multi-Function/Head Up Displays

37. An aspect of cockpit displays that is not adequately addressed in current civilian and military standards is the airworthiness requirements for Multi-Function Displays (MFDs) and Head Up Displays (HUDs). Some technical airworthiness requirements are discussed in Part 1 Section 6 of DEF STAN 00-970, and also in some MIL-STD/SPECs, but the coverage in these standards is not comprehensive. FAR/JAR requirements, when combined with the requirements of several Advisory Circulars (AC) and TSOs, provide the most comprehensive coverage of MFDs/HUDs, including a reference to SAE AS8055 - *Minimum Performance Standard for Airborne Head Up Displays (HUD)*.

38. A further complication arises if the MFD/HUD is to be certified as the Primary Flight Reference (PFR) display on the aircraft. This introduces the need for a more rigorous design and airworthiness assurance process than would be required if the HUD was to be used simply as an en-route navigation aid. In order for the MFD/HUD to be certified as the PFR display, the Contractor should demonstrate the suitability of the system for use in this role. A suitable certification basis is FAA FARs, including the following:

a. FAR 25.1301, 25.1303, 25.1309, 25.1321 and 25.1333 (and associated advisory material);

b. FAA TSO-C113 - *Airborne Multipurpose Electronic Displays*; and

c. FAA AC 25-11 - *Transport Category Airplane Electronic Display Systems.*

These requirements address the data display requirements, display quality, installation and arrangements of displays. Additionally, the AC addresses the data availability, integrity and failure detection capability of the HUD. The probability of losing data which would affect safe flight, and the displaying of erroneous or misleading data, must be extremely improbable (defined by the FAA as a likelihood of 10^{-9} per flight hour). An additional ADF requirement is that the failure or display of erroneous or misleading data in a particular data source should be detected, and that the failure be annunciated or made obvious (by removal of data or blanking of the data box for example).

39. To serve as the PFR display, the HUD should provide the flight information required by FAR 25.1321 (and other operationally determined safety of flight data) in a manner that is at least as good as panel mounted, electromechanical instruments. This should be determined by simulation and flight tests of all phases of flight, including normal, abnormal and emergency conditions. These tests should be conducted using a representative cross section of aircrew. The requirement for MFD/HUD symbology to be comprehensible in all conditions should be easily demonstrable. Furthermore, the software should be developed to a level of integrity consistent with the HUD's function as the PFR display. SCI1-DGTA are able to provide advice on whether the software level(s) proposed by a contractor for the various components of a HUD are appropriate for the item to be used as a PFR.

CRASH DATA RECORDING AND LOCATOR SYSTEMS

40. DI(AF) OPS 6-14 – *Use and Protection of Crash Data Recorder Systems and Recorded Data* provides policy on the use and protection of Crash Data Recording (CDR) systems and recorded data. The combination of aircraft fit and support equipment intended to monitor, record and analyse aircraft flight incident data, and assist in crash location and identification of the cause of an aircraft accident or incident is considered a CDR system. Cockpit Voice Recorders (CVRs), Flight Data Recorders (FDRs), Crash Position Indicators (CPIs) and Underwater Locating Devices (ULDs) are typical aircraft fit elements of CDR systems.

41. The ADF's preferred standard for CDR systems is EUROCAE specification EUROCAE ED-112 *Minimum Operational Performance Specification for Crash Protected Airborne Recorder Systems*. Additional requirements are detailed in annex A. Some tailoring of ED-112 may be necessary when fitting CDR systems to legacy aircraft, since budgetary and/or practical constraints may preclude the installation of sensors for the acquisition of particular parameters specified in ED-112. In such circumstances, appropriate waivers should be sought from Directorate of Defence Aviation and Air Force Safety (DDAAFS).

ENVIRONMENTAL DESIGN REQUIREMENTS

42. Appropriate environmental design and test requirements should be considered for all aircraft equipment. Many aircraft equipment specifications have the environmental design and test requirements addressed as part of the requirements. The more commonly referenced documents are discussed below.

43. ***US Military Systems.*** Equipment/systems built for the US Military are generally adequately designed and tested to appropriate standards. The design of equipment, if not detailed in the procurement specification, generally conforms to the requirements of MIL-HDBK-454 Revision A - *General Guidelines for Electronic Equipment*, and MIL-HDBK-5400 Revision 95, *Electric Equipment, Airborne General Guidelines*. These documents should be used concurrently. Environmental qualification of equipment is addressed by MIL-STD-810F – *Department of Defense Test Method Standard for Environmental Engineering Considerations and Laboratory Tests*, which provides test methodologies for qualification of equipment to different environments.

44. ***FAR/JAR Systems.*** Equipment/systems built for commercial use can be built to a number of standards. Physical characteristics are set out in documents such as ARINCs and SAEs, however these are not mandated by any higher level standards. Suitability of design and build is usually determined by testing for functionality and for environmental suitability. RTCA/DO-160E - *Environmental Conditions and Test Procedures for Airborne Equipment*, and EUROCAE ED-14E - *Environmental Conditions and Test Procedures for Airborne Equipment* (equivalent standards) set the test requirements for environmental qualification of commercial equipment/systems. These standards are not always mandated, unless the system is a TSO-compliant system, where both function and environmental performance is addressed.

45. ***DEF STAN 00-970 Systems.*** Equipment/systems built to DEF STAN 00-970 requirements should be adequately designed and environmentally qualified. Requirements provided in the applicable parts of the DEF STAN give sufficient detail, and refer to appropriate other standards to ensure a product will operate in its intended environment. One of the principal standards referred to is British Standard 3G100 (*General Requirements for Equipment Use in Aircraft*) which provides design and test requirements for avionics equipment.

AIRBORNE LASERS

46. Where Projects intend to introduce or modify airborne lasers, compliance is required with the aircraft-related laser safety requirements included in SAFETYMAN Volume 1, Part 4, Chapter 3. Further information is available from the Defence Safety Management Agency (DSMA).

Annex:

A. Crash Data Recorder Requirements

Blank Page

CRASH DATA RECORDER REQUIREMENTS

1. These Crash Data Recorder (CDR) requirements apply to all new ADF aircraft acquisitions, to provide flight incident data for analysis in the event of a flight incident, mishap or crash. The requirements presented in this section are additional to, or amplify, those contained in EUROCAE specification ED-112 - *Minimum Operational Performance Specification for Crash Protected Airborne Recorder Systems.*

2. These CDR requirements apply to the following three broad categories of aircraft:

a. Category I – Fixed wing, multi-engine aircraft (includes AEW&C, ASW and transport aircraft);

b. Category II – Fixed wing, fighter/attack/trainer aircraft; and

c. Category III – Rotary wing aircraft.

3. For each aircraft category, the CDR system should comprise a combination of at least Flight Data Recorder (FDR), Cockpit Voice Recorder (CVR), Emergency Locator Transmitter (ELT) and Underwater Location Device (ULD). Whilst separate CVR and FDR systems are preferable, a combined flight recorder system may be necessary where weight and space considerations prohibit the installation of two separate recorders. Acceptable minimum CDR system configurations are shown in Table 3–B–1. Aircraft category-specific requirements from ED-112 for CDR systems are shown in Table 3–B–2 (CVR) and Table 3–B–3 (FDR). Where the ADF is procuring an aircraft that holds a recognised civil type certification, the CDR system requirements of those regulations, both for type certification (eg FAR 25) and operation (eg FAR 121), should also apply.

Table 3–B–1 Minimum Acceptable CDR System Configuration

Aircraft Type	Acceptable CDR System Configuration			
	CVR + ULD	FDR + ULD	CVR/FDR + ULD	ELT
Category I	1	1		1
	Or			
		1	1	1
	Or			
	1		1	1
	Or			
			2	1
Category II	1	1		1
	Or			
			1	1
Category III	1	1		1
	Or			
			1	1

Table 3–B–2 Applicable ED–112 CVR Requirements for Aircraft Categories

Recorder Class	Aircraft Category		
	I	II	III
Class 1 CVRs	Part I	N/A	N/A
Class 2 CVRs	N/A	Part I	Part I

Table 3–B–3 Applicable ED–112 FDR Requirements and Recorded Parameters* for Aircraft Engines

Recorder Class	Aircraft Category / Manufacture Date								
	I			II			III		
	Pre-12Oct91	After 11Oct91	After 19Aug02	Pre-12Oct91	After 11Oct91	After 01Jan04	Pre-12Oct91	After 11Oct91	N/A
Class A FDRs	Part II List V	Part II List W	Part II List X	N/A	N/A	N/A	N/A	N/A	N/A
Class B FDRs	N/A	N/A	N/A	Part II List V	Part II List W	Part II List X	Part II List Y	Part II List Z	N/A

* Parameter list types are defined (to improve readability of the table) as follows:

List V: Part II & Annex II-A, Table II-A.1, Serials 1- 15

List W: Part II & Annex II-A, Table II-A.1, Serials 1- 44

List X: Part II & Annex II-A, Table II-A.1 (entire table)

List Y: Part II & Annex II-A, Table II-A.2, Serials 1- 21

List Z: Part II & Annex II-A, Table II-A.2 (entire table)

ADDITIONAL CDR EQUIPMENT REQUIREMENTS

Cockpit Voice Recorder

4. Each CVR system installation should comply with FAA Advisory Circular (AC) 25.1457-1A - *Cockpit Voice Recorder Installations*. This AC is applicable to all ADF aircraft categories (I, II and III), and provides additional guidance pertaining to cockpit area microphones, CVR location, and CVR erasure features.

Flight Data Recorder

5. Any novel or unique design or operational characteristics of the aircraft should be evaluated to determine if any dedicated parameters should be recorded by the FDR in addition to or in place of existing requirements detailed in ED-112, Annex II–A. In such circumstances, appropriate guidance should be sought from Directorate of Defence Aviation and Air Force Safety (DDAAFS).

Recorder Independent Power Supply

6. Where practical each CVR, FDR and/or combined CVR/FDR should be fitted with a Recorder Independent Power Supply (RIPS) compliant with ED-112, Section 5. Guidance should be sought from DDAAFS on the requirement for RIPS in particular aircraft types.

Emergency Locator Transmitter

7. Each ELT should comply with the requirements of:

a. FAA TSO-C91a - *Emergency Locator Transmitter Equipment*, or

b. JTSO-2C91a - *Emergency Locator Transmitter Equipment,* and

c. FAA TSO-C126 - *406 MHz Emergency Locator Transmitter, or*

d. JTSO-2C126 - *406 MHz Emergency Locator Transmitter*

8. The above standards call out RTCA/DO 183 Minimum Operational Performance Standards for Emergency Locator Transmitters (ELT's) and RTCA/DO 204 Minimum Operational Performance Standards for 406MHz Emergency Locator Transmitters (ELT's).

9. From February 2009 ELTs that only comply with TSO-C91a and transmit on 121.5/243 MHz will not be monitored by COSPAS-SARSAT. Thus for new ELT installations, consideration may be given to requiring only compliance with TSO-C126.

Underwater Locating Device

10. Each ULD should comply with FAA TSO-C121 - *Underwater Locating Devices (Acoustic) (Self-Powered)*, except that Impact Shock test requirements should be as specified in ED-112 Section 2-1.16.4.

Deployable Recorders

11. Where aircraft mission profiles may reduce the likelihood of recovering aircraft wreckage following an accident, consideration should be given to installing a deployable recorder system compliant with ED-112, Section 3. Guidance should be sought from DDAAFS on the requirement for deployable recorders in particular aircraft types.

TEMPEST Considerations

12. TEMPEST threat assessments, in accordance with Part 4 chapter 6 of the Defence Security Manual, are to be undertaken on proposed CDR system installations and appropriate design measures implemented to minimise any threats so identified. For further information or guidance contact 462SQN Det Laverton on (03) 9256 4144.

Support Equipment

13. Where practical, new CDR equipment should be compatible with existing ADF CDR Support Equipment. Existing or new support equipment should facilitate operational maintenance and operational validation of the CDR equipment, as well as CDR data recovery, data compression, data analysis, flight reconstruction and flight replay.

Blank Page

SECTION 2

CHAPTER 4

AIRCRAFT LIGHTING

INTRODUCTION

1. This chapter provides ADF-specific lighting requirements to supplement other civil and military standards. It applies to all exterior and interior lighting including aircrew station illuminated visual signals.

APPLICATION AND TAILORING GUIDANCE

UK Military Systems

2. DEF STAN 00-970, Section 1.1.21 - 26, Section 4.15.33 - 64, Section 4.22.8, Section 4.22.56, Section 4.23.13, Section 4 Leaflet 64, Section 6.2.7 - 6.2.8, Section 6.7, Section 9.5.28 - 34 and Section 9 Leaflet 12, provide requirements that define the fundamental design considerations necessary to obtain an aircraft lighting system that is considered airworthy. It contains sufficient detail to be used in aircraft acquisition and modification however it currently addresses Night Vision Imaging Systems (NVIS) by referring to STANAG 3224. While the requirements of STANAG 3224 are adequate, they contain less detail than US Military standards, which are preferred for ADF NVIS lighting requirements.

FAR/JAR Systems

3. FARs/JARs cover aircraft lighting for various types of aircraft, however specific requirements are limited and in some cases may not provide sufficient detail for ADF aircraft acquisition or component modifications. FARs/JARs cover emergency exit lights, emergency lighting, instrument lights, landing lights, position lights, anti-collision lights and wing icing detection lights. However, they do not cover lighting required for military-specific roles.

4. Where the lighting system of an aircraft being acquired is to be designed to FAR/JAR requirements, the following ADF unique requirements should be considered:

a. lighting for inflight refuelling (both tanker and receiving aircraft),

b. lighting compatibility with NVIS (both internal and external lighting),

c. suitability of landing lights for unprepared landing strips, and

d. formation lights.

US Military Systems

5. US Military Specifications, Standards and Handbooks provide detailed requirements for aircraft lighting systems including those required to be NVIS compatible. However, they normally require tailoring to the ADF specific application.

6. ***JSSG-2010-5, Crew Systems Aircraft Lighting Handbook.*** This Specification Guide provides guidance for the development of requirements and verification for exterior and interior airborne lighting equipment, including specific requirements for interior lighting compatible with Type I or II and Class A, B or C Night Vision Imaging Systems (NVIS). It also provides guidance on aircrew station signals and alerting systems. This document provides guidance only, and should not be cited as a requirement itself.

7. ***MIL-L-6503, Lighting Equipment, Aircraft, General Specifications for Installation of.*** MIL-L-6503 details the requirements for aircraft exterior lighting, interior illumination and emergency lighting. All lighting systems are covered appropriately with the exception of instrument lighting and aircrew station visual signals, which are omitted. With effect 25 Mar 96, this specification was declared inactive for new designs. However, as it provides appropriate system design and component selection requirements for aircraft exterior and interior lighting systems, it is considered suitable for ADF use. This specification refers the user to numerous associated specifications and standards that, in

some cases, may exceed ADF requirements. If this specification is used as a basis for lighting system certification, the following issues should be considered:

a. MIL-L-6503 details the use of military specification components however, depending on the installation being designed or acquired, the best outcome may be achieved by tailoring the requirements document to allow the use of commercial equivalents.

b. Due to the various types of instruments used in an aircraft instrument panel, several different lighting specifications may be used. Lighting of instruments is generally determined by the prime manufacturer and in most cases would be acceptable for ADF requirements provided they have compatible illumination levels.

NIGHT VISION IMAGING SYSTEMS

8. An aircraft Night Vision Imaging System (NVIS) uses helmet mounted, binocular, image intensifier tubes to produce an enhanced image of a scene in light conditions too low for normal navigation and pilotage. When using Type I NVIS, aircrew look through the image intensifier tubes to see outside the aircraft, and under the tubes, with the unaided eye, to read instruments and displays in the cockpit. With Type II NVIS, the intensified image is projected on a see-through medium in the user's line of sight.

9. Requirements for interior lighting compatibility depend upon the characteristics of the NVIS with which the lighting is intended to be compatible. For this reason NVIS-compatible aircraft interior lighting is divided into the following types and classes as detailed in MIL-L-85762 and MIL-STD-3009:

a. Type I - Lighting compatible with any direct view image NVIS utilizing Generation III image intensifier tubes;

b. Type II - Lighting compatible with any projected image NVIS utilizing Generation III image intensifier tubes;

c. Class A - Lighting compatible with NVIS utilizing 625nm minus blue objective lens filters. Class A is not compatible with red cockpit lighting because of the overlap between the spectrum of red light and the sensitivity of Class A NVIS;

d. Class B - Lighting compatible with NVIS utilizing 665nm minus blue objective lens filters. Class B is compatible with properly filtered red lights and colour electronic displays that meet appropriate requirements; and

e. Class C - Lighting compatible with NVIS having a 'notch' or 'leak' in the green part of the spectrum which allows viewing of HUD imagery. Lighting meeting Class B compatibility criteria is also compatible with Class C NVIS.

10. Night vision goggles (NVGs) amplify and convert available ambient light at night to produce a monochromatic, near day like image of the night time scene. Current NVGs used for flight are sensitive to wavelengths from about 625 nm or 665 nm (depending on objective lens coating) to about 900 nm. All unfiltered aircraft cockpit lighting emits sufficient energy in this wavelength range to cause unacceptable interference.

11. Unmodified aircraft cockpit lighting can interfere with the proper operation of NVGs in two ways. Firstly, incompatible light may be reflected into the FOV of the NVG, leading to obscuration of the outside scene by a false image. Secondly, incompatible light (either direct or reflected) can trigger the automatic gain control function of the NVGs, reducing image contrast. For each interference mechanism, the effect on the image seen through the NVGs is a reduction of the light level or contrast of the view outside the aircraft. This reduction in contrast can manifest as a reduction in visual acuity. Many techniques have been developed to produce cockpit lighting, including instrumentation and displays, which is reasonably compatible with the operation of NVGs. 'Reasonably compatible' means that there is sufficient illumination for the pilot to view his/her instruments and displays unaided (note, pilots look under the NVGs to directly view their instruments for only Type I NVGs) but the lighting is such that it does not significantly interfere with the image of the exterior scene viewed through the NVGs.

12. The conversion of internal lights in aircraft cockpits and cabins to meet US Military Specifications can involve the following conversion techniques, based on cost effectiveness and operational requirement:

a. Replacement of instrument panel glass with filter material;

b. Installation of filter material to warning, caution and annunciator indicators;

c. Replacement of existing lighting with LED or electro-luminescence based lighting;

d. Installation of NVIS compatible bridge and bezel lighting; and

e. Use of NVIS compatible floodlights in conjunction with de-energising unmodified lighting.

13. Other issues which should be evaluated during the introduction of NVGs into the aircraft are:

a. Reflections of incompatible light from transparencies such as the HUD, windshield and canopy in the field of view of the NVG;

b. The retention of daylight readability in modified lighting, annunciator and display systems;

c. The NVIS compatibility of multi-function displays based on back-lit LCD technology;

d. The ability of lighting control circuits to reduce cockpit illumination to the required intensity levels;

e. Shadowing of instruments by introduced NVIS compatible lighting bezels;

f. The degrading effects of aircraft transparencies upon NVG visual acuity;

g. The effects of external lights on NVG performance;

h. Displacement of the NVIS objective lens from the cockpit ‘design eye’ position; and

i. Physical interference of helmet mounted NVIS with the aircraft canopy in small cockpits.

14. To fully evaluate these effects, an aircraft NVIS compatible cockpit lighting evaluation should be conducted upon initial modification or when major changes to cockpit displays or lighting are made. The US Armstrong Laboratory procedure AL/HR-TR-1995-0617 is suitable for conducting a field evaluation of NVIS lighting.

15. The ADF currently uses, or is in the process of acquiring aircraft with, the following NVGs:

a. Type I, Class A – Blackhawk, Chinook, Caribou, C-130H, Iroquois and Kiowa;

b. Type I, Class B – F-111, Seahawk, Seasprite and C-17;

c. Type I, Class C – F/A-18A/B and C-130J; and

d. Type II, Class B - Tiger and MRH-90 will use the TOPOWL system for night vision. TOPOWL is a binocular helmet-mounted display and sight specially developed for helicopter pilots. It provides the pilot with visor projection of flight symbols, images from Image Intensifier Tubes (IIT) and Forward Looking Infrared (FLIR) sensors.

16. NVIS are currently not addressed in FARs, although RTCA/DO-268, Concept of Operations, Night Vision Imaging System for Civil Operators and RTCA/DO-275, Minimum Operational Performance Standards for Integrated Night Vision Imaging System Equipment, have been released. DEF STAN 00-970 also does not directly address NVIS however it does refer the reader to STANAG 3224, Aircraft Interior and Exterior Lighting Night Vision Goggle (NVG) and Non-NVG Compatible, which provides appropriate design criteria for aircrew station lighting in order to achieve NVG compatibility. US Military Specifications and Standards are comprehensive and cover all aspects of NVIS and NVG and are the recommended source of information and requirements for ADF NVIS lighting systems.

17. ***MIL-STD-3009, Lighting, Aircraft, Night Vision Imaging System (NVIS) Compatible.*** This standard establishes requirements for the emission characteristics of aircraft lighting and display equipment that is intended for use with night vision imaging systems (NVIS). It is applicable to all systems, sub-systems, component equipment and hardware that provide the lighting environment on aircraft where NVIS are employed. This document provides

interface requirements and testing methodologies to ensure NVIS compatibility with aircraft interior lighting. It does not contain general lighting requirements. MIL-STD-3009 supersedes MIL-L-85762 except for USN aircraft.

18. ***MIL-L-85762, Lighting, Aircraft, Interior, Night Vision Imaging System (NVIS) Compatible.*** MIL-L-85762 is a comprehensive document which defines the performance requirements and test procedures applicable to NVIS compatible lighting for new or modified aircraft lighting equipment and crew stations. This specification includes NVIS radiance (NR), chromaticity, luminance and contrast requirements.

19. ***MIL-STD-411, Aircrew Station Alerting Systems.*** MIL-STD-411 covers aircraft, aircrew station, alerting systems including general functions; operational logic; information content of messages; and physical characteristics of the alerting system's visual, auditory and tactile signals. It also contains detailed requirements for NVIS lighting compatibility.

ASSOCIATED SPECIFICATIONS AND STANDARDS

20. The following is a list of associated aircraft lighting specifications and standards which can provide additional information relating to the design of aircraft lighting systems:

a.	MIL-DTL-6363	Lamps, Incandescent, Aircraft Service, General Specification for
b.	MIL-HDBK-87213	Electronically/Optically Generated Airborne Displays
c.	MIL-L-25467	Lighting, Integral, Red, Aircraft Instrument, General Specification for
d.	MIL-L-25866	Light, Emergency Exit, Aircraft, LEU-1/A
e.	MIL-L-3661	Lampholders, Indicator Lights, Indicator Light Housings, and Indicator Light Lenses, General Specification for
f.	MIL-L-6723	Lights, Aircraft, General Specification for
g.	MIL-L-85314	Light Systems, Aircraft, Anti-Collision, Strobe, General Specification for
h.	MIL-PRF-85676	Lighting, Emergency Egress, Subassembly
i.	MIL-STD-1787	Aircraft Display Symbology
j.	RTCA/DO-268	Concept of Operations Night Vision Imaging System for Civil Operators
k.	RTCA/DO-275	Minium Operational Performance Standards for Integrated Night Vision Imaging System Equipment
l.	SAE ARP 1088	Aircraft Indicating Systems
m.	SAE ARP 4168	Night Vision Goggle (NVG) Compatible Light Sources
n.	SAE ARP 4392	Lighting, Aircraft Exterior, Night Vision Imaging System (NVIS) Compatible
o.	SAE ARP 4967	Night Vision Imaging System (NVIS) Integrally Illuminated Information Panels
p.	SAE ARP 503	Emergency Evacuation Illumination
q.	SAE AS 18276	Lighting, Aircraft Interior, Installation of
r.	SAE AS 25050	Colour, Aeronautical Lights and Lighting Equipment, General Requirements for

s.	SAE AS 50571	Lights, Instrument, Individual, General Specification for
t.	SAE AS 7788	Panels, Information, Integrally Illuminated
u.	STANAG 3153	Aircraft Navigation and Anti-collision Lights
v.	STANAG 3224	Aircraft Interior and Exterior Lighting Night Vision Goggle (NVG) and Non-NVG Compatible.
w.	STANAG 3379	In-Flight Visual Signals
x.	STANAG 3870	Emergency Escape/Evacuation Lighting

Blank Page

SECTION 2

CHAPTER 5

ELECTRICAL POWER GENERATION, STORAGE AND DISTRIBUTION

INTRODUCTION

1. This chapter provides ADF-specific electrical power generation, storage and distribution requirements, to supplement common civil and military standards.

ELECTRICAL POWER GENERATION

2. ***UK Military.*** DEF STAN 00-970, Part 1, Section 6.6, *Electrical Systems*, provides appropriate electrical power generation guidance. Section 4, Leaflet 94, specifies characteristics for electrical generating, distributing and consumer units. If DEF STAN 00-970 is specified in contract documentation, the minor standardisation enhancements, detailed at Annex A, should be included.

3. ***FARs/JARs.*** FARs and JARs provide commercial aircraft requirements for power supplies and associated control, regulation, and protective devices. Commercial class aircraft require analyses to be undertaken to establish compliance. An alternative standard, RTCA/DO-160 - *Environmental Conditions and Test Procedures for Airborne Equipment*, provides test methods for qualifying commercial aircraft equipment. RTCA/DO-160 covers a range of environmental conditions and includes power and electromagnetic characteristics. It provides similar guidance to DEF STAN 00-970, Part 1, Section 4, Leaflet 94 for electrical systems. Additionally, an Aircraft Electrical Load Data (AELD) analysis is mandatory for transport and commuter aircraft. All aircraft require an analysis to determine a safe operating capability in Visual Flying Rules (VFR) conditions for a minimum of five minutes, with normal power inoperative. FARs use broad requirements that concentrate on safety related issues. If FARs or JARs are specified in contract documentation, the additional requirements, detailed in Annex A, should be included.

4. ***US Military.*** MIL-STD-704, *Aircraft Electric Power Characteristics*, defines the requirements for, and characteristics of, aircraft electrical power to be provided at the input terminals of consumer equipment. This standard provides detailed requirements for normal, abnormal and emergency power, load balance and transients for 115VAC, 28VDC and 270VDC, however, it has no coverage of electrical system functional testing and gives no requirements for distribution system design and installation. If the original design requirements of a power supply cannot be established, MIL-STD-704 characteristics should be used to set the operating requirements for load equipment. MIL-STD-704 is suitable for specifying aircraft acquisition requirements but is less useful for setting test requirements of individual avionics components and equipment. If MIL-STD-704 is specified in contract documentation, the additional requirements, detailed in Annex A, should be included.

ELECTRICAL POWER STORAGE

5. Batteries are used widely in ADF aircraft applications. They supply electrical power prior to engine start, during emergencies and for equipment which operates independent of normal aircraft power supplies. Batteries used in aircraft are of various chemical compositions and range from 50 ampere hour ‘main’ aircraft batteries to ‘button’ batteries used for computer data retention.

6. ***Main Batteries.*** Several types of secondary (rechargeable) ‘main’ batteries are currently fitted to ADF aircraft. While these batteries are used for various applications, including engine and APU starting, powering aircraft systems when ground power is unavailable etc, their primary purpose is to provide emergency electrical power to flight critical systems when all other aircraft power supplies are unavailable. The types of main batteries currently approved for use in ADF aircraft are:

a. ***Vented lead acid batteries***. These batteries are the most widely used of the secondary battery types. The advantages of these batteries are low cost, simple maintenance, ruggedness and reliability.

b. ***Sealed lead acid batteries (SLABs)***. These batteries are a relatively new technology that is gaining wide acceptance in the aerospace industry. They are virtually maintenance free however they will be irreversibly damaged if over-discharged. SLABs have been retro-fitted to several ADF aircraft due to excessive maintenance problems encountered with their original Nickel Cadmium battery systems.

Sealed lead acid batteries are the preferred technology for ADF aircraft main batteries, however they may not always be suitable where engine starting from the battery is required.

c. ***Vented nickel cadmium batteries***. This type of battery is constructed with a number of replaceable vented cells that have a nominal discharge voltage of 1.2 volts. While some of the performance characteristics of these batteries exceed those of lead acid batteries, they have a higher initial cost and increased maintenance requirements. Nickel cadmium batteries are also subject to 'memory effect'. This is a phenomenon wherein the cells retain the characteristics of previous cycling. That is, after repeated shallow discharges followed by recharging, the battery will fail to provide its full discharge capacity.

7. ***Equipment Batteries.*** Various other cells and batteries, both non-rechargeable (primary) and rechargeable (secondary), are approved for fitment in ADF aircraft equipment such as computers, clocks, emergency beacons and radios, torches and emergency exit lighting. These battery types are:

a. ***Carbon Zinc, (primary).*** Carbon Zinc batteries provide an economical power source for devices requiring light to moderate drain. The open circuit voltage of a fresh carbon zinc cell is typically 1.55 to 1.6 volts. The average capacity remains above 90% after storage for one year at 21 °C. These are primary cells and cannot be recharged.

b. ***Alkaline, (primary).*** Alkaline batteries provide an economical power source for devices requiring heavy or continuous use. The open circuit voltage of a fresh alkaline cell is typically 1.58 volts. The average capacity remains above 95% after storage for one year at 21°C. These are primary cells and cannot be recharged.

c. ***Sealed Nickel Cadmium, (secondary).*** Sealed nickel cadmium batteries are the most widely used sealed rechargeable batteries. They maintain a relatively constant potential during discharge and can be stored in any state of charge. During discharge, the average voltage of a sealed nickel cadmium cell is approximately 1.2 volts. The charge retention of nickel cadmium cells is poor and will drop to approximately 50% after storage for 5 weeks at 21°C. They can be recharged many times, however sealed nickel cadmium cells suffer from memory effect if subjected to repeated shallow discharge/charge cycles. While sealed nickel cadmium cells can be discharged over a wide temperature range, (-20°C to 45°C), charging must be carried in a much narrower range. To obtain maximum charge retention, cell temperature should be maintained at 20 to 35°C.

d. ***Nickel Metal Hydride, (secondary).*** Nickel Metal Hydride (NiMH) cells are essentially an extension of the proven sealed nickel cadmium technology with the substitution of a hydrogen absorbing negative electrode for the cadmium based electrode. This substitution increases the cell electrical capacity for a given weight and volume (up to 40%) and eliminates the cadmium toxicity concerns. The nickel metal hydride cell has similar cell voltage to the nickel cadmium cell, however it has a much lower self discharge rate and little or no memory effect.

e. ***Lithium, (primary and secondary).*** The electrical characteristics and outstanding performance of lithium cells make them an ideal choice for applications where cost is not the overriding consideration. The safety concerns surrounding the use of lithium batteries have been reduced with the introduction of safer chemistries and cell constructions. Batteries based on lithium chemistries have the highest specific energy (energy per unit weight) and energy density (energy per unit volume) of all chemistry types. Certain types of lithium batteries also have extended operating temperature range, enabled by the absence of water and the nature of the materials used. Specifically, lithium/thionyl chloride ($Li-SOCl_2$) can operate at temperatures as low as –55°C and as high as 85°C. Lithium batteries have an excellent shelf life (low self-discharge rate) of up to 15 years, however due to toxic materials, they also have specific handling, storage and disposal requirements.

8. Appropriate cells and batteries should be selected to provide a reliable and effective power source under all envisaged operating conditions. Several of the listed batteries have specific protective and handling requirements and these must be addressed in the aircraft/component design. For further detailed information on all these battery types, refer to the DGTA website.

ELECTRICAL POWER DISTRIBUTION

9. ***UK Military*****.** DEF STAN 00-970 provides adequate design and selection guidance for wiring and wiring devices for use in aircraft and is acceptable for ADF aircraft, provided it is supplemented by the additional ADF requirements at paragraphs 12 to 15. However, SAE AS 50881 (see paragraph 11) provides substantially more comprehensive guidance, and is therefore preferred by the ADF.

10. ***FARs/JARs*****.** Parts 25.1307, 25.1351, 25.1353, 25.1355, 25.1357 and 25.1363 cover aircraft electrical equipment and installations for various types of aircraft, however, specific requirements are limited and generally do not provide sufficient detail for aircraft acquisition or modification. FARs/JARs should be supplemented with commercial specifications such as SAE ARP4404, *Aircraft Electrical Installation*, which provide guidance on electrical installations for transport aircraft. This document is acceptable for ADF aircraft, provided it is supplemented by the additional ADF requirements at paragraphs 12 to 15. SAE ARP4404 guidance is equivalent to that provided by SAE AS 50881, favouring the installation perspective rather than functional requirements. Topics covered include wire selection and routing, connectors and terminations, circuits for essential equipment, circuit protection, bonding and grounding, provisions for future electrical equipment, corrosion protection, load distribution, system tests, and emergency controls and procedures. In addition, SAE ARP4404 details functional testing, which is not covered in SAE AS 50881.

11. ***US Military*****.** SAE AS 50881, *Wiring Aerospace Vehicle*, has replaced MIL-W-5088 and provides detailed design and selection guidance for wiring and wiring devices for use in aircraft, and is acceptable for ADF aircraft provided it is supplemented by the additional ADF requirements at paragraphs 12 to 15. The intent of this document is to provide background on wide ranging installation requirements pivotal to aircraft safety, performance and reliability, ease of maintenance, and aircraft service life. Since all aircraft classes are covered, requirements must be tailored for a particular aircraft or installation. A cross-reference of hardware, materials and procedural specifications is provided at the front of the document. It is important to recognise that the requirements for equipment, parts or components are based on military standard products, and in many cases these may not provide the most cost effective solution (ie invoking military standard products when suitable less expensive Commercial Off The Shelf (COTS) equivalents are satisfactory). SAE AS 50881 is the primary electrical system design document as it describes an installation rather than a function. It also has sound information for in-service management of aircraft electrical systems and is the standard upon which the ADF's aircraft wiring manual (AAP 7045.002-1) is based.

Additional ADF Wire Requirements

12. The major civilian and military wiring standards, as detailed in paragraphs 9 to 11, are largely acceptable to the ADF, with the exception of some wire insulating materials. These exceptions are detailed below, and are included as suggested contract requirements at Annex A.

13. ***Polyimide Insulated Wiring*****.** Polyimide based wiring insulation (commonly known by the Du Pont trade name Kapton) exhibits a property known as flashover or arc tracking. For this phenomenon to occur, damaged insulation, a conductive path to ground, and sufficient voltage and source current capability to sustain arcing are required. When these conditions exist, an arc is produced which converts the insulation to a conductive carbon residue. Polyimide insulation is prone to radial cracking which is a result of hydrolytic degradation in humid environments, and also a property known as memory effect where, after installation, the wire tends to regain its original manufactured lay (ie coiled on a spool). For these reasons, the use of polyimide-insulated wiring in ADF aircraft should be avoided. However, totally prohibiting its use is not always practical (or even possible). As such, where the use of this insulation is unavoidable, the ADF should ensure that the conditions that can lead to these undesirable properties, are absent. Obviously, the use of small amounts of this wiring in a sealed LRU presents a very low risk, and is acceptable without further analysis. For a non-sealed LRU, its use may still be acceptable if the undesirable conditions are absent, although some engineering analysis will be required to confirm this acceptability. For further detailed information on Polyimide insulated wire, refer to the DGTA website.

14. ***Hybrid Polyimide Insulated Wiring*****.** In an attempt to overcome the deficiencies of Polyimide insulation, a hybrid construction has been introduced and widely accepted by the civil aviation industry. This insulation consists of the basic polyimide insulation 'sandwiched' between two layers of fluoropolymer. This is a relatively new innovation and appears to have eliminated many of the problems experienced with Kapton. However, all insulation chemistries have some weakness and while this hybrid has performed well, it may not have been in service long enough at this time for any faults to arise, remembering that Kapton faults took six to eight years to initially surface. For this reason the use of hybrid polyimide insulated wire in ADF aircraft is discouraged. Where its use is unavoidable, details of quantities and areas of use should be well documented.

15. ***Prohibition of Polyvinyl Chloride (PVC) Insulated Wiring.*** Burning PVC releases hydrogen chloride (HCl) gas, which is very acidic in the presence of moisture. The HCl poses a health threat, and along with smoke, can be transported throughout the ventilated areas of an aircraft. The acidic HCl will also corrode electronic equipment. Coaxial cables historically have relied on PVC jackets in their manufacture and instances may arise where a PVC jacketed cable has no replacement. On rare occasions it may be necessary to utilise cables falling into this category, however, if used, they must be excluded from the flight deck, cabin and ventilation system.

NOTE

Clearly the use of PVC insulation in portable electronic devices and COTS role equipment does not conform to this requirement, since they are employed in the cabin. However, realistically almost all such equipment would contain PVC-insulated wire, so its use is probably unavoidable. The FAA also acknowledges this in Advisory Circular 25-16, by stating that wire such as PVC:

"… may be used inside the cases of video or audio tape players, television receivers, telephones, or other passenger convenience or entertainment equipment purchased on the general commercial market where similar, economically-feasible equipment having wire which complies with § 25.1359 (d) does not exist. In such instances, the equipment should be located where smoke or fire would readily be noticed, and a readily identifiable switch, located away from the equipment, should be provided to enable its safe and rapid disconnection."

This stance is logical and reasonable, and provides a convenient safety benchmark for ADF aircraft. Accordingly, the SDE may approve the use of PVC insulated wire in portable electronic devices and COTS role equipment within these same constraints.

16. ***Ribbonised Arranged Cable Systems.*** Ribbonised Arranged Cable Systems are considered suitable for use in ADF aircraft. This cabling system uses military specification wire woven into a flexible harness. As an extremely flexible wiring arrangement, ribbonised cable offers advantages in weight reduction and heat dissipation and allows a consistent baseline to be set for electromagnetic compatibility (EMC) design. Use of composite circular connectors is another weight saving measure that compliments ribbonised cable. However, composite connectors do not have the same level of immunity to the effects of lightning as metal connectors.

Circuit Breakers in Aircraft Electrical Systems

17. A circuit breaker is a device designed to open and close an electric circuit and to open the circuit automatically at a predetermined overload current, without damage to itself. The primary purpose of circuit breakers in ADF aircraft is to provide overcurrent protection for wire and cable and to minimise the danger of smoke and fire.

18. Correct circuit breaker selection should result in a protective device with the lowest standard rating that will not trip inadvertently. It must interrupt the fault or overload current by disconnecting the faulted line from the power distribution point before any wire or insulation damage occurs.

19. The nameplate current rating of circuit breakers is a nominal rating for identification and the actual useable rating for a particular application may be considerably different. Most circuit breakers will carry well over 100% of their rated current indefinitely. The applicable Military Standard (MS) should be reviewed when determining the actual trip current for a circuit breaker.

20. When selecting a circuit breaker for a particular application all the variables should be considered. These variables include time-current characteristics of the circuit breaker, start-up surges of equipment, wire type, size and location (ambient temperature) and the maximum altitude at which the equipment is likely to operate. The current carrying capacity of a wire varies considerably depending on the application and should be determined using the graphs contained in SAE AS50881.

21. Both magnetic and thermal type circuit breakers are available, however circuit protection in ADF aircraft is primarily provided by thermal circuit breakers which are dependent on temperature rise in the sensing element for actuation. Operation is achieved by deflection of a bi-metal strip that will open the circuit at a pre-determined temperature. Temperature rise in the sensing element is caused principally by the load current however this is affected by ambient temperature which can raise or lower the actual current at which the circuit breaker will trip.

22. Trip-free circuit breakers are normally used for all aircraft applications. Manual resetting of this type of circuit breaker cannot be effected while an over current circuit fault remains. Non trip-free circuit breakers are used

when the application requires over-riding of the tripping mechanism, in an emergency, when the fault still exists. Both types of circuit breaker can be manually operated to both ON and OFF positions with power applied, without damage to the electrical contacts, however circuit breakers should not be used as switches unless specifically designed for this purpose.

23. Where practicable, 'power in' and 'power out' wires should be physically separated to avoid the possibility of a short circuit negating the effect of the circuit breaker.

Lead-free Solder

24. Lead-free solder in new equipment is now a requirement throughout the European Union (EU). The legislation became effective from July 2006. Lead-free solder in electronics is already an accepted and widely practiced process in Japan and is rapidly being implemented worldwide.

25. Exemptions are provided for aerospace and defence contractors, however with the increased use of COTS equipment in military aircraft, and the use of commercial aircraft in military applications, it is inevitable that equipment containing lead free solder will be introduced into ADF aircraft.

26. It is imperative that all equipment containing lead-free solder be identified and documented during the acquisition/modification process and then clearly marked prior to installation into the aircraft. Any lead contamination of a lead-free solder joint will significantly reduce the reliability of the joint. Additionally, as there is currently no 'standard' lead-free solder, it will be necessary to identify the particular type of lead-free solder utilised in each individual component.

AIRCRAFT ELECTRICAL LOAD DATA ANALYSIS

27. ***Aircraft Acquisition Projects.*** An Aircraft Electrical Load Data (AELD) analysis should be provided during acquisition, with the data supplied in accordance with the requirements of MIL-E-7016F. The data should be provided in an appropriate electronic format to facilitate data transfer into the current ADF Aircraft Electrical Load Analysis software tool.

28. ***Aircraft Modifications.*** During an aircraft modification development process, the current AELD should be reviewed to provide assurance that the additional electrical loads are within the capacity of the power source and its associated busses, wiring and circuit protection devices. After acceptance/incorporation of the modification, the AELD should be amended to reflect the current aircraft configuration.

ASSOCIATED SPECIFICATIONS AND PUBLICATIONS

29. The following is a list of specifications and publications containing additional information on electrical power generation, storage and distribution systems:

a. AAP 7045.002-1, ADF Aircraft Wiring and Bonding Manual.

b. ANSI C18.1M, Portable Primary Cells and Batteries with Aqueous Electrolyte.

c. ANSI C18.2M, Portable, Rechargeable Cells and Batteries.

d. ANSI C18.3M, Portable Lithium Primary Cells and Batteries.

e. ARINC 609, Design Guidance for Aircraft Electrical Power Systems.

f. ASCC AIR STD 70/24, Aircraft Electrical System Characteristics.

g. ASTM F2490, Standard Guide for Aircraft Electrical Load and Power Source Capacity Analysis

h. BS 2G 239, Primary Active Lithium Batteries for Use in Aircraft.

i. MIL-B-29595, Batteries and Cells, Lithium, Aircraft, General Specification For.

j. MIL-B-8565, Battery Storage, Aircraft, General Specification For.

k. MIL-HDBK-454, General Guidelines for Electronic Equipment.

l. MIL-HDBK-5400, Electronic Equipment, Airborne, General Guidelines For.

m. MIL-STD-704, Aircraft Electric Power Characteristics.

n. MIL-STD-7080, Selection and Installation of Aircraft Electric Equipment.

o. MIL-STD-810, Environmental Test Methods and Engineering Guidelines.

p. RTCA/DO-160, Environmental Conditions and Test Procedures for Airborne Equipment.

q. RTCA/DO-227, Minium Operational Performance Standards for Lithium Batteries.

r. RTCA/DO-293, Minimum Operational Performance Standards for Nickel Cadmium and Lead Acid Batteries.

s. SAE ARD 50055, Aircraft Electrical Systems.

t. SAE ARP 1199, Selection, Application and Inspection of Electric Overcurrent Protective Devices.

u. SAE AS 58091, Circuit Breaker, Trip Free, Aircraft, General Specification for

v. STANAG 3219, Electrical Switches in Aircraft – Location and Grouping.

w. STANAG 3456, Electrical System Characteristics.

Annex:

A. Requirements for Aircraft Electrical Power Generation, Storage and Distribution Systems

REQUIREMENTS FOR AIRCRAFT ELECTRICAL POWER GENERATION, STORAGE AND DISTRIBUTION SYSTEMS

1. ***General Requirements.*** Regardless of the specification or standard used as a basis for an aircraft electrical power generation and distribution system, the following requirements apply:

a. Primary power systems should operate such that, through all phases of flight, ground operation and under any engine power setting, continuous operation of essential electrical loads is assured.

b. Aircraft external AC power supply receptacles and associated electrical circuits should comply with ASCC AIRSTD 25/19, Figure 4a to maintain standardisation with the ADF aircraft fleet and compatability with ground support equipment.

c. Aircraft bonding/grounding receptacles should comply with the requirements of MIL-STD-7080.

d. Aircraft bonding/grounding receptacles should be located on the aircraft as detailed in AAP 7045.002-1.

e. Aircraft electrical bonding should comply with the requirements of AAP 7045.002-1and MIL-STD-464.

f. Polyimide (Kapton) insulated wire and cable should not be used in the aircraft electrical system.

g. Polyvinyl Chloride (PVC) insulated wire and cable should not be used in the aircraft electrical system.

h. For all battery performance calculations, a figure which is 80% of battery rated capacity should be used.

i. Each circuit for essential loads should have individual circuit protection.

j. Circuit breakers should not be used as ON/OFF switches unless specifically designed for this purpose.

k. Electrical system functional testing, both ground and air, should be carried out to demonstrate compliance with the specified system characteristics and requirements.

l. An Aircraft Electrical Load Data (AELD) Analysis, in accordance with MIL-E-7016, should be provided.

m. Identification and marking of electrical wire and cable should comply with the requirements of AAP 7045.002-1 and SAE AS 50881.

n. Identification and marking of EMI sensitive wire and cable should comply with the requirements of AAP 7045.002-1.

o. Wiring for redundant systems should be separated to the maximum possible extent.

p. Fuel Quantity Indication wiring should be physically separated from power wires.

2. ***DEF STANDARD 00-970, Design and Airworthiness Requirements for Service Aircraft.*** If DEF STAN 00-970 is used as a basis for system certification, the following requirements should be included in addition to the general requirements listed in paragraph 1:

a. Where practicable, for standardisation, circular electrical connectors used in the aircraft electrical system should be qualified to MIL-DTL-5015 or MIL-DTL-38999.

3. ***MIL-STD-704, Aircraft Electric Power Characteristics.*** If MIL-STD-704 is used as a basis for system certification, the following requirements should be included in the system specification in addition to the general requirements listed in paragraph 1:

a. Equipment used in the electrical power generating and distribution system should be selected and installed in accordance with MIL-STD-7080.

b. Where practicable, for standardisation, circular electrical connectors used in the aircraft electrical system should be qualified to MIL-DTL-5015 or MIL-DTL-38999.

c. An independent emergency power source should be provided to supply power to all essential loads in the event of failure of the normal power source.

d. A reserve generating capacity, at least 50% greater than the maximum continuous demand, should be supplied to facilitate through life increases in electrical power requirements.

e. Allowance should be made for at least 10% increase in the number of main cable runs, connectors, and circuit breakers to facilitate through life development of aircraft systems.

f. Nickel Cadmium batteries which are part of the main electrical system should have an automatic charge control system and an overheat warning system with a means of disconnecting the battery from its charging source in the event of an over temperature condition.

g. The aircraft wiring installation should comply with the requirements of AAP 7045.002-1 and SAE AS 50881.

4. ***FARs/JARs.*** If FAR/JARs are used as a basis for system certification, the following requirements should be included in addition to the general requirements listed in paragraph 1:

a. The electrical system power characteristics should comply with the requirements of MIL-STD-704.

b. Provision for connection of external electrical power supplies to the aircraft electrical system should be incorporated using receptacles that are qualified to MIL-C-81790.

c. A reserve generating capacity, at least 50% greater than the maximum continuous demand, should be supplied to facilitate through life increases in electrical power requirements.

d. Allowance should be made for at least 10% increase in the number of main cable runs, connectors, and circuit breakers to facilitate through life development of aircraft systems.

e. Wiring harness power density should not exceed that specified in SAE AS 50881.

SECTION 2

CHAPTER 6

OXYGEN SYSTEMS

INTRODUCTION

1. ADF aircraft require the fitment of breathing equipment which can supply oxygen or a mixture of air and oxygen to crew members and passengers for protection against the effects of hypoxia at cabin altitudes above 10,000 feet, and against the inhalation of toxic materials which may be present in the aircraft in an emergency (refer DI(AF) OPS 3-5). Hypoxia is defined as any state where a physiologically inadequate amount of oxygen is available to, or is utilised by, body tissue and the brain.

2. Most common aerospace oxygen standards do not adequately address oxygen system requirements for ADF aircraft, and as a result, do not provide an adequate basis for certification of ADF oxygen systems. This chapter supplements the common aerospace oxygen standards to reflect current best practice oxygen system design and verification practices. Design requirements for aircraft oxygen systems utilising stored (high and low pressure) gaseous oxygen, stored liquid oxygen, or an on-board oxygen generating system (OBOGS) as the breathing gas source are discussed. Relevant military and civilian standards, as well as specific ADF requirements derived from operational experience and investigations carried out at Aeronautical and Maritime Research Laboratory (AMRL), have been included.

APPLICATION AND TAILORING GUIDANCE

General

3. Historically, when acquiring a new aircraft, the ADF generally accepted the oxygen system supplied with that aircraft, as most systems were based on existing military specifications. However, some current specifications may fail to provide a suitable end product, as they contain primarily functional compliance statements, leaving details such as selection of components and materials open to interpretation.

4. With the emergence of improved testing methods and technology, some materials that were widely accepted in the past, are now considered unsuitable for use in certain applications. For example, the use of aluminium is considered unsuitable for high-pressure oxygen applications. Unfortunately, many oxygen system components are still manufactured from these materials, and are generally the products offered by original equipment manufacturers (OEM), as they are the most economical. OEMs can usually supply alternative materials when required for a particular application. Reducing the risk of a fire or ‘explosion’ through the use of the most compatible materials is a priority for ADF oxygen systems.

Description of Applicable Standards

5. Depending on the aircraft and its proposed operations, the following specifications are considered suitable for acquisition provided the ADF requirements in annex A are included where appropriate.

6. ***JSSG-2010-10, Crew Systems Oxygen Systems Handbook.*** This handbook provides guidance for the development of requirements for aircraft oxygen systems. It is for guidance only and should not be cited as a requirement itself.

7. ***MIL-D-85520, Design and Installation of On Board Oxygen Generating Systems in Aircraft, General Specification For.*** This specification provides a detailed account of components and typical system layouts and requirements for an OBOG system. The specification divides the system into the bleed air oxygen delivery system and the oxygen enriched air system, and provides requirements for both sub-systems. Backup and emergency oxygen requirements are also discussed.

8. ***MIL-D-19326, Design and Installation of Liquid Oxygen Systems in Aircraft, General Specification For.*** This specification covers the general requirements for the design and installation of liquid oxygen systems (both 70 and 300 psig) in aircraft. It is a comprehensive document that details oxygen system requirements for fighter, bomber, transport and training aircraft. Tables covering crew and passenger oxygen requirements, converter characteristics and

various other system specifications are included. With effect 23 Jul 97, this specification was declared inactive for new designs. However, as it provides appropriate system design and component selection requirements for aircraft oxygen systems, it is considered suitable for ADF use.

9. ***MIL-D-8683, Design and Installation of Gaseous Oxygen Systems in Aircraft, General Specification For.*** This specification provides detailed information on components and system requirements for both high and low pressure gaseous oxygen systems in fighter, bomber, transport and training aircraft. Typical system layouts and associated military specifications are also provided. With effect 23 Jul 97, this specification was declared inactive for new designs. However, as it provides appropriate system design and component selection requirements for aircraft oxygen systems, it is considered suitable for ADF use.

10. ***DEF STAN 00-970, Part 1 Section 6.13, Oxygen Systems.*** This document provides a basic description of what is required in an oxygen system. There is less detail than that provided in the military specifications, however, all points are covered. The physiological requirements in this UK MoD document are similar to those of the ADF, since both the UK MoD and ADF are signatories to the relevant Air and Space Interoperability Council (ASIC) agreement on the physiological requirements for aircrew. DEF STAN 00-970 also briefly addresses material compatibility in oxygen enriched environments.

11. ***Federal Aviation Regulations.*** FARs provide commercial aircraft requirements for oxygen systems. They are safety of flight related and contain limited design requirements and no details of component or material specifications. Some physiological details are included and these are consistent with the requirements of the ASIC documentation. FARs alone are often inadequate for specifying ADF oxygen systems and additional ADF requirements must normally be included.

12. ***Oxygen Equipment Installation.*** The following standards are guides for use in selecting materials for applications relating to the production, storage, transportation, distribution and use of oxygen: ASTM G 63, Standard Guide for Evaluating Non-Metallic Materials for Oxygen Service; and ASTM G 94, Standard Guide for Evaluating Metals for Oxygen Service. The purpose of these guides is to furnish qualified technical personnel with pertinent information for use in selecting materials for oxygen service in order to minimise the probability of ignition and the risk of ‘explosion’ or fire. They are not intended for use as specifications for approving materials for oxygen service.

Design Considerations

13. An aircraft oxygen system consists of the following oxygen subsystems: the crew breathing systems (main, backup and emergency); paratrooper systems; aero-medical systems; passenger oxygen systems; and walk around (portable) oxygen systems. The oxygen subsystem characteristics are all dependent on the aircraft role, and various subsystem components are common to ADF aircraft, including demand regulators, supply source (cylinders and converters), heat exchangers, content gauges, filler valves, pressure reducing valves, filters, tubing, etc.

14. The design considerations for an aircraft oxygen system involve all the oxygen subsystem characteristics, maintenance, safety and interface options. A brief description follows:

a. Oxygen subsystem characteristics include the physical, operational and electrical aspects, environmental conditions, electromagnetic radiation immunity and materials selection for oxygen compatibility. Further details of each are as follows:

(1) ***Physical Characteristics.*** The physical characteristics are the supply source, plumbing, regulators, valves, hoses, face masks, warning systems (sound / indicators) etc. Considerations include volume/space constraints, weight and centre of gravity constraints, and oxygen system interface with other aircraft systems.

(2) ***Operational Characteristics.*** Normally these will be unique to the aircraft type. Prime considerations are that the oxygen system should function properly under all envisaged operating conditions such as high “G” forces or that the engine performance is not degraded by the demands of the OBOGS system. Other operational considerations could be that indicators and controls are visible and easily accessed and operated by the crewmember without interfering with other crewmembers tasks.

(3) ***Electrical Characteristics.*** Power requirements should be considered. As the oxygen system is a primary life support system, an independent back-up power supply or connection to the aircraft emergency power system may be required.

(4) ***Environmental Conditions.*** There are many factors to be considered including low and high temperature exposure, altitude cycling, humidity, salt, dust, vibration, acceleration loading and explosive decompression.

(5) ***Electromagnetic Radiation Immunity***. Oxygen system electric and electronic controls should be tested to confirm appropriate immunity.

(6) ***Material Selection for Oxygen Compatibility.*** Materials selection is addressed in Para 18.

b. Accessibility, maintainability and serviceability design considerations are important aspects often overlooked. Factors include:

(1) Special tools should not be required for removal and replacement of oxygen system components.

(2) Leak tests will need to be conducted on oxygen system plumbing, necessitating easy access to joints etc.

(3) Oxygen breathing masks and delivery hoses are subject to damage if not properly stowed when not in use; however stowage must not compromise rapid donning of the mask assemblies in an emergency.

(4) All systems require periodic replenishment and maintenance. It is therefore essential that quick and easy major component replacement capability be provided in the system design.

c. Safety design considerations include:

(1) The design should locate supply sources and route plumbing to minimise hazards. For example, do not locate storage containers under or near hydraulic accumulators.

(2) Appropriate warning indications, labelling and marking should be detailed in oxygen system design.

(3) The design should enable ease of maintenance and facilitate contamination prevention.

d. If an oxygen subsystem interfaces with other oxygen subsystems (eg. portable system connects to the main system for recharging or an aero-medical system connects to a main system for supply) then the overall oxygen system performance should also be considered (ie. is the oxygen supply sufficient to support both subsystems). If the oxygen subsystem interfaces with an aircraft system (eg. an OBOGS system obtaining bleed air from an engine or environmental control system) then consideration must be given to ensuring that the operational envelope of the supply system (engine or ECS) is not exceeded.

ADF Unique Design Requirements

15. ADF unique design requirements are a result of investigations carried out at AMRL, in conjunction with the efforts of AESSO-ALSE, into oxygen system defects and incidents that have occurred in the past. Certain incidents have caused considerable damage (Orion and Caribou fires in the early 1980s) and there have been other similar incidents of oxygen system internal fires that fortunately have self extinguished with only minor internal damage. Contamination is of prime concern, necessitating the use of filters, the most appropriate materials and components and safe working practices; all of which will minimise the risk of a fire or ‘explosion’ in an oxygen system.

16. ADF unique design requirements are contained in annex A, while the rationale behind the requirements are included in paragraphs 17 to 20. ADF unique requirements for oxygen systems take precedence over other requirements detailed in referenced specifications and standards.

17. ***Filters.*** A filter with a particle retention of 12.5 micron or less should be used within gaseous filler valves, upstream of the check valve. Similar size filters should also be used at the inlet to pressure reducers.

a. ***Rationale.*** Particulate contamination and the resultant effects are highly undesirable in any oxygen system, particularly high-pressure gaseous oxygen systems. The action of connection and disconnection of ground support equipment used to replenish oxygen systems will produce swarf that is injected into

the oxygen system. This process cannot be avoided. Pressure reducers also naturally create a region of increased gas velocity through the design of the component and this also cannot be avoided. Hence, a safety measure is to install a filter to entrap any contaminant produced by system operation (system replenishment) before it enters these regions of increased risk. Another region of increased risk is the inlet to oxygen regulators, however, this is not discussed here as regulators are fitted with filters at their inlets as part of the regulator design. When choosing an oxygen regulator, care should be exercised to ensure the filter supplied with the regulator is capable of adequately filtering the inlet gas and is firmly secured.

18. ***Materials Selection.*** Materials for use in oxygen systems should be selected using guidance contained in ASTM G 63 and ASTM G 94, and details contained in annex A to this chapter.

a. ***Rationale.*** The selection of the most appropriate material for use in an oxygen enriched atmosphere is primarily a matter of understanding the circumstances that cause oxygen to react with the material. Most materials in contact with oxygen will not ignite without a source of ignition energy. When this energy input exceeds the configuration dependent threshold, ignition and combustion may occur. Thus, the material flammability properties and the ignition energy sources within a system must be considered. These should be viewed in the context of the entire system design so that specific factors will assume the proper relative significance.

19. ***Liquid Oxygen Converters.*** Stabilised liquid oxygen converters should be used in aircraft where the converters cannot be readily removed for replenishment.

a. ***Rationale.*** Following replenishment of a liquid oxygen converter, thermal stratification takes place and the converter cannot be used for periods of six to twelve hours, dependent on converter size and operating pressure. The phenomena of thermal stratification occurs when a converter is replenished and the colder liquid, introduced during filling, settles to the bottom, leaving a layer of the warmer original liquid on top. If shaken or disturbed during the initial stabilisation period, the colder liquid at the bottom of the converter mixes with the slightly warmer liquid at the top of the converter and reverts some of the boiled off gas back to a liquid. This results in a drop in the pressure created by the gas, preventing delivery and hence, system failure. This phenomena has been observed in many liquid oxygen systems and may be overcome by one of the following practices:

(1) Using stabilised converters. A stabilised converter, in this context, is one which contains either a mixing device in the converter to allow the temperature to equalise more quickly, or one which has a secondary uninsulated canister which allows the liquid in it to boil off rapidly and then pass back through the main liquid converter producing a stirring effect, thus more rapidly equalising the temperature in the main converter.

(2) Replacement of an empty converter with a full converter, which has been allowed to reach a stable temperature (this option is only practical where the aircraft system is designed for out-of-frame replenishment, such as the F/A-18).

(3) Wait the required stabilisation period after replenishment of the aircraft converter, grounding the aircraft for this time.

20. ***Pressure Reducing Valves (PRV).*** The fitment of pressure reducing valves as an integral part of the cylinder valve in both main and portable high-pressure gaseous oxygen systems is highly desirable. Where this is impractical, the PRV is to be positioned as close as possible to the supply source.

a. ***Rationale.*** MIL-D-8683 states that pressure reducing valves may be fitted if required. Past experiences have shown there is a definite requirement for pressure reduction prior to the oxygen regulator in high-pressure gaseous oxygen systems. The Caribou fire and numerous high-pressure portable oxygen regulator fires confirm the need to reduce the pressure prior to the regulator.

ASSOCIATED SPECIFICATIONS AND STANDARDS

21. The following list of specifications and standards provides additional information relating to the design, construction and operation of aircraft oxygen systems:

a. ASIC AIR STD 15/14A, Breathing Oxygen Characteristics (Including Supply Pressure and Hoses);

b. ASIC AIR STD 25/27B, Aircraft Liquid Oxygen Replenishment Connections;

c. ASIC AIR STD 25/34A, Aircraft Gaseous Oxygen Replenishment Connections;

d. ASIC AIR STD 61/101/02C, Physiological Evaluation of Aircraft Oxygen Delivery Systems;

e. ASIC AIR STD 61/101/06A, Minimum Physiological Requirements for Aircrew Demand Breathing Systems;

f. ASIC AIR STD 61/101/10, The Minimum Quality Criteria for On-Board Generated Oxygen;

g. ASIC AIR STD 61/101/15, Minimum Standards For Smoke Protection Breathing Equipment Used by Mobile Aircrew in Non Ejection Seat Aircraft at Pressure Altitudes up to 10,000 Feet;

h. ASIC AIR STD 61/101/16, Minimum Standards For the Protection of Aircrew Against Hypoxia and Decompression Sickness on Parachuting Operations Between 25,000 and 38,000 Feet;

i. ASTM A269-04, Standard Specification for Seamless and Welded Austenitic Stainless Steel Tubing for General Service

j. ASTM G 88-05 Standard, Guide for Designing Systems for Oxygen Service;

k. ASTM G 128-02e1, Standard Guide for Control of Hazards and Risks in Oxygen Enriched Systems;

l. ASTM Manual 36, Safe Use of Oxygen and Oxygen Systems, Guidelines for Oxygen System Design, Materials Selection, Operations, Storage and Transportation

m. Australian Standard, AS 1572-1998, Copper and Copper Alloys - Seamless Tubes for Engineering Purposes;

n. British Standard 4N100 - General Design Requirements for Aircraft Oxygen Systems and Equipment;

o. MIL-PRF-27210, Oxygen, Aviators, Breathing, Liquid and Gas;

p. NASA Reference Publication 1113, Design Guide for High Pressure Oxygen Systems;

q. NATO STANAG 3198 ED 4.4, Functional Requirements of Aircraft Oxygen Equipment and Pressure Suits;

r. NATO STANAG 3296 ED 1.7, Aircraft Gaseous Oxygen Replenishment Couplings;

s. NATO STANAG 3545 ED 2.6, Characteristics of Breathable Liquid Oxygen;

t. NATO STANAG 3865 ED 2.5, Physiological Requirements for Aircraft Molecular Sieve Oxygen Concentrating Systems;

u. SAE AIR 822 - Oxygen Systems for General Aviation;

v. SAE AIR 825 - Oxygen Equipment for Aircraft; and

w. SAE AMS-T-7081, Tube Aluminium Alloy, Seamless, Round, Drawn, 6061, Aircraft Hydraulic Quality.

ASSOCIATED INSTRUCTIONS AND PUBLICATIONS

22. Other ADF publications that should be referenced during the design/selection/modification of an oxygen system are:

a. DI(AF) AAP 7002.023, Oxygen General, General and Technical Requirements.

b. AAP 7055.001-99, Liquid and Gaseous Dry Breathing Oxygen Maintenance Instructions.

c. AAP 7550.001-2M, Oxygen Equipment.

d. RAAF SPEC (ENG) G172, Quality Standards and Testing of Liquid and Gaseous Dry Breathing Oxygen For Aircrew Use.

Annex:

A. Oxygen System Requirements

OXYGEN SYSTEM REQUIREMENTS

1. Oxygen Systems General. Regardless of the type of oxygen system to be installed in an ADF aircraft, the following requirements should be included:

a. Breathing oxygen, used in ADF aircraft, should comply with the requirements of RAAF Spec Eng G172, Quality Standards and Testing of Liquid and Gaseous Dry Breathing Oxygen for Aircrew Use.

b. Materials used in aircraft oxygen systems should be selected using guidance contained in ASTM G63 and ASTM G94.

c. In addition to paragraph 1b, the following materials requirements should apply:

(1) For all plumbing exposed to oxygen pressures above 500 psi, annealed copper tubing qualified to AS 1572-1998 or an alternative assessed as acceptable to the TAR, should be used.

(2) For all plumbing exposed to oxygen pressures up to 500 psi, corrosion resistant steel tubing qualified to ASTM A269, annealed copper tubing qualified to AS 1572-1998, or an alternative assessed as acceptable to the TAR, should be used.

(3) For all plumbing exposed to oxygen pressures up to 150 psi, aluminium alloy tubing qualified to MIL-T-7081D, corrosion resistant steel tubing qualified to ASTM A269, annealed copper tubing qualified to AS 1572-1998, or an alternative assessed as acceptable to the TAR, should be used.

(4) Stainless steel (316 corrosion resistant steel) should be used for circlips exposed to enriched oxygen flow.

(5) Oxygen cylinders manufactured from aluminium should not be used in ADF aircraft.

(6) Composite oxygen cylinders constructed with an aluminium liner should not be used in ADF aircraft.

d. Cadmium plated components, including circlips, should ***not*** be used in aircraft oxygen systems where they are exposed to enriched oxygen flow.

e. The physiological requirements for aircrew breathing systems should comply with ASIC AIR STD 61/101/6A, (formerly ASCC AIR STD 61/22A). Consideration should be given to the following:

(1) For particular aircraft types (ie. unpressurised) it may be necessary to depart from the physiological requirements specified in ASIC AIR STD 61/101/6A. For example, the lowering of the pressure altitude that safety pressure is onset or lowering of the altitude that automatic switchover to 100% oxygen occurs, are two parameters that may be varied to allow for special considerations such as medium altitude flight for long periods in unpressurised aircraft. Contractors should detail all variations from the nominated standard and the rationale for these variations.

(2) The effects of G can be very fatiguing, and high G induced loss of consciousness is a major concern. The use of Positive Pressure Breathing (PPB) equipment, also referred to as pressure breathing with G (PBG), reduces fatigue and allows the crewmember to fly more efficiently, comfortably and for longer periods in high G situations. Peak G tolerance is also enhanced.

(3) Because PPB equipment provides increased intrathoracic pressure in the lungs as a function of increasing G, a chest counter pressure garment, in conjunction with a lower body G suit inflated to the same pressure as the mask, makes the crewmember forcibly exhale rather than strain to inhale. A mask tensioning device is also used to allow higher mask pressures during the PPB phase of flight.

(4) As the ADF is evaluating the use of PPB equipment for its fast jet fleets, Contractors should detail the ability of their proposed solution to be equipped with PPB oxygen systems either on delivery or as an in-service modification.

f. Overall oxygen consumption requirements should be met from calculations complying with MIL-D-8683, MIL-D-19326, MIL-D-85520 or DEF STAN 00-970.

g. Oxygen regulators should be of the diluter demand type. Preference is for diluter demand type regulators however, depending on the selected oxygen system and aircraft role, this requirement may not always be appropriate.

h. Oxygen regulators should be of the panel mounted type. Preference is for panel mounted regulators however, depending on aircraft type and role, chest or seat mounted regulators may be more appropriate.

i. All cockpit oxygen system controls and connections operated by the pilot should be operable with the pilot's single gloved hand.

j. The oxygen regulator mode control function should transition the oxygen regulator, under pilot control, to the following modes. Depending on the oxygen regulator selected, all of the listed modes may not be required.

(1) ON (allowing the flow of oxygen),

(2) OFF (terminating the flow of oxygen),

(3) air-mix,

(4) 100% oxygen,

(5) emergency, and

(6) mask test.

k. All cockpit oxygen system hose connections operated by aircrew should lock positively. Bayonet connections are preferred.

l. When the aircraft cabin altitude is greater than 10,000 feet, and nil or continuous oxygen flow occurs for 15 seconds on any oxygen regulator, the pilot should be advised by the following:

(1) a master caution light,

(2) a panel warning light, and

(3) an audible warning which may be cancelled under pilot control.

m. All oxygen supply warning systems and instrumentation should be operable upon initial aircraft power up and should remain operable under all flight conditions.

n. If required, aircraft should incorporate an emergency oxygen supply, independent of the main oxygen system, capable of supplying oxygen during an emergency or ejection.

o. The aircraft should have provision for checking the contents of the emergency oxygen supply.

p. Sintered tin-bronze filters with a particle retention capability of 12.5 micron or less should be used in gaseous filler valves upstream of the check valve and at the inlet of pressure reducers. Oxygen gas velocity is highly accelerated at pressure reducers and this is where particulate contamination is most likely to cause a fire. Due to the potential for generation of heat at very fine filters, the filter and its housing should be designed to facilitate the dissipation of heat to the maximum extent possible.

q. Filters should be readily accessible for replacement or cleaning.

r. Vent valves should be used to facilitate safe depressurization of oxygen systems prior to maintenance.

s. Oxygen system venting should be routed overboard.

t. Main ON/OFF valves should:

(1) use brass-on-steel (316 corrosion resistant steel) seats, and

(2) have at least six full turns from the fully closed to fully open position.

u. A visual indication of nil flow, demand flow, and continuous oxygen flow should be provided to each pilot and crew station.

v. Oxygen system storage cylinders should have an ON/OFF valve so that the cylinders may be disconnected and removed from the aircraft without the need to empty cylinder contents.

w. In transport and maritime aircraft capable of operations at altitudes between 10 000 feet and 35 000 feet, all aircrew should have access to oxygen masks for immediate use in an emergency.

x. In transport aircraft capable of operations at altitudes above 30 000 feet, oxygen masks should be available to all passengers.

y. Where there is a requirement for aircrew to use oxygen, portable oxygen equipment should be available for aircrew if there is a requirement for them to move about the aircraft.

z. In aircraft capable of operating between 41 000 feet and 50 000 feet, a pressure breathing capability should be employed.

aa. In aircraft capable of operating above 50 000 feet, pressure suits should be employed.

2. Gaseous Oxygen Systems. High pressure gaseous oxygen systems are preferred over low pressure gaseous oxygen systems as the capacity of low pressure systems is limited by the quantity of cylinders necessary to obtain the required system endurance. If the aircraft is to contain a gaseous oxygen system, the following requirements should be included in the system specification over and above the general requirements listed in paragraph 1:

a. High pressure gaseous oxygen systems (500 to 2200 psi) should comply with the requirements of MIL-D-8683 and ASIC AIR STD 25/34A.

b. High pressure gaseous oxygen systems (500 to 2200 psi) should incorporate a pressure reducer valve at the cylinder or as close to the cylinder as practicable.

c. High pressure gaseous oxygen systems (500 to 2200 psi) should incorporate a filter at the inlet to the oxygen regulator. This filter is normally incorporated into the oxygen regulator by the manufacturer and is usually acceptable for ADF requirements.

d. All cockpits should be provided with an indication of the following:

(1) oxygen supply pressure, and

(2) oxygen storage vessel pressure.

3. Liquid Oxygen Systems. Liquid oxygen systems have an advantage over gaseous systems in that the expansion rate of liquid to gas provides a large supply of oxygen in a small volume at relatively low pressure. The disadvantage of liquid oxygen is that it is constantly being reduced by evaporation, which, in addition to the obvious wastage, also causes a build up of contaminants that remain when the oxygen boils off. Evaporation losses can range from 5% to 20% in a 24 hour period. If the aircraft is to contain a liquid oxygen system, the following requirements should be included in the system specification in addition to the general requirements listed in paragraph 1:

a. Liquid oxygen systems (70 psig and 300 psig) should comply with the requirements of MIL-D-19326, and ASIC AIR STD 25/27B.

b. Liquid oxygen systems (70 psig and 300 psig) in aircraft where the converters cannot be readily removed and replaced, should incorporate a thermal stratification stabilised liquid oxygen converter that does not require a destratification waiting time of more than 30 minutes after filling. Liquid oxygen system (70 psig and 300 psig) converters that are easily removable to facilitate out of airframe replenishment are preferred.

c. Liquid oxygen system (70 psig and 300 psig) heat exchangers should be rated to match the maximum converter flow rate.

d. All cockpits should be provided with an indication of the following:

(1) oxygen supply pressure, and

(2) liquid oxygen volume remaining.

4. Onboard Oxygen Generating Systems (OBOGS). OBOGS have the same supply advantage as liquid oxygen over the gaseous systems but without the logistics problems associated with storage and dispensing of the liquid. The disadvantage with OBOGS is that the maximum oxygen concentration obtainable is around 94%. Additionally, the effects of low engine power settings on the oxygen output supply should be critically assessed. In certain aircraft installations, the pressures at which air is supplied to the Molecular Seive Oxygen Concentrator (MSOC) during engine low power settings may be insufficient to provide a flow of product gas at an adequate pressure.

5. If the aircraft is to contain an OBOGS, the following requirements should be included in the system specification over and above the general requirements listed in paragraph 1:

a. The On-Board Oxygen Generating System (OBOGS) should comply with MIL-D-85520.

b. The OBOGS should not require planned removal from the aircraft at intervals less than that of the deepest level of maintenance.

c. The OBOGS should achieve a MTBF of at least 2500 hours.

d. The pressure at which air is supplied to the Molecular Seive Oxygen Concentrator (MSOC) during engine low power settings should be sufficient to provide a flow of product gas at an adequate pressure for all envisaged operating requirements. (Refer paragraph 1e)

e. The backup oxygen supply for the OBOGS should be mounted so that it does not occupy space within the survival pack seat pan.

6. Chemical Oxygen Generators. Chemical oxygen generators are primarily used in civilian aircraft as emergency supply sources. As there are several disadvantages with chemical oxygen generators, specialist review and approval must be obtained prior to use in ADF aircraft.

SECTION 2

CHAPTER 7

SOFTWARE FOR AIRBORNE AND RELATED SYSTEMS

INTRODUCTION

1. Rapid increases in the processing power and storage capacity of digital computers and the widespread adoption of digital avionics in aircraft have lead to unprecedented levels of complexity in weapon system software. This complexity is driven by the integration of previously federated functions into software hosted on common computing resources, along with the addition of new functions and software technologies themselves only now possible because of the technology increases and proliferation of modern digital computers. Furthermore, there has been extraordinary growth in the use of computers and software to monitor and/or control safety related sub-systems and functions. While these advancements have lead to new and enhanced weapon system capabilities, the increase in complexity has driven corresponding increases in the technical, cost and schedule risk associated with the development and maintenance of weapon system software. Only through the appropriate application of software safety engineering and management best practice is it possible to constrain these risks.

2. This chapter identifies a number of 'key issues' which DGTA considers fundamental to establishing a successful development program for ADF aerospace software. While their adoption is not mandatory, justification for their omission would normally be expected.

SCOPE AND APPLICABILITY

3. This chapter discusses those aspects of design acceptance that pertain to software for airborne systems and equipment, or ground based equipment that have physical and/or functional interfaces with these systems. It is intended for the acquisition of new, or modification of existing, software intensive weapon systems (including in-service support) but is not intended for the in-service engineering management of those systems (refer to Section 2, Chapter 17 for this).

SOFTWARE SYSTEM SAFETY

4. The purpose of Software System Safety is to provide assurance that the software will execute with an acceptable level of safety within the system context. A software specification error, design flaw, or the lack of initial safety requirements can contribute to or cause a system failure or erroneous human decision. Software System Safety is used to address software's contribution to aircraft hazards. It is an element of the total system safety and software development program and cannot function independently of the total effort. It involves the identification of system level hazards, software's contributions to those hazards, development of requirements to mitigate the hazards and the development of software to provide assurance that the hazards do not occur or that they have been adequately mitigated. Software System Safety brings together elements of traditional system safety approaches in conjunction with approaches used to address the unique properties of software.

Software Safety Program

Key Issue: A Software Safety Program (SwSP) should be established to coordinate hazard identification and mitigation efforts for hazards with software-related causal factors.

5. A Software Safety Program that fully supports the System Safety Program is required for all software intensive system developments containing safety critical or safety related software. MIL-STD-882C or FAR/JAR 2X.1309 are the ADF's preferred System Safety paradigms. For more information on these standards and their associated application, the reader should refer to Section 2 Chapter 1 of this manual. While both these paradigms require software to be considered within the system context, in isolation neither provides adequate guidelines for conducting the software activities required to assure that the software will execute with an acceptable level of safety. IEEE STD 1228-1994, 'Standard For Software Safety Plans', provides an industry accepted standard for the preparation and content of a Software Safety Program Plan (SwSPP). Specific tasks, processes, and activities detailed in this standard can be integrated into the System Safety Program Plan (SSPP) or documented separately in the SwSPP. Guidance on the development and implementation of an effective Software Safety process can be sourced from the US Joint Software System Safety Committee Software System Safety Handbook (JSSSCSSSH).

Interaction of the Software Safety Program with the System Safety Program.

6. An effective Software Safety Program should functionally link software architecture to hazards and their failure pathways. The results of all software safety analyses should be formally documented in a closed-loop hazard tracking database. The information should be correlated in such a manner that it can be easily and systematically extracted from the database to produce the necessary deliverable documentation (ie. PHA, SRCA, SSHA, SHA, O&SHA, FMEA, etc.) as required by the deliverables of the System Safety Program. The maturity of the software safety analysis should be commensurate with the maturity of system design in accordance with the acquisition life cycle phase. All software safety analyses should be conducted and made available to support the goals, objectives and schedule of the parent System Safety Program.

7. To achieve an acceptable level of safety for software used in critical applications, software safety engineering must be given primary emphasis early in the requirements definition and system conceptual design process. Poor Software Safety Programs that lag development inevitably result in the safety engineer trying to defend an already developed product rather than conscientiously ensuring appropriate rigour was applied from the outset. This leads to an over reliance on procedural or training mitigations for hazards that should have been eliminated through design selection, or removed through the incorporation of safety features or devices. If left unchecked, safety mitigators will not be commensurate to risk. In this situation, the safety engineer must ensure that a systematic approach of hazard analysis, risk assessment, and risk management continues to be applied (or is applied retrospectively). In severe cases, this may involve a temporary cessation of project development and a corresponding acceleration of the system safety program. Programs in this situation should seek guidance from DGTA immediately.

8. Consideration should be given to linking milestone payments to not only the developers' implementation of functionality, but also to the system and safety analyses that have been completed for that phase of the project. To ensure that significant engineering issues are recognised and reflected in the payment schedule, project managers should stress the importance of this issue to the commercial managers in their project to have the contract provide incentives for the achievement of these milestones.

Software Safety Requirements and the Safety Case

9. The Safety Case produced by the System Safety Program should encompass software, so the outputs of the SwSP should be produced cognisant that they will eventually be incorporated within an overall Safety Case. Thus the SwSP should identify the top level approach used to argue the safety of software, and how this will guide the generation of software safety (analysis and test) evidence throughout the SwSP.

10. One propitious approach to argue the safety of software is to provide evidence of the absence or handling of all potential software failure modes. Software failure modes refer to the software's failure to carry out an intended or implied function, OR the software carries out a function that was not intended. Specific software failure modes might include the omission and commission of services, timing inconsistencies (early or late execution of services), and value based failures in services. Services are defined as a communication event, such as a data or control flow within the software. Techniques that specifically support this approach, in terms of analysis outputs that form appropriate evidence, include the Software HAZOP (Def Stan 00-58 Computer HAZOP), and Software Hazard Analysis and Resolution in Design (SHARD) – a refinement of Software HAZOP. Other software specific techniques such as software functional failure analysis, software fault tree analysis, markov analysis, petri nets, and sneak software analysis can be used to complement this approach. These analyses are useful for generating the necessary lower-level software requirements to ensure that the software will execute with an acceptable level of safety risk within the system context. Additionally, these analyses should form part of the evidence used to support the software aspects of the safety case argument.

11. Apart from those software requirements generated from analyses to address specific identified risks, software requirements may also be derived from general design requirements and guidelines for safety critical software; for example, those described in the Appendix E to the JSSSCSSSH. These general design requirements are a useful reference to software safety requirements from previously developed safety critical and safety related systems, and should not be discounted from any new development without careful consideration.

12. Programs are advised to seek DGTA advice on the adequacy of their software safety argument if it differs significantly from the approach described here. Programs should also seek DGTA advice on the quantity of software safety evidence (analysis and test) that is required commensurate with the risk for supporting the software safety argument.

Independent Safety Assessors

Key Issue: An Independent Safety Assessor (ISA) is recommended where there is significant development of safety critical software components, no approved National Airworthiness Authority is involved and where the level of expertise of Software System Safety within the Project Office is assessed as low.

13. The role of an ISA is to provide an independent professional opinion that system hazards have been appropriately identified and subsequently reduced to an acceptable level. Since the safety assessment provided by the ISA is independent of existing safety analysis and assessment, it provides confidence that safety claims are justified and any weaknesses are identified and dealt with. As well as providing assurance of safety, using an ISA can help to focus safety planning and analyses. This can come about naturally by answering questions and providing safety information for the ISA. In addition, an ISA is often able to offer generic guidance that does not compromise independence, particularly in the early stages of a project.

14. For further information on ISAs, the reader is referred to Section 2 Chapter 1 of this manual as well as the compliance finding and design acceptance guidance found at Annex C to this chapter.

Capability Maturity vs Software Safety.

15. Capability models such as the Capability Maturity Model Integration (CMMI®) for Systems, Software and Integrated Product and Process Development (CMMI-SE/SW/IPPD) provide a framework against which an organisation's ability to produce a product of defined quality within cost and schedule constraints can be assessed. Such maturity models can provide motivation for organisations to improve their processes for the benefit of both the organisation and the Commonwealth. Defence Materiel Organisation has extended CMMI® to include organisational safety maturity. The extension, called +SAFE v1.1, covers the key practices for appraising safety engineering and safety management process maturity. While CMMI+SAFE does provide valuable insight into the maturity of an organisation's safety culture, it does not provide the level of airworthiness assurance that a safety-related development standard provides. Therefore, a CMMI+SAFE accreditation should not be considered an alternative to an appropriately applied software safety program. For further information on the CMMI process and its usage in Defence acquisition and sustainment refer to the DMO Quality and Environmental Management System (QEMS).

Integrating Software Assurance Requirements into the Software Safety Process.

16. Software assurance is an integral and necessary component of the Software Safety Program. Software assurance is covered in greater detail in the next section of this chapter, however for the purposes of understanding the relationship to software safety, some high level software assurance principles will be discussed here.

17. Unlike hardware components that are subject to random failures (e.g. wear in or wear out failures) which generally can be characterised by failure probability distributions, software does not fail randomly. Instead latent defects in software can cause it to fail systematically when the set of initial conditions and internal state cause the section of code containing the latent defect and related data to be executed. While there has been some effort amongst researchers to characterise such failures using probabilistic means and quantify software reliability, such approaches are not widely accepted. Therefore, the traditional use of a Hazard Risk Index Matrix characterising risk as a function of severity and probability is unsuitable for application to software because there is no easy means to define a probability for software. This problem is, however, recognised by system safety and software assurance standards, and alternative means of defining a Hazard Risk Index and integrating software assurance requirements have been defined; although approaches do differ between standards and Commercial or Military paradigms. The following is a brief description of the common approaches:

a. **FAR/JAR 2x.1309 programs**. The FAR/JAR 2x.1309 paradigm normally involves a SAE ARP4754/4761 System Safety Program integrated with Software Assurance as defined in RTCA/DO-178B. Further information on RTCA-DO-178B is provided in the next section of this chapter. For programs using this paradigm, software levels and processes for compliance, as defined in RTCA/DO-178B, are related to the failure condition classifications and are assigned taking account of the item development assurance level as defined in SAE ARP4754 (refer Table 7-1). The system's development assurance levels are assigned based on the most severe failure condition classification associated with the applicable aircraft-level function. This approach basically ignores any concept of software reliability and assigns assurance levels directly against failure condition severities.

Table 7–1 SAE ARP4754 Development Assurance Level Assignment

Failure Condition Categorisation	Development Assurance Level (RTCA/DO-178B Software Level)
Catastrophic	A
Hazardous / Severe Major	B
Major	C
Minor	D
No Safety Effect	E

b. **MIL-STD-882C programs**. For programs using MIL-STD-882C, a Software Hazard Risk Index is defined based on the hazard category or failure condition severity and a control category as defined in an accepted SHRI matrix for the program (refer Table 7-2). This approach also basically ignores any concept of software reliability and assigns assurance levels directly against failure condition or hazard severities. It also extends the approach by considering the degree of direct control the software exercises over the function (i.e. the control category – refer MIL-STD-882C for control category definitions). The basic principle behind control categories is that the less direct control the software has over the functions, then some relaxation of software assurance may be permissible. The SHRI should then be mapped to a software level, such as those defined in RTCA/DO-178B, to define the level of effort and rigour applied to each design phase commensurate with the safety risk of the system and its related functionality (refer Table 7-3). Alternatively a Software Assurance Task Matrix can be developed (refer to the section on In-Service Software Modifications for further information on developing a Software Assurance Task Matrix).

Table 7–2 Example Software Hazard Risk Index Matrix from MIL-STD-882C

HAZARD CATEGORY / CONTROL CATEGORY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
I	1	1	3	5
II	1	2	4	5
III	2	3	5	5
IV	3	4	5	5

Table 7–3 Example MIL-STD-882C Software Risk Index Mapped to Software Level

Software Hazard Risk Index	Suggested Criteria	SAE ARP4754 Development Assurance Level (RTCA/DO-178B Software Level)
1	High risk - significant analysis and testing resources	A
2	Serious risk - requirements and design analysis and in-depth testing required	B
3-4	Moderate risk - high level analysis and testing acceptable with Managing Activity approval	C-D
5	Low Risk – Acceptable	E

SOFTWARE ASSURANCE

18. Software Safety is an integral component of the overall System Safety program. Likewise, software assurance is an integral component of the Software Safety program. Software assurance is the systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures. "Processes" include all of the activities involved in designing, developing, enhancing, and maintaining software; "products" include the software, associated data, its documentation, and all supporting and reporting paperwork.

19. The Software Safety Program delivers safety requirements and software levels as input to the software assurance program. Output from the software assurance program includes further formalisation of derived requirements and evidence of the verification of these requirements.

Software Assurance Standards

Key Issue: A software assurance standard is required for the development of all software that is safety related.

20. Software assurance standards rely on the identification of software's contribution to system level failure; most allocate an associated Software Level based on the severity of this failure. Some standards allow the software level to be adjusted based on the degree of control it has over a system or the probability of an accident once the failure has occurred. The software level is then used as the basis for allocation of development objectives to the software development process. As the software level increases, more rigorous development requirements are applied.

21. Safety related software can be considered as all software whose anomalous behaviour, as shown by the system safety assessment process, would cause or contribute to a failure condition that affects the aircraft operational safety or pilot workload. DGTA recognises that the FAA processes and standards for software in airborne systems are widely used in industry, and accepted by many international airworthiness authorities. Hence, RTCA/DO-178B is the ADF's preferred software assurance standard for safety related airborne software development. DEF STAN 00-55 is a suitable alternative standard to RTCA/DO-178B. Where alternative standards are proposed, RTCA/DO-178B should be used as the benchmark against which the proposed standards are assessed.

22. **RTCA/DO-178B**. RTCA/DO-178B is compatible with SAE ARP 4754 and 4761 and can be used with MIL-STD-882C. Software levels range from level A, which requires the greatest rigour in the development process, to level E, which levies no assurance requirements on the development. SAE ARP 4754 provides guidance on the allocation of system assurance levels and subsequent allocation of Software Levels. Software Levels are based on the most severe failure condition classification associated with the applicable system-level function. RTCA/DO-248B and FAA Order 8110.49 provides clarification to DO-178B.

23. **DEF STAN 00-55**. DEF STAN 00-55 is used exclusively by the UK MoD and needs to be considered for acquisition of avionics equipment developed in the UK. This standard has been withdrawn through the update of DEF STAN 00-56, but may still be used for the purposes defined in this chapter.

24. **MIL-STD-498**. This standard requires that a strategy be developed for handling safety critical requirements and that safety critical requirements be identified, but provides no indication as to what constitutes an acceptable strategy. While many of the objectives under RTCA/DO-178B have placeholders in MIL-STD-498, there are no criteria that can be used to assess the adequacy of completion of the activity. For example, there is a requirement for unit and integration testing, but there are no criteria that define when testing can be considered complete. Therefore MIL-STD-498, in isolation, does not provide an adequate basis for software assurance and, by itself, is not recognised by DGTA as a software assurance standard.

Software Assurance Products

25. **Planning.** The planning phase conducted prior to the commencement of software development should propose and justify the software level that has been allocated to the software from the software safety program and to define the level of rigour which will be applied to the development. Within the RTCA/DO-178B framework, the Plan for Software Aspects of Certification (PSAC) documents this information for the approval authority. Other software assurance standards may provide equivalent activities for documenting this information for example the DEF STAN 00-55 Software Safety Plan. Alternatively the information may be documented as part of the software safety program plan. DGTA should be involved in assessing the adequacy of the information provided and an agreement reached prior to contract signature. The completed documentation (PSAC or equivalent documentation) should be a contract deliverable, over which the Commonwealth has approval rights. DGTA should be consulted as part of the approval process.

26. Summary of Accomplishments. The purpose of summarising the software accomplishments is to present an argument that the safety-related software requirements have been satisfied and that software assurance has been conducted commensurate with the allocated software level. This will incorporate the argument that software contributes sufficiently to system integrity and adequately mitigates system-level hazards. Within the RTCA/DO-178B framework, the Software Accomplishment Summary (SAS) documents this information for the approval authority. Other software assurance standards may provide equivalent activities for documenting this information, for example the DEF STAN 00-55 Software Safety Case. Alternatively the information may be documented as part of the system safety case. DGTA should be involved in assessing the adequacy of the information provided and an agreement reached prior to design acceptance by the Commonwealth. The completed documentation (SAS or equivalent documentation) should be a contract deliverable over which the Commonwealth has approval rights. DGTA should be consulted as part of the approval process.

27. Software Safety Assessment. The purpose of the software safety assessment is to provide confidence that the software is acceptably safe and of a quality (i.e. sufficiently low defect rate) commensurate with the application. It is an assessment that the software safety argument is well articulated and defensible, that the evidence produced provides suitable support to the argument, and that the evidence supports demonstrated compliance with the contractor-proposed and DGTA-endorsed software assurance standard. The safety assessment forms part of the design acceptance and compliance finding process required by AAP 7001.053(AM1). Further guidance is provided at Annex C to this chapter.

Capability Integrity, Missionised Hazards and Safety Assurance.

Key Issue: Software assurance techniques should be considered for all mission systems containing software regardless of the outcome of the hazard assessment.

28. Aircraft systems used by the ADF have military-specific roles, including specialised wartime functions. Section 2 Chapter 1 of this manual requires aircraft system hazards to be considered not only in benign operating environments but also within worst credible missionised scenarios. For mission critical systems, these missionised hazards, as defined by the hazard assessment, will form the basis of the development assurance requirements at the system level, and thereby the software assurance requirements at the item level. Missionised hazards form part of the functional and system-level hazard assessments and continue to be tracked through the hazard log.

29. RTCA/DO-178B defines the requirements for software assurance and not capability integrity. There may be situations, however, where the Commonwealth requires a higher level of assurance to ensure that the required level of capability is achieved. For example, a back-end mission system may be assessed as having no airworthiness impact and therefore, under RTCA/DO-178B, assigned Level E. Whilst technically correct, software assurance standards generally work to facilitate the production of reliable software of a quality commensurate with the application. The Commonwealth may benefit by applying assurance standards to achieve greater integrity and visibility of those software systems with capability integrity implications; and the contractor may benefit by adopting a standardised process for development. This approach must be assessed carefully against the programs operational requirements to ensure the outcome is cost effective for the Commonwealth.

30. In situations where the Commonwealth identifies a benefit in applying assurance processes to mission systems, the contractor should be tasked with identifying failure of these systems (or system of systems) as one of the following:

a. **Mission critical failure**. Failure conditions would prevent continued conduct of primary mission objectives or place aircrew in situations of undue safety risk.

b. **Mission serious failure**. Failure conditions would reduce the capability of the aircraft or the ability of the crew to cope with adverse mission conditions to the extent that there would be:

(1) a large reduction in mission capabilities, or

(2) higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or

(3) increased risk to aircrew and occupant safety.

c. **Mission important failure**. Failure conditions would not significantly reduce aircraft mission capability or aircrew safety. Failures not considered mission critical or mission serious will fall into this category.

31. Once the mission system failure categorisation has been established, the minimum software level of the mission system (or system of systems) should be assigned. Table 7-4 proposes appropriate software assurance levels, although some higher or lower levels may be justifiable for some mission systems or software technologies. This assignment requires engineering judgement to ensure an effective solution is maintained. In situations where mission systems have missionised hazards that are dealt with separately through the hazard analysis process, the system (or system of systems) should take on the highest of the assurance requirements.

Table 7–4 Mapping of Mission Failure Categorisation to Software Levels

Mission Failure Categorisation	Software Level Assignment
Mission Critical	The objectives of RTCA/DO-178B Level C or equivalent
Mission Serious	The objectives of RTCA/DO-178B Level D or equivalent
Mission Important	No additional assurance objectives required

Capability Maturity vs Software Assurance.

32. Refer to para 15 for an introduction to CMMI. While CMMI does provide valuable of insight into the maturity of an organisation's processes, it does not provide the level of airworthiness assurance that a software assurance standard provides. Therefore, a CMMI accreditation should not be considered an alternative to an appropriately applied software assurance standard.

SOFTWARE QUALITY

33. Software quality is the discipline of ensuring that planned and systematic sets of activities as documented in software development processes are conducted to ensure quality is built into the software products. It consists of the combination of quality assurance, quality control, and quality engineering as related to software. Attributes of software quality are the degree to which a system, component, or process meets specified requirements and the degree to which a system, component, or process meets customer or user needs or expectations. Software quality and software assurance are closely related in some regards, and importantly, both must work supportively within the overall context of the Software Safety Program. Software quality is even an integral process of some software assurance standards, and should be viewed as such regardless of the framework or standard. Since software quality and assurance objectives are so intimately intertwined, this section on Software Quality is included as a supplement to the previous sections on Software Safety and Software Assurance. The intent is not to cover software quality in great detail or completeness here, rather identify areas that have shown, over time, to be attributes of a successful program.

Software Development Capability

Key Issue: For major projects with substantial software development, an assessment of the contractor's software development capability should be part of the tender evaluation process.

34. A mature software development process is an important contributor to the quality of the software product. The level of detail and control required to manage software development makes it very difficult for ADF project teams to force quality into the product. Even a comprehensive Critical Design Review will only cover a fraction of the overall design decisions and difficulties facing the product's development. In all cases, the integrity of the development process and the personnel that apply it will be the key factor.

35. ISO accreditation provides evidence that a framework of regulated and repeatable processes exists. ISO 9000 Part 3 'Guidelines for the application of ISO 9001 to the development, supply and maintenance of software' provides software specific requirements. Like ISO 9000-3, a Capability Maturity Model (CMM) provides a conceptual framework within which specific processes can be optimised to efficiently improve the capability of organisations. An

organisation's software maturity may be appraised against CMMI for systems, software and integrated product and process development. The results of the appraisal may be used to identify organisational strengths and weaknesses early in the life-cycle of the program so that the Commonwealth can better position itself to manage the program effectively. DGTA can assist in assessing the adequacy of the results of the appraisal and in determining appropriate resolutions for identified deficiencies.

Software Life-cycle and Development Standards

Key Issue: Software process standards should be applied to the development of software for airborne and related systems.

36. Software assurance standards are strongly oriented towards ensuring that the software being developed has adequate integrity for its intended role. This means that their scope is often limited to the development phase of the lifecycle and safety aspects of software development. In order for a project to adequately manage a contractor, it is recommended that more detailed software engineering lifecycle requirements be placed on contractors. The two software standards most commonly used in ADF software-intensive acquisitions and support are MIL-STD-498, *Software Development and Documentation* and IEEE/EIA 12207, *Industry Implementation of ISO/IEC 12207:1995 Standard for Information Technology - Software Lifecycle Processes*.

37. **MIL-STD-498**. MIL-STD-498 defines software development lifecycle models and identifies the format and content requirements for software data. For this reason it is an often-used standard for documenting software development. The MIL-STD-498 guidebooks (Overview & Tailoring, and Application & Reference) provide information on applying the standard and should be referred to when tailoring.

38. **IEEE/EIA 12207**. IEEE/EIA 12207 deals with the whole system lifecycle from concept development through to disposal. It provides guidance for all stakeholders in software development, including those organisations performing the roles of acquirer, supplier, developer, operator and maintainer. It is flexible in its application, in that it may be invoked multiple times by different parties in the one project. For example, where a Prime Contractor is acquiring software from a sub-contractor, it is acting in the Acquirer role and should develop processes that comply with the acquisition processes of the standard. This would be the same process requirement that the Commonwealth could apply in managing the Prime Contractor itself. During the in-service support phase, the SPO would act as an Acquirer, using the acquisition processes to contract for software maintenance. The Maintenance Contractor would act as the Supplier, Maintainer, and Developer. It may also use the acquisition processes to acquire support from subcontractors. This holistic view of the software lifecycle means that IEEE/EIA 12207 is helpful to ensure all aspects of software development are considered by both the Contractor's and the Project Office's processes. Because IEEE/EIA 12207 encompasses the entire software lifecycle, its application should be tailored to only include those processes applicable to the project-lifecycle phases included in the contract. The ASDEFCON templates include references to ISO 12207 to standardise this approach.

39. IEEE/EIA 12207's software life cycle data requirements are unlikely to ensure that enough data is produced and delivered to enable software support by a third party. IEEE/EIA 12207.1 Life Cycle Data provides additional guidance, but is not as comprehensive as MIL-STD-498. Therefore, for highly developmental programs or those proposing a third party for in-service support where IEEE/EIA 12207 is used for software engineering processes, the DIDs from MIL-STD-498 should be used to define the Contract Document Requirements List (CDRL). Advice from DGTA should be sought to determine which DIDs may be suitable to include in the CDRL.

Reviews and Audits

40. Software reviews and audits are a fundamental component of a software assurance and software engineering framework. IEEE Std 1028-1997 'Standard for Software Reviews and Audits' provides a good framework for this activity. The standard covers management and technical reviews, software inspections, walk-throughs and audits. Whilst formal reviews are required by software assurance standards and should be attended by the Commonwealth, the Commonwealth is also encouraged to attend internal company reviews, as this has been shown to add significant value to the overall program.

Metrics

41. One way to gain insight into the cost and schedule performance of software development is to quantify and report key measures of the software development process. These measures are referred to as software metrics and can be grouped into six metric categories: requirements, size, effort, capacity, quality and milestones.

42. Metrics provide management insight into how the project is progressing, so that timely remedial action can be initiated if required. The update frequency of software metrics data is dependent upon the duration and complexity of the software development effort, hence complex software being developed under a tight schedule should be monitored more frequently. Metrics are only valid for a limited time, hence automated data collection and analysis is important to ensure the metrics are received by stakeholders within a time frame that enables accurate judgements and decisions to be made.

43. Often metrics programs fail because too much data (or inappropriate data) is acquired, and consequently the Commonwealth and the Contractor are not able to assimilate the meaning of it. Practical Software and System Measurement (PSM) is a recommended approach to determining the metrics requirements for a project. When determining program metrics requirements each stakeholder should first identify the issues that need to be monitored. Stakeholders should then determine what information they need and then investigate which metrics would provide this information. By taking this approach, only data that is going to be used for a specified purpose (ie information used in decision-making) is collected and metrics program costs can be minimised. Issues to be managed by a project rise and fall in their importance over time. Hence, the metrics program should be reviewed frequently, at least each time the project moves to the next phase of the life cycle, for example, from Design to Coding Phases. This will ensure that the metrics program continues to provide useful information.

44. Further information on metrics and their usage in defence acquisition and sustainment can be found by searching the DMO Quality and Environmental Management System (QEMS).

Independent Verification and Validation (IV&V)

45. The principal reason for employing an IV&V agent is to reduce the high costs of correcting latent software errors further along the life-cycle. If the software development is considered to be medium to high technical risk because of complexity or novel design, then IV&V may be warranted. Alternatively, if the software being developed controls safety-critical functions where software errors could cause loss of life or personal injury, then IV&V may be used to compliment and reinforce the software engineering process. The IV&V agency selected should use IEEE Std 1012-1998 to structure their processes.

46. **IEEE STD 1012-1998**. IEEE Std 1012-1998 Software Verification and Validation (V&V) describes processes to determine whether development products of a given activity conform to the requirements of that activity, and whether the software satisfies its intended use and user needs. This determination may include analysis, evaluation, review, inspection, assessment, and testing of software products and processes. V&V processes assess the software in the context of the system, including the operational environment, hardware, interfacing software, operators, and users. The associated guide, IEEE Std 1012a-1998 defines the relationship between the requirement of plans for verification and validation of software for both IEEE Std 1012-1998 and IEEE/EIA 12207.1-1997, so that the user may produce documents that comply with both standards.

47. Independence in V&V does not always refer to organisational independence; it may refer to intellectual independence. While there are obvious advantages for some activities to be organisationally distinct (independence from technical, managerial and financial control), there are some disadvantages in doing this (e.g. timing, access, appropriateness of advice). When tailoring the IV&V effort, intellectual independence within the developer's organisation should also be considered within the overall context of IV&V.

48. Validating complex inter-related activities is more difficult than the individual tasks themselves. For an IV&V agent to be effective, they must be highly skilled domain experts that are capable of detecting errors not usually found by the software developer themselves. IV&V expertise should be a key component when establishing the requirement for IV&V support and should be 'hand-selected' to do the job.

SOFTWARE ACQUISITION

49. Software development is typically an area of high cost, schedule and technical risk, and therefore tenderers are expected to show evidence of their ability to conduct an adequate software development program. This is especially important for projects with complex integrated software, short delivery times or where tenderers do not have a history of relevant software development experience.

50. The majority of new aircraft-related acquisition/modification projects use DMO's ASDEFCON Strategic Material (SM) framework. However, the standard ASDEFCON software DIDs have previously been found lacking for safety-related airborne software. For this reason, applicants using the ASDEFCON templates should replace the SMP

(Tender and Contract) and SWLIST DIDs with those found in Annex A Appendix 1, 2 and 3 respectively. Annex A provides the SOW requirements for airborne software.

51. The Tender-delivered SMP provides insight into the maturity of a Tenderer's software management processes and procedures. Therefore, each SMP must be closely evaluated to determine whether or not a company is capable of conducting the software development effort, and whether they have demonstrated an appreciation of the scope of the project. The Tender SWLIST is also a useful indicator for how much software development is required.

52. It is important that the Commonwealth, in reviewing tendered SMPs, ensures that its own acquisition life cycle model will be compatible with that which is tendered. This may require that the Commonwealth rethink its acquisition strategy to ensure it manages the Contractor appropriately and gains greatest value from the life cycle model that was tendered. For example, when using an evolutionary approach to software development, an acquisition model that includes once-off preliminary and critical design reviews will not be compatible. Instead, progressive design reviews should be conducted as requirements and the design evolves. Similarly, a tender that includes incremental delivery of software capability would require an acquisition model that enables incremental fielding of that capability to gain the most benefit from this model.

53. **Provision of Software Estimates**. Care should be taken in interpreting software estimates, and comparison of development schedules with a software cost estimation tool may be appropriate. These tools will help to highlight optimistic or unrealistic schedules. For a detailed list of appropriate tools, consult Annex G of the DOD 'Guidelines for Successful Acquisition and Management of Software Intensive Systems' or the Software Technology Support Centre - USAF (STSC) 'Report on Project Management and Software Cost Estimation Technologies'. Additional information on software estimates and their usage in Defence are available in the DMO Quality and Environmental Management System (QEMS).

SOFTWARE TRANSITION TO IN-SERVICE SUPPORT

54. Transitioning software from the acquisition program into an in-service support arrangement is a vital yet often under-estimated element of the total program. The technical risk involved differs greatly depending on the support strategy proposed for the project. For instance, the technical risk of establishing and maintaining an in-service support arrangement significantly increases the further removed the arrangement becomes from the OEM organisation. The highest technical risk, at least initially, comes when the link back to the OEM is disestablished. This occurs, in part, when the Commonwealth intends to take on the in-service support role or use a non-associative third party (a third party organisation not contractually associated with the OEM). The following section provides guidance and tailoring advice for consideration when transitioning software into service.

Transition of Standards

Key Issue: Software should transition to an in-service support arrangement with the extant standards that applied during the acquisition phase.

55. Acquisition programs of new or modified software intensive weapon systems should transition to in-service support with the extant standards that applied in the acquisition phase. However, when waivers against approved contracted standards exist, then these waivers must also consider the transition to in-service support. It does not naturally follow that waivers found acceptable during acquisition will be acceptable for in-service support since there may be a reduction in the level of developer knowledge of the system when the system is transitioned from initial development to in-service software support.

56. Where waivers were raised to document and mitigate the deficiencies of the acquired software then, as a separate requirement, a waiver must be sought to cover the transition of those deficiencies to in-service support. The same mitigations may not be appropriate in both situations; DGTA should be contacted to assist in this determination.

Deliverable Requirements

57. The amount of deliverable documentation required for effective follow-on software support, depends on the in-service support strategy proposed. Once the project office understands the in-service strategy required, the deliverable documentation requirements should be tailored as described below:

a. **In-service support by OEM.** If the OEM conducts Life-of-Type (LOT) in-service support using the original development environment or site used during the acquisition phase, then a significant reduction in the delivered documentation can be planned. To support this approach, the

Commonwealth should conduct a review or audit of development documents to ensure they form an adequate basis for in-service support. This activity will normally require full access to the Contractor's development process and is often conducted at the Contractor's site to limit the requirement for the Contractor to deliver documentation to the Commonwealth.

b. **In-service support by the OEM's subcontractor**. If the OEM subcontracts in-service support to another business unit or a separate third party, then the risk to the Commonwealth increases as the original developers, support facilities, and processes may change. If in-service support is never intended to be done by the Commonwealth or a non-associative third party agency, then a significant reduction in delivered documentation can still be planned; however as a minimum, the contract should deliver a plan detailing the software transition, installation and support strategy. Again, to support this approach, the Commonwealth should conduct a review or audit of development documents to ensure they form an adequate basis for in-service support. This activity will normally require full access to the Contractor development process and is often conducted at the Contractor's site.

c. **Commonwealth or non-associative third party**. When the Commonwealth intends to take on the in-service support role or use a third party agency that is not contractually associated with the OEM, then the associated technical risk increases. In this case, transitioning sufficient software documentation is critical to ensuring the in-service organisation has sufficient data from which to support any software modification and maintenance activities. The amount of documentation required will be project specific; however it is likely to be a tailored subset of Annex A Appendix 5. DGTA should be contacted to assist in this tailoring process.

58. Transition Plan. The software component of the transition plan identifies the hardware, software, and other resources required for support of the software product. It presents the developer's plan for the smooth transition from the developer to the support agency or contractor, including the delivery of the necessary tools, analysis, and information required to support the delivered software. From a safety perspective, the developer has the responsibility to identify all software design, code, and test activities that were in the development process that had safety implication. The transition package should include the hazard analyses and the hazard tracking database that documented the software specific requirements and traced them to both the affected module(s) of code and to the hazard or failure mode that derived the requirement.

Intellectual Property Rights

Key Issue: The Commonwealth should obtain the appropriate data rights to ensure the software can be supported throughout the life of the aircraft system.

59. The Commonwealth must ensure the software can be supported throughout the life of the aircraft system. Obtaining the appropriate level of proprietary rights to use and modify the software is essential, whether or not updates to the software are envisaged. This provides insurance against unexpected changes in ADF requirements. Note that delivery of the software and associated documentation does not automatically transfer the right to modify the code; the contract must explicitly state that these rights are to be granted.

60. For COTS, non-developmental items (NDI) and modified COTS software the Commonwealth is unlikely to be entitled to proprietary rights for delivered products. This must be confirmed up-front and the impact assessed along with other associated project risks. Particular care should be given to NDI's that are not widely used in fielded products, and those with ongoing licensing agreements.

61. The issue of data rights is far more complex than outlined in this chapter, and it is recommended that a contracting specialist be consulted to determine the specification of further requirements.

IN-SERVICE SOFTWARE MODIFICATIONS

Introduction

62. The underlying philosophy for ADF airworthiness is that the acquired aircraft should continue to maintain an equivalent level of safety throughout its LOT or where necessary, reflect improvements in safety as determined by DGTA to be appropriate. In the case of software, this means that the software safety program and software assurance standard that are applied during acquisition should continue to be applied for in-service modifications, and supplemented over time to ensure current guidelines are met.

63. Some legacy aircraft have been acquired where no software assurance standard has been explicitly applied; instead, software development standards such as DOD-STD-2167A or MIL-STD-498 are relied on to provide adequate assurance of the software product. As has been described previously within this chapter, development standards like MIL-STD-498, in isolation, do not provide an adequate basis for ensuring software assurance. Inevitably, these standards must be supplemented to provide an equivalent level of confidence in the product that assurance standards such as RTCA/DO-178B can provide. DGTA's preferred option would be to retrospectively apply a software assurance standard, such as RTCA/DO-178B. However this must be assessed within the context of the legacy system to ensure the application is value adding and does not become cost prohibitive.

64. Software assurance standards need to be applied in conjunction with an applicable system safety standard. The assumption in this section is that the legacy system has a system safety program in place, and that program is likely to map to the requirements of MIL-STD-882C or similar. If this is not the case, then guidance on In-Service System Safety Program requirements given in Section 2 Chapter 1 of this manual should be sought in addition to the information presented here.

Migrating to a Software Assurance Standard

65. The objective in applying a software assurance standard to in-service software support is to improve safety assurance of the software through the application of a systematic approach to identifying and addressing the causes of software failure. DGTA's preferred option would be to retrospectively apply a software assurance standard, such as RTCA/DO-178B. However, while full application of any software assurance standard to legacy software support may be beyond the resources available in-service, application of a tailored subset has been shown to improve safety assurance significantly. In particular, tailoring should focus on the specification, derivation and traceability of software requirements with appropriate fidelity and formality; and verification against requirements, including consideration for normal and robustness test cases and test coverage of requirements and software structure.

66. The FAA provides guidelines in Notice 8110.49 Chapter 10 on the application of RTCA/DO-178B to legacy systems. The guidelines are intended for application to systems developed to RTCA/DO-178 and 178A; however a similar approach can be applied to legacy military systems where DGTA has determined the original development processes to be sufficiently robust. If the original development processes were not sufficiently robust, then additional software assurance activities, analysis and testing may be required to further establish the software integrity.

67. In addition to the guidelines provided in FAA Notice 8110.49 and supplemental direction provided by DGTA, the following guidelines apply when considering the application of RTCA/DO-178B to legacy systems:

a. Legacy software may be considered to meet the objectives of RTCA/DO-178B provided the most recent change meets the objectives of RTCA/DO-178B, and the original processes were sufficiently robust. There is no requirement to show that the original processes that were used to develop the legacy software were equivalent to RTCA/DO-178B. However, a service history argument should be developed that addresses the criteria in Section 12.3.5 of RTCA/DO-178B to establish that the previous processes were sufficiently robust.

b. The tools (both verification and validation) which were used in the development of the legacy software are not required to be RTCA/DO-178B qualified, provided a valid service history argument can be made. Although tool qualification is not required, the contribution of the tools to satisfy RTCA/DO-178B objectives and the existence of tool faults must be adequately identified and tracked.

68. There will be occasions where changes to the functionality of a CSCI result in an associated increase in the software level required by that CSCI, as determined by the system safety program. When this occurs, several factors should be considered in determining the appropriate approach to adopt; including the size and complexity of change, the required change in software levels, service history and LOT remaining for the system. Whilst early consultation with DGTA is recommended on this issue, in general two approaches are possible:

a. application of the processes of the new software level to the entire CSCI; or

b. application of the processes of the new software level to the affected area and those areas determined to be associated through data and control coupling (i.e. those sub-components of the software that are not sufficiently partitioned from the sub-components being modified).

Software Assurance Task Matrix

Key Issue: For in-service software modifications where a software assurance standard is not explicitly applied, a Software Assurance Task Matrix should be defined.

69. An alternative approach to migrating to a software assurance standard is to define a Software Assurance Task Matrix. A Software Assurance Task Matrix (refer Table 7-5) can be developed which defines the level of effort and rigour applied to each design phase commensurate with the safety impact of the system and its related functionality. For programs (or SPOs) that do not specifically apply a software assurance standard, RTCA/DO-178B provides a good benchmark for tailoring the Software Assurance Task Matrix to the specific application.

Table 7–5 Example Software Assurance Task Matrix

Phase / SRI	Design	Code	Unit Test	Integrating Unit Test	System Integration
1 High Risk	– Architecture verified with independence	– Data and control flow verified with independence	– MCDC Coverage	– 100% Regression Testing	– 100% Regression Testing
2 Serious Risk	– Req & algorithms verified with independence	– Traceable to low level req. – Code verified with independence – Safe subset identified	– Independent test case review – Decision Coverage	– Independent test case review	– Independent test review – Test coverage of low level requirements
3-4 Moderate Risk	– Architecture reviewed – Partitioning integrity confirmed – High level req. traceable to system req. – Derived req. indicated to SS process	– Complies with low level req. and architecture – Code walkthrough – Derived req. indicated to SS process	– Formal unit testing – Statement Coverage – Normal range and Robustness Testing – Derived req. indicated to SS process	– Derived req. indicated to SS process	– Integrated in target computer – Test coverage of high level requirements – Derived req. indicated to SS process
5 Low Risk	– Normal Software Design IAW Software Development Plan	– Normal Software Code IAW Software Development Plan	– Normal Software Unit Test Activity IAW Software Development Plan	– Normal Software Unit Integration Test Activity IAW Software Development Plan	– Normal Software System Integration Test Activity IAW Software Development Plan

70. The purpose of the Software Assurance Task Matrix is to allow a flexible approach to applying rigour in the software process commensurate with software criticality. For example, for low risk items, normal software development processes would be acceptable. As the safety impact increases then a proportionate amount of additional rigour is placed on the normal development processes to gain an increased level of assurance. This approach makes no assumptions on the current architecture of the systems being modified. For some systems, it may be that the partitioning of safety-critical systems makes the application of a flexible approach seemingly limited. That is, the lower order functions being modified take on the criticality of the worst credible severity of the higher level function. This cannot be avoided and is a limitation of the legacy architecture; however, the requirement to do so is driven from the safety assessment and not from the limitation of the software processes. DGTA can provide advice on how best to tailor this approach to the current legacy platform.

SOFTWARE DESIGN ACCEPTANCE

Commonwealth Oversight

Key Issue: Direct Commonwealth oversight is required for all software changes to safety critical systems regardless of whether the change is considered simple or complex.

71. Because of the nature of software, an aircraft modification which is assessed as having a Minor airworthiness impact but which involves a modification to safety related software, may still have the potential to have catastrophic consequences. This is because it is difficult to ensure that modification of one area of code does not adversely impact another area and have unintended consequences. Therefore, for safety critical systems containing software, the Commonwealth is required to provide direct oversight to the development of these systems. This includes exercising all elements of the design acceptance process, not merely organisational competency.

Software Compliance Findings

Key Issue: A Compliance Finding should be made against the software assurance standard which is defined directly or indirectly in the Certification Basis, or for in-service support in the approved Engineering Management System.

72. For acquisitions and modifications, a compliance finding leading to design acceptance is required to be made against the software assurance standard which is either called out directly or indirectly in the Certification Basis. For in-service support, a compliance finding is required to be made against the software assurance standard or objectives defined in the approved Engineering Management System. This assessment involves the review of objective evidence that all relevant requirements of the software assurance standard have been met. The assessment requires an understanding of software development techniques and the ability to assess whether the developer's process complies with those techniques. For high integrity software it requires individuals with appropriate experience and domain knowledge to perform the compliance finding. As this may not always be possible, an independent third party may be contracted to assist with the compliance finding. DGTA should be engaged to assist in defining the compliance finding activities or, in exceptional circumstances, act as the compliance finding agency. The preferred method for undertaking compliance findings is through in-process reviews rather than through formal milestone reviews. However, this does not negate the need to have formal milestones in the development program. Further information on compliance finding and design acceptance for software can be found at Annex C to this chapter.

ADDITIONAL GUIDANCE

Language Selection

Key Issue: The selection of the programming language should be justified where software is being developed specifically for, or at the request of, the ADF.

73. The programming language is central to the role of translating the intended design into executable code to run on the target system. Thus, the chosen programming language for a given application should seek to minimise the likelihood that language related errors are introduced into the implementation commensurate with the safety risk. The following factors should be considered as part of the language justification.

a. The language definition should be documented in a recognised standard, and compiler implementations should comply with the standard. Unique solutions can result if compiler implementations do not comply with the standard language definition.

b. The language definition should generally be independent of any particular hardware or operating system. Portability can be compromised if a language is not independent of a particular system. This is likely to limit the hardware and software options both for development of the original system and for future upgrades.

c. A language subset and suitable enforcement tools should be considered for all software that is safety related. All languages have features that, if not controlled properly, can lead to problems. For example: programmers may be prone to making errors when using the features; compilers may be prone to poor, inconsistent or incorrect implementation of the features; programs written using the features may be more difficult to analyse, test or prove; and the features may introduce implementation dependencies, reducing portability.

d. The language should support the principles of software-engineering, discouraging or prohibiting poor practices, and promoting and supporting maintenance activities.

e. The language should effectively support the application domain(s) of interest. Poor support for the application domain may make the development of a clear solution difficult. This can also have an impact on the performance characteristics of the code.

f. The language should support the required level of system integrity.

g. Appropriate software engineering based support tools and development environments should be available. Developer productivity and system quality can be compromised if there is a lack of appropriate tool support. In addition, the cost of the tools should not be disproportionably greater than the tools' contribution to developer productivity; and system quality, reliability and safety.

h. Sufficient expertise should be available for the chosen language within the development team, or in industry from which to recruit from, or consult with. Further consideration should be given as to how expertise in the chosen language will be maintained over the life of the software system. However, the availability of programmers or programmers' preferences towards 'popular' languages shall not be used as justification to dismiss the other criteria listed in this section. The development of software for safety critical or safety related applications, including airborne software, embodies principles that are not widely adopted in the broader commercial information technology industry, and thus 'popularity' alone is not a sound basis for selection of a language.

i. Where possible, a new development on an existing platform should seek to rationalise the number of software languages, tools and associated support mechanisms that are required in the software-engineering environment. In reality, however, often the ADF is a customer of existing systems and cannot afford to specify a single language for a platform.

74. IEC61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures (Annex C - Table C.1) provides recommendations on the suitability of specific programming languages based on criteria similar to that listed here. Programs are advised to seek DGTA advice on the suitability of the proposed language or language subset, in particular if the language does not address the criteria listed here.

Firmware

75. Firmware is usually defined as a combination of a hardware device, computer instructions and data, that reside as read-only software on that device. The term is sometimes used to refer only to the hardware device or only to the computer instructions and data and thus may include binary source code, Programmable Logic Devices (PLDs), Application Specific Integrated Circuits (ASICs), or Field Programmable Gate Arrays (FPGAs). This chapter will not attempt to define firmware formally here. Rather, it assumes that during system definition, functions have been allocated to either hardware or software. For functions allocated to software, the guidance in this chapter applies. For functions allocated to hardware, the design assurance principles of RTCA/DO-254 or equivalent may be appropriate. Programs are advised to seek DGTA advice on the application of RTCA/DO-254.

Operating Systems

76. The integration of previously federated functions into software hosted on common computing resources has prompted traditional embedded software architecture approaches incorporating often proprietary cyclic or multitasking executives to move to using Commercial Off the Shelf (COTS) Real-Time Operating Systems (RTOS). These COTS RTOS handle the interface between application software (scheduling, resource allocation, task communication, etc) and essential hardware services (device drivers, interrupts, memory management, etc). A number of RTOS are protected domain (partitioned), which provides isolation between functionally independent software components to contain and/or isolate faults. RTOS that are compliant with ARINC 653 are generally able to support partitioning of applications. Protected Domain RTOS is core to the Integrated Modular Avionics (IMA) approach now being incorporated in modern military aircraft (F-22 and JSF) and civilian aircraft (A380 and Boeing 787).

77. Where possible all new software development that involves hosting multiple functionally independent software components on a single computing resource should use a Protected Domain RTOS to provide partitioning. Partitioning also provides scope for reducing the software assurance requirements on less critical software components, as failures within these components can be contained by the RTOS. Furthermore, several COTS Protected Domain RTOS have been 'certified' to various levels of RTCA/DO-178B. The use of 'certified' Protected Domain RTOS and the associated data can reduce program risk while achieving safety goals in a cost-effective manner.

Emulation

78. Emulation of legacy micro-processors can enable reuse of legacy software (binaries) with minimal changes on modern COTS micro-processors. Achieving high integrity in emulated systems can be challenging, particularly for safety critical systems, however emulation may prove useful for mission and safety–related systems. A number of approaches have been evaluated by DGTA including:

a. dynamic translation of legacy binaries, which is most suitable for older processors (generally more than 15 years old) due to the processing overhead;

b. static translation of code for execution on modern processors (generally less than 15 years old); and

c. hybrid approaches using both static and dynamic translation to overcome architectural issues such as complex instruction sets and coupling with the runtime environment or operating system.

DGTA's proposed approach for ADF acceptance of emulation technologies involving dynamic translation is covered in a discussion paper located on the DGTA intranet website under DAIRENG/SCI1. Early engagement with DGTA is strongly encouraged for all proposed emulation solutions.

Software Assurance and Concept Technology Demonstration

79. Concept Technology Demonstration (CTD) is one means by which research establishments such as DSTO mitigate the risks associated with determining if a particular technology is feasible to solve a given class of problems. The limited timeframe and funding associated with these programs mean that it is rarely possible to apply assurance activities commensurate with its safety or mission impact. This is particularly the case for software development. CTD software (source code) is unlikely to be suitable for direct migration into a full-scale development. It is not possible to simply conduct additional testing in an attempt to achieve the same confidence as software developed under an appropriate assurance process. The CTD should be used to capture the positive design outcomes, and then these design outcomes applied to a full scale development with appropriately defined safety and assurance activities.

EFB/MPS

80. The ADF and civil aviation communities are seeing a wide array of systems entering service that automate mission planning and make available a large amount of information with the intent to move towards a "paperless-cockpit". Such applications include (but are not limited to) maps, intelligence, weather, weapons data, takeoff/landing performance data and weight and balance calculations. Operators benefit from the fusion and automation that these applications offer. These systems may be generically grouped into Electronic Flight Bags (EFB) and Mission Planning Systems (MPS).

81. DGTA's proposed approach for ADF acceptance of these systems is covered in a discussion paper located on the DGTA intranet website under DAIRENG/SCI1. The discussion paper predominantly covers the technical issues involved in the acceptance of these systems into service, however, it also highlights some operational considerations.

Annexes:

A. Statement of Work Requirements for Airborne Software

- Appendix 1 Software Management Plan (Tender)
- Appendix 2 Software Management Plan (Contract)
- Appendix 3 Software List
- Appendix 4 Software Support Plan
- Appendix 5 Contract Deliverable Requirements List

B. Sample CBD Entries for Software

C. Software Compliance Findings

- Appendix 1 Compliance Finding Plan Template

STATEMENT OF WORK REQUIREMENTS FOR AIRBORNE SOFTWARE

Software Safety

1. The Contractor shall establish, implement and conduct a Software Safety Program (SwSP) for [Project Name] in accordance with the approved SwSP Plan. The SwSP shall consider potential hazards in the specification and/or derivation of requirements, design, integration, operation, maintenance and disposal of software for [Project Name] and coordinate hazard identification and mitigation efforts for hazards with software-related causal factors.

2. The SwSP plan shall meet the requirements of:

a. IEEE 1228 'IEEE Standard for Software Safety Plans';

b. Parent Contract and Commonwealth-level System Safety Program Plans.

NOTE TO TENDERERS

IEEE STD 1228-1994, 'Standard For Software Safety Plans', provides an industry standard for the preparation and contents of a Software Safety Program Plan (SwSPP). Specific tasks, processes, and activities detailed in this standard can be integrated into the System Safety Program Plan (SSPP) or documented separately in the SwSPP. The software safety schedule of events should correspond with the software (and hardware) development life cycle, and be in concert with each development and test plan published by other technical disciplines associated with the program.

Guidance on the development and implementation of an effective Software System Safety process can be sourced from the Joint Software System Safety Committee's Software System Safety Handbook.

NOTE TO DRAFTER

Synergy between the Software Safety requirements and the System Safety requirements is required.

Software Assurance

3. The Contractor shall meet the objectives of a software safety assurance standard for the development of all software that is safety related.

NOTE TO TENDERERS

Safety related software can be considered as all software whose anomalous behaviour, as shown by the system safety assessment process, would cause or contribute to a failure condition for the aircraft that affects the aircraft operational safety or pilot workload.

4. The software safety assurance standard shall meet the requirements of:

a. RTCA/DO-178B, or

b. DEF STAN 00-55, or

c. A suitable alternative standard where the alternative standard proposed can be shown to provide an equivalent level of software assurance to RTCA/DO-178B.

NOTE TO TENDERERS

MIL-STD-498 is not considered to provide an equivalent level of assurance to RTCA/DO-178B. Alternative standards or processes shall be detailed in the draft SMP delivered under the contract and should include an argument on the equivalence to RTCA/DO-178B.

5. The Contractor shall prepare the following deliverables as part of the SwSP and deliver them in accordance with the document delivery schedule shown in the approved SwSPP:

a. *Planning* CDRL xxx which meets either the requirements of RTCA/DO-178B, Plan for Software Aspects of Certification, or the DEF STAN 00-55 Software Safety Plan;

b. *Summary of Accomplishments* CDRL xxx which meets either the requirements of the RTCA/DO-178B Software Accomplishment Summary, or DEF STAN 00-55 Safety Case;

6. The Contractor shall include an assessment of missionised hazards as an integral part of the safety analysis, as they relate to software assurance.

NOTE TO TENDERERS

Missionised hazards are aircraft system hazards considered within the worst credible missionised scenarios. As most analysis of this type can only be qualitative, operational requirements and basic mission assumptions must be provided as input to the System Safety Working Groups (SSWGs).

7. The Contractor shall apply software safety assurance objectives to Mission Systems as defined in AAP 7001.054 Section 2 Chapter 7 para 27-29.

Software General

NOTE TO DRAFTERS

The software engineering aspects of this SOW have been aligned with ISO/IEEE 12207, which covers all software life cycle phases. In the case where a Contractor is not involved in software development, the Contractor is still expected to satisfy this SOW for the acquisition and supply life cycle phases of ISO/IEEE 12207 as a minimum. As such, the SMP is to capture the Contractor's tailoring of ISO/IEEE 12207 and integrate applicable software safety standards including data deliverable's, as applicable for the Contract and the Contractor's internal procedures

A tender SMP is also included and should be called as part of the conditions of tender.

8. The Contractor shall develop, deliver and update a Software Management Plan (SMP) in accordance with CDRLxxx – (Appendix 2 to Annex A).

9. The Contractor shall plan and conduct its software engineering activities in accordance with the requirements of ISO/IEEE 12207, as tailored by the approved Software Management Plan.

10. The Contractor shall require each approved Subcontractor to plan and conduct software engineering activities in accordance with the requirements of ISO/IEEE 12207, as tailored by the Subcontractor in its plans for conducting software engineering activities.

11. The contractor shall approve Subcontractor tailoring of ISO/IEEE 12207, ensuring it is consistent and compatible with the Contractor's SMP and the Contract.

12. The Contractor shall develop, deliver and update a list of all software used in the aircraft and Support System in accordance with CDRL - (Appendix 3 to Annex A).

Software in-service support

NOTE TO DRAFTER

The amount of deliverable documentation required for transitioning software into an in-service support arrangement, and to ensure effective follow-on software support, is dependent on the in-service support strategy proposed. For instance, the risk of establishing and maintaining an in-service support arrangement significantly increases the further removed the arrangement becomes from the OEM organisation. The Commonwealth must tailor the deliverable documentation requirements based on the in-service support

strategy proposed. As a minimum, the Commonwealth should select one of the following options to tailor for the specific project requirements:

[Option 1 – OEM Support]

13. The Contractor shall prepare the following CDRLs as part of the software support program and deliver them in accordance with the document delivery schedule shown in the approved SMP:

a. Software Transition Plan (STrP) in accordance with MIL-STD-498 Data Item Description DI-IPSC-81429;

b. Software Support Plan (SSP), in accordance with CDRL – (Appendix 4 to Annex A).

NOTE TO TENDERERS

A single document deliverable may be proposed provided the document contains all of the requirements specified in DI-IPSC-81429 and CDRL – (Appendix 4 to Annex A).

The Software Management Plan may be used initially for this purpose during the contract negotiation phase, after which a separate deliverable should be developed for the express purpose of managing the transition to in-service support.

[Option 2 – Third Party Support]

14. The Contractor shall prepare the following MIL-STD-498 CDRLs as part of the software support strategy and deliver them in accordance with the document delivery schedule shown in the approved SMP:

a. Software Installation Plan (SIP) DI-IPSC-81428;

b. Software Transition Plan (STrP) DI-IPSC-81429;

c. Operational Concept Document (OCD) DI-IPSC-81430;

d. System/Sub-systems Specification (SSS) DI-IPSC-81431;

e. System/Sub-system Design Description (SSDD) DI-IPSC- 81432;

f. Software Requirement Specification (SRS) DI-IPSC-81433;

g. Interface Requirements Specification (IRS) DI-IPSC 81434;

h. Software Design Description (SDD) DI-IPSC-81435;

i. Interface Design Description (IDD) DI-IPSC-81436;

j. Database Design Description (DBDD) DI-IPSC-81437;

k. Software Test Description (STD) DI-IPSC-81439;

l. Software Test Report (STR) DI-IPSC-81440;

m. Software Product Specification (SPS) DI-IPSC-81441;

n. Software Version Description (SVD) DI-IPSC-81442;

o. Software Users Manual (SUM) DI-IPSC-81443;

p. Software Input/Output Manual (SIOM) DI-IPSC-81445;

q. Computer Operation Manual (COM) DI-IPSC-81446;

r. Computer Programmers Manual (CPM) DI-IPSC-81447;

s. Firmware Support Manual (FSM) DI-IPSC-81448;

t. COTS manuals as acceptable *alternatives to COM, CPM and SUM.*

NOTE TO DRAFTER

The amount of documentation required will be project specific and should be tailored accordingly. Under a DO-178B program, deliverables can be combined where there is overlap. For example a Software Test Description and the DO-178B Software Verification Plan.

15. The Contractor shall deliver all aircraft software encapsulated in a CASE tool.

16. The CASE tool shall provide the capability to store and manipulate specification, design data and source code, while maintaining configuration control.

17. The Contractor shall demonstrate that the source code for all delivered CSCIs compiles and links using the delivered software support environment, as outlined in the Software Product Specification (SPS) or equivalent document. The generated machine code must be validated against the delivered software product.

18. The Contractor is to provide intellectual property rights to the Commonwealth, for all software developed under the Contract.

NOTE TO DRAFTER

The issue of data rights is a complex issue, and it is recommended that a contracting specialist be consulted to determine the specification of further requirements. It is important to note, however, that data rights is not the real issue and that, from a software acquisition perspective, the primary concern is maintaining the capability to support the software during its life cycle at reasonable cost.

19. The Commonwealth is to be granted the rights to use and modify all non-developmental and modified COTS software. These rights are to be transferable to a third party, approved by the Commonwealth, to support or modify the software.

20. The Contractor shall transfer to the Commonwealth all intellectual property rights for the support environment.

NOTE TO TENDERERS

Tender responses are to detail the intellectual property rights applicable to all delivered COTS and modified COTS software. This requirement applies to tools and other applications that are required for software support.

The ability to obtain rights to modify software items associated with the primary product or its support, will be essential in assessing support costs and risks inherent in any tender response.

Table 7–A–1 SOW Document Delivery Schedule

CDRL	QTY	Delivery	Frequency	Review Period	Commonwealth Review Rights
SwSPP	2	RFT, ED+30	Annual, and as required	30	Approve
Planning: DO-178B PSAC or DEF STAN 00-55 Software Safety Plan	2	RFT, After completion of software planning process	Once or as required	30	Approve
SMP	2	RFT, ED+30	Annual, and as required	30	Review
Summary of Accomplishments: DO-178B Software Accomplishment Summary or DEF STAN 00-55 Software Safety Case	2	FTRR-60	Once	30	Approve

Appendices:

Appendix 1 Software Management Plan (Tender)

Appendix 2 Software Management Plan (Contract)

Appendix 3 Software List

Appendix 4 Software Support Plan

Appendix 5 Contract Deliverable Requirements List

Blank Page

DATA ITEM DESCRIPTION

1. DID NAME: DID-ENG-SW-SMP-V1.2

2. TITLE: SOFTWARE MANAGEMENT PLAN (TENDER)

3. DESCRIPTION AND INTENDED USE

The Tender Software Management Plan (TSMP) shall describe relevant sections of the Tenderer's plans for developing software. This requires a subset of the information usually provided in a normal MIL–STD–498 SDP and is aimed at allowing effective evaluation of tendered proposals. The information provided shall be included in the final Project SMP and may be presented as a draft of the final SMP. Alternatively, Tenderers may respond directly to the specific content requirements of this TSMP. The term "software development" is meant to include new development, modification, reuse, re-engineering, maintenance, and all other activities resulting in software products.

These plans are intended to describe the relevant life cycle processes as described in AS/NZS ISO/IEC 12207: Software Life Cycle Processes as the Contractor intends to apply them to the activities of the Contract.

The Contractor will use the Software Management Plan to document the approach, plans and procedures for managing software activities and will use the SMP to monitor progress of software activities.

For Contractors acquiring and/or supplying software under the Contract, this plan is expected to describe the approach, plans and procedures to be applied to the management of the software being acquired and/or supplied. This would typically include the monitoring and review of Subcontractors developing software, the configuration management of acquired software and the integration and Verification of this software with other elements being supplied under the Contract.

For Contractors developing software, this plan is expected to include the approach, plans and procedures for software development in addition to those applied to the acquisition and/or supply. The contractor is encouraged to ensure the cost-effective application of the recognised development standards. Contractors may propose any specific tailoring of standards. The benefits of any changes should be highlighted where possible. Documents are to be supplied in the contractor's preferred format, particularly where data is already available.

The Commonwealth will use the Software Management Plan to gain an accurate insight into the approach, plans and procedures being employed by the Contractor in the execution of software related activities.

The SMP is to avoid replicating any detail of activities that are addressed directly by company procedures, simply stating the applicable instruction is acceptable. Any such detail should only be included to establish how company procedures are to be applied to the software development activity. However, the Commonwealth may request access to any procedural document to confirm that the supporting documents meet content requirements.

4. INTER-RELATIONSHIPS

The Tender Software Management Plan is a draft subset of the Software Management Plan.

5. APPLICABLE DOCUMENTS

The following document form a part of this DID to the extent specified herein.

DI-IPSC-81427A Software Development Plan Data Item Description

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

This data item shall comply with the general format, content and preparation instructions contained in the TDRL Description and Response Procedures.

6.2 Specific Content

6.2.1 General

6.2.2 The Tenderer Software Management Plan (TSMP) shall comply with the following requirements and the requirements of DI-IPSC-81427A as tailored by Table 1. For the tendering stage, the TSMP is not meant to be complete. However, a detailed outline should be provided with detailed references to standards. The TSMP should then be used as a draft for later acquisition phases.

Note to drafters:

Table 2 of Annex G to Attachment A of the Conditions of Tender provides a list of minimum requirements for the SMP for use when the Commonwealth intends to shortlist to 2 or more tenderers. These items are the most useful and relevant; SCI recommends that these criteria are sufficient for tender evaluation.

6.2.3 The TSMP shall contain a brief description of what previous projects have been completed using the proposed software development method.

6.2.4 The TSMP shall contain a list of accreditations (ISO 9000, CMMI or other) including when they were achieved, the scope of coverage and current status.

6.2.5 The TSMP shall contain a complete list of any existing company procedures and standards to be applied to the development activity. The issue date and current amendment status of these documents shall be included.

6.2.6 The TSMP shall describe the scope of sub-contractor activities; a summary TSMP should be produced for these sub-contractors if significant development is anticipated, or if safety critical and/or complex changes are required.

Table 7–A1–1. Tailoring to be applied to DI-IPSC-81427A

Affected Paragraph	Tailoring to be Applied
All	Replace all occurrences of “software development plan” with software management plan”.
All	Replace all occurrences of “SDP” with “SMP”.
All	Delete all occurrences of “It shall cover all contractual clauses concerning this topic.”
4.1 Software development process	Replace with: The proposed standards under which the software development activity shall be conducted is to be stated, for example, MIL–STD–498, RTCA/DO–178B, IEEE 12207.0. The actual scope of application shall be detailed for each CSCI including sub-contracted items. This section shall clearly outline the proposed development life cycle, detailing the use and the functional content of incremental builds. Schedule date and objectives for each activity shall be specified in latter sections. Note to Contractor: Contractors are encouraged to identify a build strategy that mitigates project risks and allows early access and usage of system components where applicable.
4.2.3.1 Incorporating reusable software products	Add: Implications for supporting the software shall be specifically addressed for each item affected and include an assessment of vendor viability, level of support available, alternate sources of support, ownership of intellectual property rights, licensing arrangements (including costs and restrictions), dependencies such as operating system and/or hardware compatibility and constraints.
4.2.4.1 Safety Assurance	Add: It shall describe the integration of software safety as part of the system safety program. It shall include the tailoring and use of selected software safety standards and guidelines and associated data deliverables.
4.2.4.4 Assurance of other critical requirements	Add: It shall describe any mission critical software and the steps either taken or planned to ensure failure of this software will not compromise the system’s mission. It shall describe the application of assurance standards to missionised hazards and for capability integrity (see AAP 7001.054 S2Ch7).
4.2.7 Access for acquirer review	Replace with: This paragraph shall describe the approach to be followed for providing the Commonwealth and its authorised representatives access to Contractor and Subcontractor facilities for review of work products, activities and data including engineering and measurement data. Access should include at least physical access to facilities and preferably include electronic access to data (eg measurement data) and work products (eg design information).

Affected Paragraph	Tailoring to be Applied
5.2.1 Software Engineering Environment	Add: This paragraph shall identify the application of development tools to support each phase of the development cycle. For example, the usage of CASE tools for design, configuration management, test case generation, requirements management, computing resources (number, type, configuration, etc.), the associated performance requirements of the environment (eg required compile and link times), and other activities should be listed. For safety critical software, this paragraph shall address the airworthiness certification implications of the software engineering environment (ie tool qualification). Where a software support environment is to be provided, the scope of changes possible to the CSCIs using the support environment is to be detailed. This assessment should include consideration of provided design data. Note that demonstration of successful CSCI compilation from source code, using the support environment, shall be included in the project plan.
5.2.5 Non-deliverable software	Add: It shall identify any non-deliverable software and describe how this software will be treated differently from deliverable software. It shall address specifically the application and tailoring of the standards identified for software development to non-deliverable software. For safety critical software, this paragraph shall address the certification implications and use of non-deliverable software.
5.4.1 System-wide design decisions	Replace with: This paragraph shall include details of how system design decisions affecting or affected by software are to be made and recorded. It should address how such decisions and the rationale for making them will be preserved and applied during through life support of the system.
5.5 Software requirements analysis	Add: It shall describe how software requirements will be identified and allocated to software components, how software requirements will be reviewed to ensure a common understanding with relevant stakeholders and how software requirements will be managed and controlled.
5.6.1 CSCI-wide design decisions	Add: It shall detail the criteria used to define and select CSCIs including the rationale for each of the selection criteria. It shall include design decisions regarding the partitioning of the software and the consideration given to enhancement and modification during through life support of the software.
5.19.1 Risk management	Add: This paragraph shall detail the techniques used for identifying software related risks and mitigation strategies. It shall include details of any software risks identified and the selected mitigation strategy to be adopted where these are not detailed in the Contractor’s Risk Management Plan and Risk Register.

Affected Paragraph	Tailoring to be Applied
5.19.2 Software management indicators	Add: This paragraph shall detail the use of measurement as a management tool. It should identify how the Contractor intends using measurement to mange the development and acquisition of software for the project. Where this information is available to the Project Authority elsewhere this section should reference the relevant information and provide a summary of the measures used for software management.
5.19.4 Subcontractor management	Add: This paragraph shall detail the Contractor's plans for managing the software engineering activities performed by Subcontractors. It shall identify and describe the scope of the software activities to be undertaken by the Contractor and each of its Subcontractors performing software engineering activities. It shall describe the Contractor's plans for review and approval of Subcontractor plan and processes. It shall describe the Contractor's plans for monitoring the progress of Subcontractor activities and how significant deviations from Subcontractor plans will be identified and addressed.
5.19.6 Coordination with associate developers	Add: This paragraph shall describe the plans for coordination of software engineering efforts with associated developers. Such coordination may include interface definition and control, the use of integrated product teams, as well as the support to be provided during integration and verification activities.
6. Schedules and activity network	Add: This paragraph shall present and describe the proposed software schedule and include a clear mapping of the life cycle development phases and major milestones. This paragraph shall include the rationale for the durations given in the schedule and include the basis of estimate, estimating assumptions and the selection of coordination points and linkage with the Contract Master Schedule.

Blank Page

DATA ITEM DESCRIPTION

1. DID NAME: DID-ENG-SW-SMP-V1.2

2. TITLE: SOFTWARE MANAGEMENT PLAN (CONTRACT)

3. DESCRIPTION AND INTENDED USE

This deliverable is intended to document the Contractor's plans for the management and development of software. These plans are intended to describe the relevant life cycle processes as described in AS/NZS ISO/IEC 12207: Software Life Cycle Processes as the Contractor intends to apply them to the activities of the Contract.

The Contractor will use the Software Management Plan to document the approach, plans and procedures for managing software activities and will use the SMP to monitor progress of software activities.

For Contractors acquiring and/or supplying software under the Contract, this plan is expected to describe the approach, plans and procedures to be applied to the management of the software being acquired and/or supplied. This would typically include the monitoring and review of Subcontractors developing software, the configuration management of acquired software and the integration and Verification of this software with other elements being supplied under the Contract.

For Contractors developing software, this plan is expected to include the approach, plans and procedures for software development in addition to those applied to the acquisition and/or supply. The contractor is encouraged to ensure the cost-effective application of the recognised development standards. Contractors may propose any specific tailoring of standards. The benefits of any changes should be highlighted where possible. Documents are to be supplied in the contractor's preferred format, particularly where data is already available.

The Commonwealth will use the Software Management Plan to gain an accurate insight into the approach, plans and procedures being employed by the Contractor in the execution of software related activities.

4. INTER-RELATIONSHIPS

The Software Management Plan is a subsidiary document to the Systems Engineering Management Plan where such a plan exists.

5. APLICABLE DOCUMENTS

The following document form a part of this DID to the extent specified herein.

DI-IPSC-81427A	Software Development Plan Data Item Description

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled "General Requirements for Data Items".

6.2 Specific Content

6.2.1 General

The Software Management Plan (SMP) shall comply with the content requirements of DI-IPSC-81427A with the exceptions contained in Table 1 below.

The SMP shall clearly demonstrate the following key aspects of the proposed software development activity:

a. the scope of the development activity to be undertaken,

b. the maturity and capability of the contractor's development process,

c. the application of development tools and techniques to ensure minimisation of software ownership costs, and

d. support proposals for all planned CSCIs (if not addressed directly by the Support Plan).

Table 7–A2–1 Tailoring to be Applied to DI-IPSC-81427A

Affected Paragraph	Tailoring to be Applied
All	Replace all occurrences of “software development plan” with software management plan”.
All	Replace all occurrences of “SDP” with “SMP”.
All	Delete all occurrences of “It shall cover all contractual clauses concerning this topic.”
4.1 Software development process	Replace with: The proposed standards under which the software development activity shall be conducted is to be stated, for example, MIL–STD–498, RTCA/DO–178B, IEEE 12207.0. The actual scope of application shall be detailed for each CSCI including sub-contracted items. The description should justify and link the selected life cycle models to project risks, major milestones, work products, deliverables and development phases to demonstrate its appropriateness. This section shall clearly outline the proposed development life cycle, detailing the use and the functional content of incremental builds. Schedule date and objectives for each activity shall be specified in latter sections. Note to Contractor: Contractors are encouraged to identify a build strategy that mitigates project risks and allows early access and usage of system components where applicable.
4.2.1 Software development methods	Add: Standards used for the following specific activities are to be detailed, including reference to company documents: (a) analysis and design techniques (object orientated, structured etc); (b) coding standards; and (c) testing techniques.
4.2.2 Standards for Software Products	Replace item (e) of the list with: e. Restrictions, if any, on the use of programming language constructs or features. Reference, where possible, the language subset definition. Add item (g) to the list: g. Reference, where possible, the standardised language definition.

Affected Paragraph	Tailoring to be Applied
4.2.3.1 Incorporating reusable software products	Add: Implications for supporting the software shall be specifically addressed for each item affected and include an assessment of vendor viability, level of support available, alternate sources of support, ownership of intellectual property rights, licensing arrangements (including costs and restrictions), dependencies such as operating system and/or hardware compatibility and constraints.
4.2.4.1 Safety Assurance	Add: It shall describe the integration of software safety as part of the system safety program. It shall include the tailoring and use of selected software safety standards and guidelines and associated data deliverables.
4.2.4.4 Assurance of other critical requirements	Add: It shall describe any mission critical software and the steps either taken or planned to ensure failure of this software will not compromise the system's mission.
4.2.5 Computer hardware resource utilisation	Add: It shall describe the interpretation of any resource utilisation requirements and how the satisfaction of these requirements will be verified.
4.2.7 Access for acquirer review	Replace with: This paragraph shall describe the approach to be followed for providing the Commonwealth and its authorised representatives access to Contractor and Subcontractor facilities for review of work products, activities and data including engineering and measurement data. Access should include at least physical access to facilities and preferably include electronic access to data (eg measurement data) and work products (eg design information).
5.2.1 Software engineering environment	Add: It shall include details of the software engineering environment including computing resources (number, type, configuration, etc.), and the associated performance requirements of the environment (eg required compile and link times). For safety critical software, this paragraph shall address the certification implications of the environment.
5.2.2 Software test environment	Add: It shall include details of the software test environment including computing resources (number, type, configuration), special test equipment and the associated performance requirements of the environment (eg simulator fidelity, instrumentation, recording etc.). For safety critical software, this paragraph shall address the certification implications of the environment.
5.2.5 Non-deliverable software	Add: It shall identify any non-deliverable software and describe how this software will be treated differently from deliverable software. It shall address specifically the application and tailoring of the standards identified for software development to non-deliverable software. For safety critical software, this paragraph shall address the certification implications and use of non-deliverable software.

Affected Paragraph	Tailoring to be Applied
5.4.1 System-wide design decisions	Replace with: This paragraph shall include details of how system design decisions affecting or affected by software are to be made and recorded. It should address how such decisions and the rationale for making them will be preserved and applied during through life support of the system.
5.5 Software requirements analysis	Add: It shall describe how software requirements will be identified and allocated to software components, how software requirements will be reviewed to ensure a common understanding with relevant stakeholders and how software requirements will be managed and controlled.
5.6.1 CSCI-wide design decisions	Add: It shall detail the criteria used to define and select CSCIs including the rationale for each of the selection criteria. It shall include design decisions regarding the partitioning of the software and the consideration given to enhancement and modification during through life support of the software. It shall include a justification for use of the specified programming language (or language subset), for the CSCI. Factors to consider in the language justification are described at AAP7001.054 Sect 2 Chap 7 Para 77.
5.13.7 Transition to the designated support site	Add: This paragraph shall detail the management strategy and plans for the transition of the software development capability to the support agency and address any special considerations (eg preservation of safety certification). It shall identify all items that have any limited or restricted warranty, data rights or licensing agreements including any other limitation on the delivery or support of the item. It shall describe all provisions, which ensure the Commonwealth's rights concerning the delivered software and associated data, and describe the plans for transferring any required licenses, warranties and data rights to the Commonwealth or its nominated representatives. It shall identify and describe those items of the development software engineering environment that will be transitioned into the software support environment including those items used for integration and test of the software and any special test equipment. Where a Transition Plan, covering transition planning for software as indicated above, is separately available to the Project Authority this section may reference that source. Where a software support environment is to be provided, the scope of changes possible to the CSCIs using the support environment, is to be detailed. This assessment shall include consideration of provided design data. Note that demonstration of successful CSCI compilation from source code, using the support environment, shall be included in the project plan.
5.18.1 Joint technical reviews, including proposed set of reviews	Add: Note to Contractor: Contractors are encouraged to propose informal technical reviews that allows commonwealth involvement in company review activities. The aim is to limit the formal reviews to address project progress and management issues.

Affected Paragraph	Tailoring to be Applied
5.19.1 Risk management	Add: This paragraph shall detail the techniques used for identifying software related risks and mitigation strategies. It shall include details of any software risks identified and the selected mitigation strategy to be adopted where these are not detailed in the Contractor's Risk Management Plan and Risk Register.
5.19.2 Software management indicators	Add: This paragraph shall detail the use of measurement as a management tool. It should identify how the Contractor intends using measurement to mange the development and acquisition of software for the project. Where this information is available to the Project Authority elsewhere this section should reference the relevant information and provide a summary of the measures used for software management.
5.19.4 Subcontractor management	Add: This paragraph shall detail the Contractor's plans for managing the software engineering activities performed by Subcontractors. It shall identify and describe the scope of the software activities to be undertaken by the Contractor and each of its Subcontractors performing software engineering activities. It shall describe the Contractor's plans for review and approval of Subcontractor plan and processes. It shall describe the Contractor's plans for monitoring the progress of Subcontractor activities and how significant deviations from Subcontractor plans will be identified and addressed.
5.19.6 Coordination with associate developers	Add: This paragraph shall describe the plans for coordination of software engineering efforts with associated developers. Such coordination may include interface definition and control, the use of integrated product teams, as well as the support to be provided during integration and verification activities.
5.19.7 Improvement of project processes	Add: This paragraph shall provide details of the Contractor's and associated organisations software engineering process improvement activities specific to this project. Where this information is available to the Project Authority in a Project Process Improvement Plan or equivalent then this section should provide a reference to the information.
6. Schedules and activity network	Add: This paragraph shall present and describe the proposed software schedule and include a clear mapping of the life cycle development phases and major milestones. This paragraph shall include the rationale for the durations given in the schedule and include the basis of estimate, estimating assumptions and the selection of coordination points and linkage with the Contract Master Schedule.

SOFTWARE LIST

1. DID NUMBER: DID-ENG-SW-SWLIST-VF

2. TITLE: SOFTWARE LIST

3. DESCRIPTION AND INTENDED USE

The Software Item List identifies and describes each item of software forming a part of the Supplies for the project, including additional attribute information on each item.

The Software Item List is used by the Commonwealth to achieve early visibility into the quantity and nature of software to be supplied and supported.

4. INTER-RELATIONSHIPS

Nil.

5. APPLICABLE DOCUMENTS

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled “General Requirements for Data Items”.

6.2 Specific Content

6.2.1 General

The Software Item List shall identify each software item of the Mission System that is a CSCI or a component of a CSCI that wholly satisfies the definition of a software category. No software item by definition is made up of software of more than one software category.

The following categories shall be used to identify software items:

a. Application Software (A);

b. Commercial Off The Shelf (COTS) Software (C);

c. Firmware as Hardware (F); and

d. Non-Deliverable Software (N).

6.2.2 Definition of Terms

All special terms used in the list shall be defined. In particular, terms such as “function point” or SLOC shall be defined in detail. Note that where multiple definitions exist for the one term, the applicable definition for an item shall be clearly identified.

6.2.3 Software Item List

The following information shall be provided for each major CSCI. CSCI specific information should be provided in the form of a consolidated table, included in the recommended section of a TSMP, or separate forms for each CSCI. Contractors may use their preferred format for the Software Item List, provided all information requirements of Table 7–A3–1 are met. The Software Item List shall contain the information identified in Table 1 for each software item in a hierarchy that reflects the system product breakdown structure, i.e. the position of the

software item in the product breakdown structure shall be clearly identifiable. Table 7–A3–2 provides an example populated software list.

Table 7–A3–1 Software Item List Attributes

Attribute	*Description*
a) Parent System/ Subsystem	Identifies the parent system/subsystem of the CSCI to which the software element belongs.
b) Parent CSCI	Identifies the parent Computer Software Configuration Item (CSCI) for the item.
c) Item Identifier	Identifies the software item with a Project unique identifier.
d) Brief Description	A brief description of the items function.
e) Category	Applicable software category (One of A, C, F or N).
f) Type	The type of item, eg CSCI, CSC, CSU.
g) Language	The applicable software programming language, including version details where applicable e.g. Ada95.
h) Size (total)	The expected total size of the item (actual and/or estimated) at delivery. This attribute would typically be expressed in units of source lines of code (SLOC), function points or feature points. For items categorised as C or F enter N/A.
i) Size (reused)	The expected size of the software being reused expressed as a percentage or as an absolute using the same units as for Size (total). For items categorised as C or F enter N/A.
j) Size (mod)	The expected size of the reused software being modified prior to delivery expressed as a percentage or as an absolute using the same units as for Size (total). For items categorised as C or F enter N/A.
k) Size (new)	The expected size of newly developed software expressed as a percentage or as an absolute using the same units as for Size (total). For items categorised as C or F enter N/A.
l) Storage and Executing Medium	The mission storage and executing mediums, e.g. stored and executed from ROM, or loaded from disk and executed in RAM, loaded from Flash PROM and executed in RAM.
m) Applicable Standards	The software standard used/to be used, e.g. MIL-STD-498, RTCA/DO-178B, IEEE 12207.0.

Attribute	*Description*
n) Documentation	*The level of documentation to be supplied for each CSCI and the standard to which it was/is to be developed. For example, if using MIL-STD-498 a compliant SRS, IRS, SDD, IDD may constitute the document set. Specific documentation requirements may be detailed in the SOW.*
o) Applicable Safety Standard	The software safety standard used/to be used, e.g. RTCA/DO-178B. For non-safety related software enter N/A.
p) Software Integrity Level	The software integrity level (or equivalent) of the applicable safety standard.
q) Developing Organisation	Organisation that was/is responsible for creating the item.
r) Supporting Organisation	Organisation who is/will be responsible for supporting the item.
s) Target Platform	The target computing hardware and operating system.
t) Host Platform	The host computing hardware and operating system.
u) IPR Owner	*The Intellectual Property Rights to be granted to the Commonwealth for each CSCI shall be detailed. The information provided shall state the rights of the Commonwealth to contract a third party to make changes to the delivered software products. This information is to be provided in addition to any other specification of IP rights. A simple Yes/No for each CSCI is appropriate.*

Blank Page

Table 7–A3–2 Example Software List

Parent system	Parent CSCI	Item	Brief Descript	Cat	Type	Lang	Size total	Size reuse	Size mod	Size new	Storage and executing medium	Applicable standards	Doc	Applicable safety standards	SIL	Developer	Support Org	Target	Host	IPR owner
SIP	N/A	SIP1	Stores Interface Processor	A	CSCI	Ada 95	10k SLOC	40%	10%	60%	ROM	12207	SDPS DD IRS IDDST PSTR PSAC	178B	B	Company XYZ	Company XYZ	Power PC	VAX VMS	CoA

Blank Page

DATA ITEM DESCRIPTION

1. DID NAME: DID-ILS-SW-SWSP-V1.2

2. TITLE: SOFTWARE SUPPORT PLAN (SWSP)

3. DESCRIPTION AND INTENDED USE

The Software Support Plan (SWSP) identifies the items and procedures that are needed to perform life-cycle software support of the contractually deliverable application software (including support software). It describes the methods to be used to ensure the existence of a complete life-cycle support capability for the contractually deliverable software.

The Contractor uses the SWSP to define the management organisation, methodology and tasks necessary to support the contractually deliverable software. It will be used by the Contractor to identify the resources (eg, tools, skills, servicing and programming equipment) required to support Preventive Maintenance and Corrective Maintenance actions as well as the development of enhancements associated with the software through its service life.

The Commonwealth uses the SWSP to determine the level of software support required, and to assess the proposed program for the provision of software support. The tender shall tailor the information requirements of this DID based on the level of support offered for each CSCI. That is, greater levels of detail are required if a Commonwealth support agency is to conduct support that the development contractor. For vendor arrangements, detail of the extent of support and a contract to enforce it is required.

4. INTER-RELATIONSHIPS

The SWSP will form part of the Integrated Logistics Support (ILS) documentation as described in the Integrated Support Plan (ISP) (DID-ILS-MGT-ISP).

5. APPLICABLE DOCUMENTS

The following document forms a part of this DID to the extent specified herein:

MIL-HDBK-1467	Acquisition of Software Environments and Support Software

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled “General Requirements For Data Items”.

6.2 Specific Content

6.2.1 General

6.2.1.1 The SWSP shall comply with the content requirements of MIL-HDBK-1467, Appendix B.

6.2.1.2 All references to “Life Cycle Software Engineering Environment User’s Guide” shall be read as “Software Support Plan”.

6.2.1.3 All references to “guide” shall be read as “plan”.

6.2.1.4 The SWSP shall address software support for all software associated with both the Mission System and the Support System.

6.2.1.5 Add Para B3.3.1.1 The table shall include columns to describe the expected number of Trouble Reports that would be received annually, the estimated effort to rectify the Trouble Reports, the level of support proposed for each CSCI based on the likelihood of change and the resultant change capability.

NOTE TO TENDERERS

The remainder of this DID provides further explanation for the contents of the table described above; in particular the level of support and the change capability.

Support Approach

The contractor shall specify the software support approach that will be applied to each software product. The Contractor may define classifications, however, where appropriate the following classifications should be used:

(1) Vendor Support (VS). Direct support from the supplier/developer of the product. Support limited to commercially driven updates with no Commonwealth enforceable contractual performance requirements. Such updates would be procured at the discretion of the Commonwealth. VS may be appropriate where an item is a Commercial Off-the-Shelf (COTS) product employed without modification.

NOTE

Unless an enforceable agreement is provided for support, it is unlikely that the Commonwealth will be able to influence, or even obtain support under this arrangement. This may have serious impacts on the actual future capability of the proposed system. The Commonwealth requires appropriate enforceable agreements for support of key system components and will evaluate this approach as unacceptable for certain components.

(2) Contracted Support Facility (CSF). Support facility established and maintained by the Contractor to directly support Commonwealth software products. The Contractor shall maintain the capability to undertake software changes and provide direct response to requests for software changes and analysis of failure data.

(3) Commonwealth Support Facility (RSF). The establishment of a software support facility to be owned and maintained by the Commonwealth that can be used to modify specified software products. The facility location shall be determined by the Commonwealth and may be established at a Contractor's site.

Resultant Change Capability

Consideration of the 'Possible Change Scenarios' shall be used to determine the scope of capability provided by the support facility. Obtaining a software change capability is dependant on Intellectual Property Rights (IPR) and access to relevant engineering data. A proposed change capability must be supported by the appropriate IPR and engineering data. Based on the proposed support approach the capability of any provided support systems or contractual arrangement shall be specified as:

(1) Rectification. Capability to analyse and rectify faults. The necessary tools to make a software change shall be included, however, testing and other related activities may require the direct use of aircraft.

(2) Development. A full development and test capability similar in scope to the initial development environment, that can produce significant software changes to the system. The capability to do off-aircraft DT&E and provide simulated stimulus for testing purposes shall be provided. Full design disclosure and IPR shall also be provided.

(3) Enhancement. A full development environment with additional simulation, modelling, and analysis tools that would allow significant enhancement of system operation. The development and test environment shall allow analysis of actual system performance using appropriate tools and techniques. The testing facilities shall enable environment testing of real time performance where appropriate to the systems. Full design disclosure and IPR shall also be provided.

CONTRACT DELIVERABLE REQUIREMENTS LIST

1. ***Software Product Specification (SPS).*** Requirements 3, 4, and 5 of the SPS DID, (Annex A, Document 1, DI-IPSC-81441) provide detail on how a CSCI is produced from delivered source. These sections are vital for in-service support. If Firmware is a delivered product then consideration should be given to including the contents of the **Firmware Support Manual (FSM) (Annex A, Document 1, DI-IPSC-81448)** in the SPS. This document could be delivered as a programmers' guide to the CSCI.

2. ***Software Installation Plan (SIP) and Software Transition Plan (STrP) (DI-IPSC-81428, 81429).*** These documents should be applied when a significant transition of a software support facility or similar capability is planned. The SIP may be of assistance when a software product is to be installed by the Contractor at various sites.

3. ***Operational Concept Document (OCD) (DI-IPSC-81430).*** An OCD may be developed in consultation with the user, to identify an operational need that can then be translated into an acquisition requirement. This document may be produced by the ADF or an independent third party, and provided to the Contractor as a means of communicating user requirements.

4. **System/Sub-systems Specification (SSS), System/Sub-system Design Description (SSDD), and Interface Requirements Specification (IRS) (DI-IPSC-81431, 81432, 81434, 81436)**. These additional documents can be requested when the development of the Hardware Configuration Item associated with the software product is also being developed. These documents along with the Interface Control Documents (ICDs) provide the overall systems requirement analysis and design documents.

5. ***Software Users Manual (SUM) and Software Input/Output Manual (SIOM) (DI-IPSC-81443, 81445).*** Given that user interaction with a CSCI is possible, the requirement for a Users' Manual should be enforced. The requirements of both of the SUM and SIOM should be integrated into a single document.

6. ***Computer Operation Manual (COM) (DI-IPSC-81446).*** This DID is only applicable in cases where instructions on operating and testing the hardware are required to supplement the users' guide. It may be applicable for systems where a software test program is delivered with the system.

7. ***Computer Programmers Manual (CPM) (DI-IPSC-81447).*** This DID requires detailed information on the programming environment of the target computer system, which should be met through supplier's guides. The CPM document should be delivered with the embedded processing system.

8. ***Firmware Support Manual (FSM) (DI-IPSC-81448).*** This DID is required when firmware products are involved. The content of this document is best included with the SPS.

9. COTS manuals are the acceptable and cost effective format for supply of the COM, CPM, and SUM. If additional information is required it should be combined into a single document

Blank Page

SAMPLE CBD ENTRIES FOR SOFTWARE

Design Standard*	Rev. Status	Airworthiness Requirement*	Compliance Method*	NAA Involvement*	Compliance Evidence Documents*	Comments*	ADF Use Only: Compliance Finding Agency*	ADF Use Only: Compliance Outcome*	ADF Use Only: Finding Reference*
(Prior Certification) DO-178A	1985	Software Assurance	S	DGA	SAS and Type certificate	Issue Paper – A330/A340 application	XXPO	Compliant	XX/123/33 (2)
(Slightly Modified Software)* DO-178A	1985	Software Assurance	IAT	DGA	SAS and Type certificate	Issue Paper – A330/A340 application	XXPO	Compliant	XX/123/33 (5)
(New and Modified items)* DO-178B	1992	Software Assurance	IAT	DGA	SAS, DGA report		XXPO	Compliant	XX/123/33 (12)
MIL-STD-498	1994	Software Engineering	IAT	DGA	SMP, QA		XXPO	Non-compliant (acceptable)	XX/123/33 (23)
(New and Modified items)* DO-178B	1992	Software Assurance	IAT	-	SRS, SDD, STD, STR, SPS, SVD, SAS		XXSPO	Compliant	XX/321/22 (4)
(Prior Certification) DEF STAN 00-55	1997	Software Assurance	S	RAF	Software Safety Case and Type Certificate		XXPO	Compliant	XX/456/33 (2)
(Slightly Modified Software)# DEF STAN 00-55	1997	Software Assurance	IAT	RAF	Software Safety Case and Type Certificate	Issue Paper – previous application	XXPO	Compliant	XX/456/33 (5)
(New and Modified items)# DEF STAN 00-55	1997	Software Assurance	IAT	RAF	Software Safety Case and RAF Report		XXPO	Compliant	XX/456/33 (11)

* As approved in the DO-178B Plan for Software Aspects of Certification

As approved in the DEF STAN 00-55 Software Safety Plan

Blank Page

SOFTWARE COMPLIANCE FINDINGS

INTRODUCTION

1. This annex examines the concepts, key activities and work products that a compliance finding agency (CFA) will encounter when making a software assurance compliance finding for a software-intensive airborne system. It extends on the key issues raised in this chapter, in particular, the key issues relating to Compliance Finding and Direct Commonwealth Oversight.

CLARIFICATION OF KEY ISSUE – COMPLIANCE FINDING

2. The above key issue states that '*a compliance finding shall be performed against the Software Assurance standard which is defined directly or indirectly in the certification basis'*. As with all compliance findings, it must be based on relevant evidence, performed by a competent agency, and relevant to the configuration being offered for acceptance and the role and environment in which the aircraft will be employed. In general, relevant evidence refers to formal documents, however, it can also be equivalent data captured in a tool and placed under configuration management. Whilst formal or informal discussion with developers provides confidence in the compliance finding and may contribute to a reduction in the depth of the compliance finding, it does not constitute evidence.

3. CFAs should endeavour to progressively review evidence as it is produced, rather than attempting to establish compliance at the end of the development. From past experience, this progressive approach has many advantages, for example:

a. it enables timely on-site visits to assess compliance;

b. where the development entails multiple builds, it ensures CFA involvement in earlier builds;

c. it enables the CFA to detect shortfalls in the contractor's understanding and implementation of the software assurance standard early in the development process; and

d. it enables the CFA to properly evaluate their level of involvement, so as to ensure that an appropriate amount of oversight is applied to the compliance finding activity.

Determining the Level of Involvement in Compliance Findings

4. The level of compliance finding rigour is normally dictated by the complexity of the software development effort and the abilities of the software development agency. This section provides guidance on the likely competency requirements for the CFA, and the level (ie depth and scope) of their involvement.

5. ***CFA competency***. For higher-risk software development efforts, for example a complex software development project by a non-OEM, the competencies required by the CFA would include:

a. a comprehensive understanding of the principles of software engineering;

b. basic familiarity with the principles of aircraft system safety;

c. a full understanding of the ADF's approach to Design Acceptance, and the role that compliance findings play in that process;

d. some experience in the maintenance of airborne software;

e. preferably some previous experience with compliance findings;

f. sound knowledge of the relevant development and assurance standards; and

g. familiarity with software quality assurance concepts.

6. For lower-risk developments, the above requirements could be moderated somewhat. For example, requirements (b), (c) and (g) will likely provide adequate coverage for a low-risk development activity.

7. Where local staff competencies are low, independent third parties including Independent Safety Assessors (ISAs), may assist in performing these tasks. Note however that to be most effective, ISAs need to be engaged early in the program to ensure that their advice can be injected with minimal cost and schedule impact. When introduced late in the program, ie after CDR or DDR, advice of potential shortcomings in the safety program will tend to be more purist in nature, difficult to reconcile and is often poorly received because of its cost or schedule impact. From past ADF experience, late ISA involvement results in the highlighting of potential (but unprovable) weaknesses in the system design, but no material increase in the safety of the system.

8. ***Scope of Compliance Finding.*** The scope is a function of the software level (or equivalent), which should be identified through the system safety program and is usually an outcome of the preliminary hazard analysis (or equivalent). For modifications to an already developed system, identifying the software level should simply be a matter of referring to the system safety assessment for the original aircraft.

9. Figure 1 provides a good starting point for assessing the required scope of the compliance finding activity. For example, modification of RTCA/DO-178B Level D software would initially indicate a low level of involvement; however, changes to Level A software may lead to a HIGH or MEDIUM level of involvement. This is based on civil guidance provided by the FAA through Order 8110.49, Chapter 3 – Determining the Level of FAA Involvement in software projects.

RTCA/DO178B Software Level	Level of Involvement
D	LOW
C	LOW or MEDIUM
B	MEDIUM or HIGH
A	MEDIUM or HIGH

Figure 7–C–1 Scope Criteria

10. ***Depth of Compliance Finding.*** The level of involvement ambiguities for software levels A, B and C in Figure 1 are included to account for the perceived level of development risk, and may be impacted by:

a. the developer's demonstrated software development capability;

b. the software product's service history, for example, prior certification of a previous version of the modified software product by a recognised National Airworthiness Authority (NAA); and

c. the complexity/novelty of the system.

11. Based on the criteria in para 10, and any other criteria deemed to be relevant by the PO, a risk level can be assigned using any standard risk management process. This can then be used as a basis for the final level of involvement determination. Take for example, a CSCI assessed as being DO-178B software level B. The initial level of involvement indication based on this software level would be either MEDIUM or HIGH. If the proposed change is perceived as a higher risk activity, then it would be appropriate to choose the higher of the two potential levels of involvement.

12. Once the level of involvement assessment has been performed, the specifics of the compliance finding agency's involvement should be documented in a Compliance Finding Plan (CFP). Appendix 1 of this Annex provides a suggested template for a Compliance Finding Plan. Figure 2 provides an example compliance finding agency involvement for HIGH, MEDIUM and LOW levels.

Developments with no Software Safety Standard Identified

13. The conventional ways of determining random failure rates in hardware (such as MTBFs etc.) do not apply to software. For this reason, evaluating the adequacy of the software development process is the primary way to gain confidence that the resulting software will be safe. A contracted software safety standard is therefore a key

requirement. Where one has not been contracted, and the system safety assessment identifies that the software has the potential to impact safety, an assessment of a software development against the ADF's preferred software assurance standard, RTCA/DO-178B, should be used as a benchmark for measurement of adequacy. Even if the Commonwealth cannot influence the development process, this assessment may still be useful in guiding the Commonwealth on imposing additional testing requirements.

Level of Involvement	Typical Project Decisions
HIGH	• CFA and DGTA involvement throughout the software life-cycle, including mentoring, on-site reviews, and desk reviews. • CFA and DGTA endorsement of all plans (PSAC, SMP) • CFA and DGTA endorsement of SAS, SCI and Verification Results • Other DGTA and CFA reviews as required.
MEDIUM	• Moderate DGTA involvement initially (planing, regulation and policy interpretation, and some mentoring) and toward the end of the project (review of SAS) • CFA to conduct at least one on-site review but mostly desk reviews of data • Review of PSAC, SCI, SAS • Potential review of Software Verification Plan, SQA plan, SCM plan, and SDP
LOW	• Minimal DGTA and CFA involvement • Review of PSAC, SCI, and SAS by the CFA

Figure 7–C–2 Example Program Decisions Based on Level of Involvement Determination

CLARIFICATION OF KEY ISSUE – DIRECT COMMONWEALTH OVERSIGHT

14. The above key issue stipulates that 'direct Commonwealth oversight is required for all software changes to safety critical systems regardless of whether the change is considered simple or complex'. This key issue specifically relates to in-service software modifications since there is potential for even simple software changes to have unintended consequences, due to the difficulty of ensuring that modification of one area of code does not adversely impact another area. As such, direct Commonwealth oversight is warranted to ensure that the integrity of the system is retained.

Assumption of Design Acceptance

15. Some changes to software residing in a safety critical system, in particular those smaller changes that do not directly affect a safety critical function, may not necessarily fall into one of the categories restricted in the TAMM (Reg 2.5.9c) for permitting Assumption of Design Acceptance. This key issue ensures that any software change to safety critical systems always has *some level of direct Commonwealth oversight*, that is, the design change will still be progressed as a typical minor change to type design but it should be judged as 'significant' regardless of the scope of the change. The following sections outline in more detail the level of direct Commonwealth oversight required.

16. The Commonwealth must be assured that the modification complies with specification requirements, in particular the standards for software development, software assurance and other related standards. The amount of verification will usually be a function of the software level and hence an assessment similar to the level of involvement determination as outlined in paras 4-12 can be made. The Commonwealth verification oversight effort can be divided into the oversight of the software lifecycle processes, categorised as follows:

a. ***Planning Processes*** – processes that define and coordinate the activities of the software development and integral processes for a project.

b. ***Development Processes*** – processes that produce the software product including the software requirements process, the software design process, the software coding process, and the integration process.

c. ***Integral Processes*** – processes that ensure the correctness, control and confidence of the software life cycle processes and their outputs. These include software verification, configuration management (CM) and quality assurance (QA). The integral processes are performed concurrently with the software development process throughout the software lifecycle.

17. The first two lifecycle process categories – planning and development – are assumed to require the least amount of oversight from the Commonwealth, because these are expected to be regularly addressed through both internal and external audits (e.g. AEO audits). Integral processes on the other hand, require the most oversight. Even though QA and CM processes may be monitored by regular internal and external audits, the Commonwealth may still inspect sample records (depending on the assessed level of involvement) to verify these processes, or even take part in a functional or physical configuration audit (FCA/PCA). The bulk of the effort however, should be directed towards the software verification processes. This will involve confirming that requirements traceability is evident and the test coverage is appropriate. An assessment of partitioning arguments should also be conducted to ensure that an appropriate level of isolation between functionally independent software components exists, if possible.

18. The recommended Commonwealth oversight focus described above is visually represented in Figure 3. The unshaded areas identify areas where the Commonwealth should focus their oversight efforts.

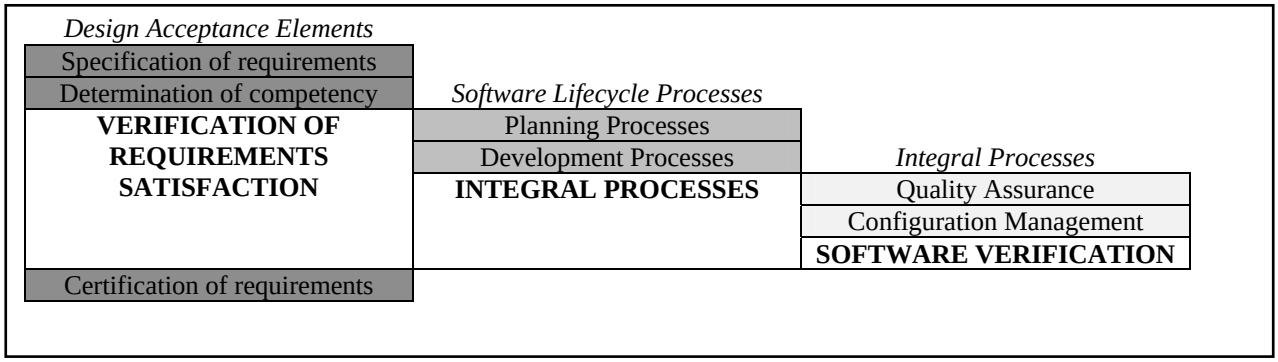


Figure 7–C–3 Focus of Direct Commonwealth Oversight of Software Changes to Safety-Critical Systems

19. The team providing the Design Acceptance recommendation to the DAR will require the same competency requirements as outlined in para 5. Since it may not be always possible to have available staff with the required competency, independent third parties may be considered to assist in performing these tasks.

COMPLIANCE FINDING PLAN TEMPLATE

1. Table 7–C1–1 presents a template for a Compliance Finding Plan. The plan should be brief and useful, covering only the information that will assist the Compliance Finding Agency (and external stakeholders, if any) in scoping the level of involvement in the compliance finding activity.

Table 7–C1–1 Compliance Finding Plan Template

Para	Instruction
1.0	Scope. State the purpose of the system and the software to which this document applies. Provide a brief description of the system and software.
2.0	Referenced documents. List any applicable documents referenced in the Compliance Finding Plan.
3.0	Plans for performing general software safety assurance activities. Divide this section into the following paragraphs.
3.1	Software Safety Assurance Standard. Briefly describe the software safety standard under which the CSCI/s will be developed. Include a brief description of the safety standard used to determine the software level of the CSCI.
3.2	Software Safety standard implementation. Briefly describe and provide references to company documentation that describe how the safety assurance standard will be implemented.
4.0	Assessment of Level of Involvement Divide this section into the following paragraphs.
4.1	Assessment of the Scope of Involvement Present the determination of the 'scope' of involvement by the compliance finding agency. Provide justification for the assessment, including reference to the DO-178B software level on which the scope is based. Guidelines for assessing the scope are provided in the Annex.
4.2	Assessment of the Depth of Involvement Present the determination of the 'depth' of involvement by the compliance finding agency. Guidelines for assessing the depth of involvement are provided in the Annex.
4.3	Overall Level of Involvement Based on 4.1 and 4.2, state the overall level of involvement
5.0	Major Project CF Activities and Decisions Divide this section into the following paragraphs
5.1	Work products for review List the major software lifecycle work products and data that the compliance finding agency intends to review and/or endorse and the major activities that the compliance finding agency intends to oversee (e.g. FQT). This list of work products may be categorised as follows: Planning documents (e.g. PSAC) Development documents (e.g. SDD) Verification documents (e.g. STR) Final Certification documents (e.g. SAS)
5.2	Schedule Propose a schedule for completion of major compliance finding milestones including on-site reviews/audits, desk reviews/audits, mentoring (if applicable), training etc.
5.3	Interfaces Outline the compliance finding team's interface with other agencies (e.g. ISAs)
6.0	CFA Competencies Outline the competencies required by the compliance finding activity and identify individuals who will be used to make the compliance finding. Justify any deviations from the competency requirements. Competency attributes are listed in the Annex.
7.0	Resource Requirements Provide a list of required resources for the total compliance finding effort.

Blank Page

SECTION 2

CHAPTER 8

EMBEDDED COMPUTER SYSTEMS

INTRODUCTION

1. DEF STAN 00-970 provides airworthiness requirements for active control systems in Part Issue 2 Section 3.10.47 for aeroplanes, and in Part 2 Issue 1 Chapter 207 for rotorcraft. More general airworthiness requirements for Avionics Equipment Installations are found in DEF STAN 00-970 Part 1 Issue 2 Section 6.2 for Aeroplanes and Part 2 Chapter 725 for Rotorcraft. Other requirements for embedded computer systems are distributed across various chapters. However, there are design aspects of embedded computer systems such as computational performance, spare capacity and architecture that are not adequately addressed by DEF STAN 00-970.

2. This chapter and Annex A supplement DEF STAN 00-970 to reflect ADF requirements by addressing the design requirements for various elements of computer hardware employed to implement functional requirements. It is aimed at guiding the acquisition process towards open architecture avionics systems and supports the compatibility requirements of DEF STAN 00-970 for Avionics Equipment Installations.

3. The guidance provided in this chapter is aimed at procuring embedded processing systems that are upgradeable. The rate of change in the commercial market place has resulted in general purpose processing systems and processors greatly exceeding the performance of military standard systems in many areas. An ADF goal for embedded computers is that they have the ‘critical mass’ to support continued development for the foreseeable future. A vast range of embedded processing systems are employed to meet design requirements of advanced avionics and support equipment.

4. On a small scale, simple processing systems are embedded in instruments and actuator controllers. These embedded computers tend to execute small programs (less than 30K lines) and operate in narrow functional domains. As a result, these systems require little or no modification in-service and are usually modified based purely on functional errors.

5. By contrast, major embedded systems perform functions across a range of problem domains. These sub-systems tend to continually evolve with the overall system through the constant addition and modification of functionality. These systems require considerable care during specification. The appropriate specification of these systems can eliminate significant costs associated with integration of new capabilities.

6. Embedded computer systems are designs that consist of hardware and software to meet system operational objectives. The software and integration requirements of embedded systems are covered in Section 2 Chapter 7 of this publication.

7. The information provided in this chapter is applicable to POs, SPOs, software support agencies (SSAs) and Defence contractors. This chapter is structured into five parts based upon the issues that should be addressed by these organisations when dealing with embedded computer systems for ADF aircraft systems and equipment. General Design Considerations covers the basic requirements for Embedded Computer Systems addressed in other chapters of this manual. Safety Critical Hardware deals with the TAA’s requirements for addressing hardware components related to safety critical functions. System Architecture for Major Processing Systems concerns the architectural design requirements for processing systems which contain embedded computer systems. System Computational Performance deals with requirements related to real-time systems. Software In Service deals with support requirements to monitor the integrity of the system throughout its life.

GENERAL DESIGN CONSIDERATIONS

8. The basic requirements for design of embedded computers are the same as for other avionics equipment, including power supply, weight, Electromagnetic Environmental Effects (E^3), survivability and maintainability.

9. ***Electromagnetic Environmental Effects (E^3).*** Requirements for protection against Electromagnetic Environmental Effects (E^3) are addressed in Section 2 Chapter 2 of this publication.

10. ***Environmental Qualification.*** Embedded computer systems may be designed from the beginning to military requirements or they may be militarised (ie ruggedised for military use). Militarisation may include environmental protection against: climatic (humidity and salt atmosphere), thermal (temperature at altitude and temperature cycling), physical (mechanical shock, vibration and explosive conditions) and electrical (lightning and other power transients) stresses. Environmental Qualification is addressed in Section 2 Chapter 3 of this publication.

11. ***Built-In Test (BIT).*** Requirements for Built-In Test (BIT) are addressed in Section 2 Chapter 3 of this manual.

SAFETY CRITICAL HARDWARE

12. Most aircraft procured by the ADF are based on existing aircraft types and most aircraft systems and equipment have been qualified for use on existing aircraft. To meet the specific requirements of the ADF, these existing aircraft, aircraft systems and equipment are developed further. In such cases, the ADF relies on the prior selection and application of hardware design standards by industry during development. In procuring aircraft, aircraft systems and equipment, the TAA's requirement for demonstration that the system has a failure probability, commensurate with the criticality of the function it provides, assures that hardware has a level of integrity appropriate to its function.

Reliability Qualification

13. To demonstrate the hardware components meet failure probability objectives, newly developed hardware components should be qualified to a reliability standard such as MIL-STD-781 - Reliability Testing for Engineering Development, Qualification, and Production. The rigour applied in testing should be commensurate with the system criticality of the component. Field data may be provided as verification of the reliability of the component; however, some engineering judgement will be necessary to determine the relevancy of this data to the particular component in question, considering the application and environment under which the data was gathered.

Design Assurance Activities

14. As stated in Section 2 Chapter 1 of this manual, SAE ARP 4754 invokes RTCA/DO-tbd, Design Guidance for Airborne Electronic Hardware. This standard is appropriately applied when the substantiation of a hardware design cannot be accomplished through rigorous testing and analysis using deterministic techniques because it is too complex. Activities for development assurance are applied according to the five levels of system development assurance defined in ARP 4754 according to the system criticality of the component. Currently, there are limited instances foreseen where this standard would be useful in ADF procurements.

15. Section 2 Chapter 1 of this manual provides for the achievement of system failure probability objectives. The requirements for hardware are derived from system safety engineering activities during the system development process.

SYSTEM ARCHITECTURE FOR MAJOR PROCESSING SYSTEMS

Open System Architectures

16. Irrespective of the original intent, major avionics processing systems are often upgraded to provide enhanced capability or simply to meet the original specification. Open system architectures are layered architectural designs that allow sub-systems and/or components to be readily replaced or modified. This is achieved through the use of standardised interfaces between layers. The selection of open system architectures through both upgradeable processors and buses will reduce costs for long-term in-service support. This is particularly relevant to the ADF because the basic architecture of our avionics systems typically remain static for considerable periods and then must be integrated with newer generation components with more demanding processing requirements.

17. For major system acquisition projects with long lead times (one to two years), consideration should be given to contracting the next generation processor/processing system from the outset. If a truly upgradeable system is offered, development can be achieved on the current generation and delivered on the next. SAE AS 4893 - Generic Open Architecture (GOA) Framework may be useful in specifying requirements for an open architecture system.

18. This type of flexibility was demonstrated in the P-3C Upgrade, where a faster processor of the same family was added early in the project, and the C-130J, where a second processor card was added to the mission computer to

alleviate performance problems. In the case of the C-130J, the adoption of a faster processing card of the same processor family may also have been possible. Paragraphs 1 through 4 of Annex A (Embedded Computer System Requirements) to this chapter provide for the specification of open architecture systems.

Redundancy

19. As a minimum, aircraft requirements for redundancy should be driven by analyses performed in the system safety engineering activities performed during design. Requirements for system safety engineering are addressed in Section 2 Chapter 1 of this manual.

20. For mission-related processing functions, system modes of degradation and tolerance for failure need to be considered. Redundant mission systems may be included in an aircraft to increase mission success and survivability. Requirements for survivability and mission redundancy need to be included in the weapon system specification for consideration during design.

Distributed Computing

21. Distributed processing, whereby computer resources are dispersed throughout the aircraft to increase survivability, is recommended where practical. Distributed computing systems rely on high speed, interconnecting buses. The selection of the type of bus architecture, communication protocol and physical interconnection depends on the data transfer and reliability requirements for the system. In addition, distributed systems offer economic, speed, reliability and incremental growth advantages over centralised systems.

22. The use of standard intra-bus systems in the embedded processing system provides the ability to upgrade integral components such as the processor or support circuitry. Most modern bus standards allow multi-processors and re-configurable memory and I/O configurations. Every effort should be made to adopt standard internal bus systems like VME (P-3C and C-130J) that allow re-configuration of the embedded computer system.

Bus Interface Standards

23. For avionics systems, compatibility with new equipment is likely to be enhanced by the adoption of one of the following standards:

a. MIL-STD-1553B. A serial multiplexed bus with a 1Mb/s data rate.

b. MIL-STD-1773. A fibre optic multiplexed bus, consistent with MIL-STD-1553B data bus protocol.

c. STANAG 3910. A double line bus based on MIL-STD-1553B with an additional data bus. Data bandwidth 20Mb/s.

d. ARINC 429. A commercial bus standard similar in performance to MIL-STD-1553B but not directly compatible.

e. ARINC 629. An upgraded bus from ARINC 429 that is capable of 2Mb/s.

f. Emerging bus standards such as the High Speed Data Bus from the F-22, or the Very High Speed Optical Network, a component of the PAVE PACE Air Force avionics system architecture.

24. Paragraph 4 of Annex A provides for the specification of these bus interface standards.

Interface Control Documents

25. Due to their importance in system integration and follow-on support, Interface Control Documents (ICDs) deserve mention. When procuring systems, POs should aim to obtain a document that can be given to another Contractor for the replacement of sub-systems. In follow-on support, this type of modification is very common and is often not well served by existing design documentation sets. The ICD should include both the hardware and software aspects of the interface and is to ensure that no detail is specified in more than one document.

26. There is no existing Data Item Description (DID) that precisely states the requirements for an ICD that includes software and hardware details. This is because the format and content requirements to define an interface

vary from interface to interface. Project Offices should be aware that ICDs are not created purely because a physical or software interface exists. Other factors, such as developmental status of the sub-systems/components, commonality of the interface throughout the system and involvement of separate development teams will influence the requirement to produce a separate ICD. In cases where an ICD is not created, the detail necessary to fully describe the interface is subsumed into a sub-system specification or drawing.

27. MIL-STD-973 does not contain a description of an ICD, but instead calls out DID DI-CMAN-81248 which defines Interface Control Drawing Documentation. MIL-STD-498 DI-IPSC-81436 provides the detail for format and content required for software interfaces. In practice, defining the physical interface may simply require reference to a physical implementation of MIL-STD-1553B or RS232. Whatever the format and content requirements of each DID, the intent is to provide a single document for each unique interface which includes the necessary detail to comprehensively define the interface.

SYSTEM COMPUTATIONAL PERFORMANCE

Spare Capacity

28. Spare capacity represents a design factor for integrating software with hardware, and for future upgrades. With the continual enhancement of data processing requirements, the first level of in-service cost saving can be achieved by ensuring delivered hardware has sufficient spare capacity. The goal of providing spare capacity is to enable the system to be effectively upgraded to meet operational objectives while potentially skipping at least one generation of hardware upgrade to the processing system. The upgrade of computer hardware can have a significant related software cost in terms of compiler, tool and partial revalidation. This type of change should be kept to a minimum. Paragraph 5 of Annex A provides for the specification of embedded computer system spare capacity.

Timing Conditions

29. Many of the exact performance criteria may be unknown by the project team. While every endeavour should be made to quantitatively specify the key conditions for response times and update rates, the more cost effective approach may be to have the Contractor provide them. In this scenario the functional requirements could be included with the RFT with only the names and types specified and the action rates/delays unspecified. The Contractor could then propose action rates/delay parameters with related justification. This would at least provide quantitative measures for final acceptance that are agreed. Paragraph 5 of Annex A provides for the specification of timing conditions.

SUPPORT IN SERVICE

Test Software for Embedded Systems

30. For complex systems, real-time logging of events is vital to allow for fault rectification and follow-on software support. Serious consideration should be given to including this capability for embedded processing systems. Paragraphs 6 through 9 of Annex A provide for specification of test software for embedded systems.

Data Storage and Handling

31. ***Loading Software.*** Software must be loaded onto various target computers, and therefore various media, memory loading equipment and procedures are required for the different applications. Operational Flight Programs (OFPs) are either loaded onto target computers while at the workbench following maintenance, or while fitted to the aircraft. These two environments have different requirements, including portability and power supply. MIL-STD-2217 specifies standard protocol for a memory loader/verifier multiplex bus interface with avionics systems. Systems for loading OFPs may be designed with in-built maintenance diagnostics, for example the Avionics Fault Tree Analyser developed for the F/A-18. Paragraph 10 of Annex A provides for specification of fault recording.

32. ***Data Storage.*** A central copying and storage site for software is required, usually within the software support agency. The tapes which are issued to operators should be ruggedised for military use. Mission data is prepared immediately prior to a flight, and therefore must be loaded on the flight line upon power-up of the aircraft. Storage media for this application must be portable and compatible with both mission preparation equipment and aircraft ports. Mission and maintenance data is downloaded following flight, and should be deposited on the same storage device as pre-flight data. Therefore the device usually remains in the aircraft for the duration of the flight, and should be accessed if memory becomes contaminated and requires re-loading. Paragraph 11 of Annex A provides for specification of embedded processing data storage and handling characteristics.

Annex:

A. Embedded Computer System Requirements

Blank Page

EMBEDDED COMPUTER SYSTEM REQUIREMENTS

System Architecture for Major Processing Systems

1. The _____ System shall be implemented using upgradeable technology components which are of commercial standard (IEEE/ANSI etc) or military standard design which results in:

a. processors which have a planned and demonstrable upgrade path, and

b. buses which are recognised or soon to be recognised by a standards body.

2. The _____ System shall utilise processors and bus systems which are supported by more than one manufacturer.

Physical Modularity

3. The _____ System shall be optimised for physical modularity, whereby there is a high degree of cohesion and interaction between functions implemented on the same physical sub-system.

Embedded Computer System Interfaces

4. The _____ System shall utilise open architecture bus structures for both internal and external connections between embedded processing systems.

System Computational Performance

5. The _____ System shall meet the following spare capacity and response time requirements:

a. Under the specified maximum load scenario the processing _____ System shall have the following characteristics:

(1) 50% spare processing time, and

(2) 50% spare I/O throughput capacity.

b. If multiple processing elements are used to meet this requirement, the developer shall attempt to evenly distribute spare capacity between all processors.

c. The processing system shall be capable of storing and executing a version of the operational program that is twice the size (measured in bytes) of the delivered version of the application program.

d. The _____ System shall respond to event _____ with completed action _____ within _____ seconds.

e. Under specified maximum load conditions, the _____ System shall complete cyclic action _____ at a rate of _____ Hz.

Test Software for Embedded Systems

6. All embedded computer systems shall include test software to verify that the host hardware and interfaces to associated processing systems are operating correctly.

7. The test software shall provide the capability for the operator to verify that host hardware and interfaces are operating correctly.

8. All test software shall be capable of being amended to incorporate modifications to the aircraft configuration.

9. The test software can be either in the form of a built-in test or a separately loadable program.

Data Storage and Handling

10. For systems that are capable of detecting and/or recovering from hardware and software errors, such errors shall be logged in an electronic format.

11. The _____ System shall use media which is optimised for data handling and storage in operational and support environments, in terms of size, weight, durability, capacity and speed. In particular the following requirements shall be met. Contractors are to propose how data is to be stored and handled, detailing the equipment and personnel requirements.

a. A deployed _____ System shall require at most the following data support requirements:___.

b. The time to load electronic ___ data onto the aircraft system shall be no greater than:___.

SECTION 2

CHAPTER 9

FLIGHT CONTROL SYSTEMS AND AIRCRAFT DYNAMICS

INTRODUCTION

1. DEF STAN 00-970 adequately addresses certification requirements for flight control systems and aircraft dynamics. This chapter provides guidance on alternate standards to DEF STAN 00-970, which could be used as a basis for certification.

2. Specialist advice on flight dynamics is provided for ADF aircraft within ARDU Aerospace Systems Engineering (ASE) Squadron by a Senior Design Engineer (SDE) established to specialise in flight dynamics. This position is responsive to both CO ASE SQN and DGTA. As DGTA's representative the incumbent provides specialist advice to support TAR and TAA Recommendations and assess the adequacy of associated design standards.

GENERAL INFORMATION

3. A primary objective of a Flight Control System (FCS) is to enable the effective and efficient manoeuvre of an aircraft. The ease by which an aircraft may be manoeuvred and held in a determined flight path is referred to as the aircraft's Flying and Handling Qualities (FHQs). Accordingly, the analysis of FHQs is an inseparable part of FCS design. This chapter provides guidance on the major FCS and FHQ specifications and standards which are likely to have been applied in the design and development of most weapon systems.

4. Flight control systems can be classified as either manual (MFCS or simply FCS) or automatic (AFCS). Manual systems consist of mechanical, hydraulic and electric/electronic components which transmit pilot control commands, or generate and convey commands which augment pilot control commands. Automatic systems contain the same components as manual systems, yet generate and transmit automatic control commands which provide pilot assistance through automatic or semi-automatic flight path control. The distinction between the two systems lies in the ability of automatic systems to control the aircraft flight path without reference to pilot commands. An example of an AFCS is an aircraft autopilot system.

5. An aircraft's dynamic performance depends heavily on the aerodynamic, weight/inertia, thrust and control characteristics of the aircraft. Accordingly, an aircraft's FHQs will vary significantly with aircraft type and flight phase/condition. As such, handling qualities requirements are usually defined in terms of the Class of aircraft, Flight Phase Category, and the Flying Qualities Level required to provide the necessary aircraft operational performance. Flying and handling qualities will normally be expressed in terms of both Longitudinal and Lateral-Directional requirements.

FLIGHT CONTROL SYSTEM DESIGN STANDARDS

6. The scope for the ADF to significantly alter/drive the design of an aircraft's FCS and hence its FHQs is extremely limited; however, given the criticality of the system in terms of both aircraft safety and performance, it is imperative to establish the baseline standard/specification to which the system was designed.

7. FCS will vary in nature, complexity and operation given the type of aircraft, its intended operational role, and the required level of performance. For example, a transport aircraft may employ a relatively simple mechanical FCS design, whereas a combat aircraft may require use of a complex Full Authority Fly-by-Wire (FBW) FCS in order to achieve enhanced manoeuvrability and performance. Accordingly FCS functionality and performance requirements must be clearly defined which are consistent with the operational role of the aircraft and the required level of performance (handling qualities).

8. The major military and civil (ICAO compliant) design standards/specifications encountered in FCS design vary quite significantly in content and emphasis. The civil design standards present the minimum requirements necessary to ensure airworthiness, or safety; FARs are quite general and usually allow flexibility in the design and verification methodology. DEF STAN 00-970 also presents the basic minimum airworthiness design considerations that UK experience has shown necessary and is based primarily around functional requirements. The US DOD

military specification MIL-F-9490D, by comparison, concentrates on all conceivable aspects of FCS performance, integrity and component construction, and is quite rigorous in relation to design methodology.

MIL-F-9490D - Design, Installation and Test of Piloted Aircraft Flight Control Systems

9. MIL-F-9490D specifies USAF FCS design requirements for piloted aircraft and serves as a comprehensive and rigorous guide to all aspects of FCS design and verification, which has direct applicability to all categories of fixed and rotor wing aircraft, civil or military. Both manual and automatic FCS design requirements are addressed. Requirements are defined in relation to FCS Operational State and Criticality Classifications. Operational states classify levels of degradation in FCS performance and subsequent degradation in FHQs (in relation to MIL-F-8785C Flying Qualities Level), and range from Operational State I (full normal operation) to Operational State V (controllable to an evacuable flight condition).

10. The FCS (manual) performance requirement simply states compliance with the flying qualities requirements of MIL-F-8785C or MIL-F-83300 (RW). Specific performance parameters for the usual range of AFCS functions (attitude/altitude/heading/Mach/Airspeed hold, automatic navigation/instrument approach etc) are defined and reference MIL-F-8785C where applicable. Provision for Flight Load Alleviation, Active Flutter Suppression and Gust/Manoeuvre Load Alleviation systems is included with reference to appropriate US DoD military specifications. Performance requirements for Automatic Terrain Following (ATF) are not specified.

11. General design requirements adequately address failure immunity (including ATF), system operation/interface, trim, stability margins and sensitivity, operation in turbulence, and system built-in-test/monitoring. Determination of system redundancy levels is left to the designer to determine based on meeting the reliability, failure immunity and invulnerability requirements of the procurement specification.

12. Manual FCS design requirements primarily address augmentation systems, specifically failure of gain scheduling systems and requirements for reversion to a backup mode. AFCS design requirements primarily address system interface and emergency override/disengagement requirements. Flight safety, invulnerability and maintenance provision requirements are all adequately addressed. Structural integrity, including strength, stiffness and durability requirements for FCS components and supporting structures are specified, with reference to MIL-A-8870C for aero-elasticity considerations.

13. Extensive design requirements relating to pilot controls and displays, electrical/mechanical signal transmission and computation, electrical/mechanical/pneumatic control power, actuation, and component design/fabrication/ installation are specified. In most cases, other US DoD military standards and specifications are referenced.

DEF STAN 00-970 Design and Airworthiness Requirements for Service Aircraft

14. FCS design requirements are dispersed throughout DEF STAN 00-970 as either specific FCS design requirements or generic component/system design requirements. DEF STAN 00-970 uses the terminology of ‘inceptor’ for input elements of the FCS directly moved by the pilot and ‘motivator’ for output elements. Furthermore, the FCS is divided into the Primary and Secondary FCS. The Primary FCS refers to the main flying controls (ie pitch, roll and yaw inceptor), the corresponding motivators, and the intervening linkages and devices, including augmentation systems. The Secondary FCS includes the trim system and all control devices which alter the configuration of the aircraft
(eg flaps, slats, speed brakes).

15. The main areas within the standard which directly relate to FCS design are Chapters 206 Control Systems, 208 Active Control Systems, 604 Flight Control Systems, and their associated Leaflets. The requirements within these chapters are similar to the corresponding areas of MIL-F-9490D but are more functionally orientated, with greater design scope being given to the designer. Greater guidance than MIL-F-9490D is provided in relation to augmentation system design, particularly requirements relating to control law and software design/development. FCS performance (FHQs) requirements are specified in Part 6 Chapters 600 to 606, which are similar in content to MIL-F-8785C. Aero-elasticity requirements are provided in Chapter 500 Aero-elasticity. Requirements relating to autopilot design are provided in Chapter 729 Design and Performance of Autopilot and Flight Director Installations.

16. As with MIL-F-9490D, failure immunity and invulnerability requirements for FCSs are adequately addressed; however, system reliability and redundancy requirements must be specified by the procurement agency. Accordingly, information detailing system reliability and redundancy should be sought.

17. ***MIL-F-18372 – Mechanical FCS Design.*** MIL-F-18372 is a reasonably old (1955) US Navy Specification; however, it is still applicable in relation to design of simple manual FCSs eg mechanical, power boosted, or power operated systems.

18. ***FAR/JAR Airworthiness Standards.*** FARs and JARs are not as extensive or comprehensive as the US DoD or UK MoD specifications and standards. The operational role of the aircraft must be considered in order to identify additional requirements that would normally only apply to military aircraft.

FLYING AND HANDLING QUALITIES STANDARDS

19. A vast amount of research has been conducted into the flying and handling qualities of aircraft over the past fifty years. Since the majority of this research has been conducted in relation to military (primarily fighter) aircraft for the US DoD, it is hardly surprising that the results of this work has culminated in the form of US DoD military specifications and standards. MIL-F-8785C and MIL-STD-1797A represent comprehensive and authoritative sources for FHQ requirements for fixed wing aircraft.

20. ***Military Specification, MIL-F-8785C Flying Qualities of Piloted Airplanes.*** MIL-F-8785C specifies flying and handling qualities requirements which are applicable to all classes of fixed wing aircraft. Requirements are divided into Longitudinal and Lateral-Directional requirements and defined in terms of the Class of aircraft, Flight Phase Category, and the Flying Qualities Level required. Although the limits placed on the stability mode parameters are based on conventional or low order aircraft response characteristics, application to Highly Augmented Aircraft (HAA) is achieved through the use of equivalent system matching. Given its simple application and applicability to all aircraft, MIL-F-8785C can be specified for any aircraft acquisition; although for HAA aircraft, the accuracy of the LOES match should be verified.

21. ***Military Standard, MIL-STD-1797A Flying Qualities of Piloted Aircraft.*** MIL-STD-1797A is a relatively new standard and is written in the new 'requirements'/'handbook' format. This new format requires the contracting authority to complete the requirements based on guidance provided in the associated handbook, which essentially represents the development, extension and elaboration on the existing MIL-F-8785C (Note that MIL-F-8785C is still current, with all requirements and terminology having been carried over into the new MIL-STD-1797A). Specifically, the handbook provides requirement and verification rationale, guidance and lessons learnt based on over fifty years experience to assist in defining requirements relevant to the specific Class of aircraft. Commentaries on the relative merits of certain designs are also provided.

22. The majority of data contained within MIL-F-8785C is retained within the MIL-STD-1797A Handbook; however, the data is presented in terms of response axes (as opposed to response modes) to better accommodate HAA. The lack of application to HAA was identified as one of the major weaknesses of MIL-F-8785C, so in this respect, the MIL Handbook includes/recommends criteria specifically applicable to this form of aircraft. Accordingly, for complex FBW FCS designs, information should be sought from the Contractor as to the extent to which the guidance provided in the MIL-STD-1797A Handbook has been considered.

23. ***DEF STAN 00-970 Design and Airworthiness Requirements for Service Aircraft.*** The FHQs requirements of DEF STAN 00-970 Volume 1 Part 6 are similar to MIL-F-8785C, however, not all aspects of FHQs are addressed.

24. ***FAR/JAR Airworthiness Standards.*** These regulations tend to be less specific in their requirements; for example, electing to specify that the stability modes be positively damped rather than assigning specific limits. For military aircraft where specific performance (FHQs) is required for operational effectiveness, more stringent requirements may be needed.

GENERAL REQUIREMENTS

25. Contractors should identify all documentation applicable to the development and assessment of the aircraft's FHQs and indicate whether Commonwealth access to the documentation would be made available if required. Contractors should provide details of the aerodynamic and stability derivative data and/or flight dynamic model available for the aircraft and indicate how this data was derived. Contractors should identify the cost associated with obtaining this data as a Contract deliverable.

Blank Page

SECTION 2

CHAPTER 10

AIRCRAFT MECHANICAL SYSTEMS

INTRODUCTION

1. This chapter provides ADF-specific aircraft mechanical systems requirements to supplement common civil and military standards. The following mechanical systems are addressed in this chapter: undercarriage systems; wheels, tyres, brakes and anti-skid systems; fuel systems; air-to-air refuelling systems; pneumatic systems; hydraulic systems; fire detection and extinguishing systems; and other airframe related systems.

2. This chapter is still under development. In its current form, the chapter provides the following:

a. additional TAR requirements to be applied, and

b. a summary of current mechanical system standards for general reference.

TAR DESIGN REQUIREMENTS

3. Annex A provides additional aircraft mechanical systems functional requirements, which are considered highly desirable to the ADF. The TAR design requirements of annex A are to be considered in addition to the requirements contained within the applicable design standard.

GENERAL REFERENCE SPECIFICATIONS AND STANDARDS

4. Evaluation of all applicable mechanical system standards for ADF use is still outstanding. Until this is complete, this chapter includes general information on standards that have been determined acceptable in the past for various ADF applications.

5. This chapter is focussed on Military Standards and documents, however, within the FAA and EASA systems, other acceptable standards that are applicable to these mechanical systems exist. There are also relevant standards for interoperability and occupational health and safety not detailed in this chapter. The Air and Space Interoperability Council (ASIC), previously known as the Air Standardisation Coordinating Committee (ASCC), is an example. Some ASCC standards are called out by annex A. Annex B provides guidance on locating the specifications and standards listed in this chapter.

6. ***JSSG 2009, Joint Services Specification Guide- Air Vehicle Sub-systems.*** This modern DoD document provides current design guidance in developing project unique specifications. JSSG-2009 contains a compilation of references, generically stated requirements, verification criteria, tailoring guidance and background information on Air Vehicle sub-systems. Appendixes contained in the JSSG-2009 cover the following sub-systems: landing gear; hydraulics; environmental control systems; fuel; fire and explosion hazard protection; mechanical; doors, hatches and ramps; airframe bearings; fasteners; actuators; cargo, aerial delivery and special operations; and pneumatics. It is recommended that project offices also consult this standard when developing specifications for mechanical systems as it provides a wealth of information from the US DoD.

Undercarriage Systems

7. ***Military Specifications.*** A previous undercarriage specification, MIL-L-87139 Landing Gear Systems, has been cancelled. The alternative, an Air Force Guide Specification AFGS-87139A has been superseded by JSSG-2009.

8. ***SAE ARP 1311, Aircraft Landing Gear.*** SAE ARP 1311 provides information to aid in the certification of undercarriage systems in civilian aircraft. It captures many of the lessons learnt by the aerospace industry in the design of undercarriage systems. Other SAE standards that could be of assistance are; SAE AIR 4566-92 Crashworthy Landing Gear Design, SAE ARP 1598-85 Landing Gear System Development Plan, and SAE AIR 4243-88 Landing Area/Landing Gear Compatibility.

9. Further guidance for in-service modification of landing gear may be obtained from the individual chapters of DEF STAN 00-970, or any of the following standards: MIL-A-8863C Airplane Strength and Rigidity Ground Loads for Navy Acquired Airplanes; MIL-A-18717C Arresting Hook Installation, Aircraft; and MIL-STD-805B Towing Fittings and Provisions for Military Aircraft, Design Requirements for. MIL-T-6053C Tests, Impact, Shock Absorber Landing Gear, Aircraft is now inactive, but may be used for existing systems designed to this specification.

Wheels, Tyres, Brakes and Anti-Skid Systems

10. ***MIL-W-5013L, Wheel and Brake Assemblies, Aircraft General Specification for.*** MIL-W-5013L is now inactive, but covers main and auxiliary wheel and brake assemblies for all types of military aircraft. However, the specification treats the brake as an assembly, rather than separating the brake down into the required components necessary to form a system. The intent of the specification is to ensure that the wheel assembly and the brake assembly are complimentary.

11. ***MIL-B-8584C, Brake Systems, Wheel, Aircraft Design of.*** MIL-B-8584C covers the brake system design requirements for aircraft equipped with wheel-type landing gear. MIL-B-8584C classifies brake systems as either hydraulic or pneumatic; manually operated, power operated, and manual-power operated, further dividing these into five types:

a. Type I – Manual pressure generating. The control unit generates pressure by manual actuation.

b. Type II – Power pressure generating. The control unit meters pressure from a power generating system.

c. Type III – Manual power pressure generating. Pressure is manually generated in a slave control unit, which in turn operates the main control unit, which meters fluid from a pressure generating system.

d. Type IV – Power-boosted manual pressure generating. The control unit generates pressure by manual actuation and in addition, the manually generated pressure is boosted by pressure from a power generating system.

e. Type V – Power brake valve with emergency master cylinder. One part of the control unit meters pressure from a power generating system, and another part of the control unit serves as a stand-by manual pressure generating unit when the power system is inoperative.

12. Of note is the requirement for aircraft that use Type II or III systems to be fitted with an emergency brake system.

13. ***MIL-B-8075D, Brake Control Systems, Anti-skid, Aircraft Wheels, General Specification for.*** MIL-B-8075D covers the requirements for aircraft anti-skid brake control systems and their components.

14. ***MIL-T-5041H, Tyres, Pneumatic, Aircraft.*** MIL-T-5041H covers the requirements for aircraft pneumatic tube type and tubeless tyres.

15. ***SAE ARP/AIR.*** SAE ARP/AIR documents provide a great deal of information to assist with in-service modifications. Those of particular interest are: ARP 1493 Wheel and Brake Design and Test for Military Aircraft; ARP 1070 Design and Testing of Anti-Skid Brake Control Systems for Total Aircraft Compatibility; AIR 1064 Brake Dynamics, and; ARP 1619 Replacement and Modified Wheels. They capture many of the lessons learnt by the aerospace industry in the design of Wheels, Tyres, Brakes or Anti-Skid systems, and identify alternative ways of meeting FAR/JAR requirements. ARP 862 Skid Control Performance has been cancelled, but may be of interest for background information.

16. ***SAE ARP 4102/2 and ARP 1907.*** ARP 4102/2 Automatic Braking Systems and ARP 1907 Automatic Braking Systems Requirements, while not common on military aircraft, may become so in the future. An automatic braking system (ABS) is described as a pilot-selectable feature that automatically applies a preselected brake pressure for rejected take-off braking or landing braking without a pilot pedal input. This system senses throttle cut or touch down of the aircraft for activation purposes, but does not override anti-skid systems. ARP 1907 describes the way this system works providing lessons learnt and some offsets to the benefits provided by the ABS. All the above SAE standards give valuable guidance for use in modifying existing systems or for designing future systems.

Fuel Systems

17. ***MIL-F-17874B, Fuel Systems, Aircraft, Installation and Test of.*** MIL-F-17874B covers the general requirements for functional operation, installation, and testing of fuel systems for all piloted aircraft, target drones and guided missiles.

Air-to-Air Refuelling (AAR) Systems

18. ***ASCC Air Standard (AIR STD) 25/13A In Flight [Aerial] Refuelling Equipment, Dimensions and Functional Characteristics.*** ASCC AIR STD 25/13A aims to facilitate in-flight refuelling between the ASIC nations by standardising the mating dimensions of the reception coupling and nozzle, the nozzle clearance envelope and the maximum refuelling pressure.

19. ***MIL-A-19736A, Air Refuelling Systems, General Specifications for.*** MIL-A-19736A covers the general requirements for design, installation and test of probe and drogue air refuelling systems for fixed wing aircraft. The requirements of MIL-A-19736A are in accordance with those of ASCC AIR STD 25/13A.

20. ***MIL-C-81975, Coupling, Regulated, Aerial Pressure Refuelling Type MA-3.*** The specification defines the requirements for an aerial refuelling coupling, Type MA-3, utilising an internal pressure regulator and surge suppression device. This coupling is compatible with type MA-2 probe and drogue refuelling systems. The requirements of MIL-C-81975 are in accordance with those of ASCC AIR STD 25/13A. The RAAF B707 AAR system uses a MA-3 type drogue coupling, as per MIL-C-81975. Hence, in order for receiver aircraft to utilise the B707 AAR system, receiver aircraft must use a probe compatible with the MA-3 or MA-2 type drogue coupling. The replacement AAR aircraft, the A330-200 will use an MA-4 type drogue coupling.

21. ***MIL-A-87166, Aerial Refuelling Receiver Subsystems.*** MIL-A-87166 is now cancelled. It was not applicable to the RAAF B707 AAR system, which utilises the probe and drogue AAR system as specified above. However, this standard was applicable to the USAF boom and receptacle style AAR refuelling system, which is used on RAAF F-111 aircraft. The JSSG-2009 Appendix F provides guidance on the latest requirements.

22. ***Aerial Refuelling Systems Advisory Group (ARSAG) Document No. 00-03-01.*** ARSAG Document No. 00-03-01 provides useful guidance on aerial refuelling pressure definitions and terms. Information on such things as typical limit and ultimate pressures for tankers and receivers is contained in this document.

Pneumatic Systems

23. ***MIL-P-5518D, Pneumatic Systems, Aircraft, Design and Installation, General Requirements for.*** MIL-P-5518D is now inactive, but provides specifies requirements for the design and installation of aircraft pneumatic systems. The specification divides pneumatic systems into types and classes. Types are classified by the charging system and fluid operating temperature. Type A is an airborne compressor charged system while Type B is a ground charged system. Type I systems have a maximum fluid operating temperature of $+160^{o}$ F and Type II systems have a maximum operating temperature of $+275^{o}$ F. Classes are classified by the operating pressure, ie Class 1500 has a supply pressure of 1500 psi, Class 3000 is 3000 psi, Class 4000 is 4000 psi and Class 5000 is 5000 psi.

Hydraulic Systems

24. ***MIL-H-5440H, Hydraulic Systems, Aircraft, Design and Installation Requirements for.*** MIL-H-5440H has been superseded and replaced by SAE AS 5440. This specification documents the design and installation requirements for Type I and Type II hydraulic systems. Type I systems are those with a maximum operating temperature of +160° F, while Type II systems have a maximum operating temperature of +275° F. Hydraulic systems have been further divided into classes, namely Class 1500 psi, Class 3000 psi, Class 4000 psi, Class 5000 psi, and Class 8000 psi. MIL-H-5440H allows the use of hydraulic fluid conforming to either MIL-H-83282 or MIL-H-5606/MIL-PRF-5606. The ADF prefers the use of MIL-H-83282 hydraulic fluid. MIL-H-5606 is an older and lower temperature rated hydraulic fluid that is gradually being phased out by ADF and overseas operators.

25. ***MIL-H-8891A, Hydraulic Systems, Manned Flight Vehicles, Type III, Design, Installation and Data Requirements for, General Specification for.*** MIL-H-8891A, now inactive, is similar to MIL-H-5440H, and can be considered a refinement of MIL-H-5440H to cover Type III systems. Type III systems are those with maximum operating temperatures of +390° F. These systems are further divided into 2 classes; Class 3000 psi where the cut out

pressure at the main pressure controlling device is 3000 psi, and Class 4000 psi where the cut out pressure at the main pressure controlling device is 4000 psi.

26. ***SAE ARP 4752 – Aerospace – Design and Installation of Commercial Transport Aircraft Hydraulic Systems.*** ARP 4752 examines each FAR/JAR requirement in detail and provides a wealth of information on good design practices for hydraulic systems. It also captures many of the lessons learnt by the aerospace industry in the design of hydraulic systems, and identifies alternative ways of meeting FAR requirements. ARP 4752 is a particularly good source of information for in-service engineering activities in the modification of hydraulic systems.

Environmental Control Systems

27. Environmental Control Systems (ECS) information can be found in Section 2, Chapter 21 of this publication.

Fire Detection and Extinguishing Systems

28. ***MIL-E-22285 (WEP), Extinguishing System, Fire, Aircraft, High-Rate-Discharge Type, Installation and Test of.*** MIL-E-22285 is now inactive, but covers the installation of high rate discharge type, fixed fire extinguishing systems for engine spaces and other potential fire zones in aircraft.

29. ***MIL-F-87168, Fire and Explosion Hazard Protection Systems, Aircraft, General Specification for.*** MIL-F-87168 establishes the performance, compatibility and verification requirements necessary for fire and explosion hazard protection provided on aircraft. This specification is unsuitable for use in projects that will purchase an aircraft already fitted with a fire and explosion hazard protection system. It is primarily for specifying the requirements for an as yet to be developed system design. The specification requires supplemental information, relating to the performance requirements of fire and explosion hazard protection systems on aircraft, to be inserted by the project authority.

30. ***SAE AIR 1076, Aircraft Fire Protection for Reciprocating and Gas Turbine Engine Installations.*** SAE AIR 1076 provides detailed information for the certification of aircraft fire detection and extinguishing systems in civilian aircraft. It captures many of the lessons learnt by the aerospace industry in the design of aircraft fire detection and extinguishing systems, and identifies alternative ways of meeting FAR requirements.

Aerial Delivery System

31. **DEF(AUST) 9009** ***Air Transport by Fixed Wing and Rotary Wing Aircraft, Design and Restraint of Equipment.*** DEF(AUST) 9009 covers the design requirements for equipment required to be air transported either internally by fixed wing or rotary wind aircraft, or externally from rotary wind aircraft.

32. **DEF(AUST) 9010** ***Cargo Air Drop – Design Requirements for Load Development and Aerial Delivery Equipment***. DEF(AUST) 9010 details the requirements for the airdrop of load items.

Annexes:

A. Mechanical Systems Design Requirements

B. Guidance for Location of Specifications and Standards

MECHANICAL SYSTEMS DESIGN REQUIREMENTS

Undercarriage Systems

1. The aircraft undercarriage shall be capable of withstanding the loads and conditions that can be expected to be experienced during operation from the types of runways detailed in the Statement of Operating Intent (SOI).

Wheel, Tyres, Brakes and Braking Systems

2. The wheels, tyres, brakes, braking systems and anti-skid systems shall be capable of withstanding the loads and conditions that can be expected to be expereinced during operation in accordance with the Statement of Operating Intent (SOI).

3. Tyre valve couplings shall comply with ASCC AIR STD 25/8.

Fuel System

4. The pressure fuelling replenishment connection shall conform to ASCC AIR STD 25/17B.

In-flight Refuelling Systems

5. For aircraft to be fitted or retrofitted with in-flight refuelling systems, it will be necessary to carry out an assessment of the existing aircraft systems, which will be affected by the tanker/receiver conversion in order to determine their suitability for integration with the proposed in-flight refuelling systems.

6. RAAF B707 AAR systems require the receiver aircraft to have a probe attachment compatible with the MA-3 type drogue coupling, as per MIL-C-81975.

7. If the tendered AAR system for the receiver aircraft uses the USAF boom and receptacle style AAR system, then the tendered system shall have a demonstrated level of safety, design and construction equivalent to that provided by JSSG-2009 appendix F.

Pneumatic Systems

8. Air supply and testing connections shall comply with ASCC AIR STD 25/15C. This standard includes air-conditioning connections, cabin pressurising connections, canopy seal inflation connections and test pressure gauge connections.

9. For pneumatic systems using gaseous air/nitrogen,the gaseous air/nitrogen replenishment connections shall comply with ASCC AIR STD 25/35A.

Hydraulic System

10. The aircraft shall use MIL-PRF-83282 [H-537, OX-19] hydraulic fluid in its hydraulic system. JFLA POLENG(Air) shall be consulted should a hydraulic fluid other than H-537 be intended for use.

Environmental Control Systems

11. Additional requirements for military derivatives of civilian aircraft relating to ECS can be found in Section 2, Chapter 21 of this publication.

Fire Detection and Extinguishing Systems

12. FAR requirements for fire detection and extinguishing are adequate for military derivatives of civil aircraft. If pyrotechnics, chaff systems, cartridge activated devices etc, are to be fitted as part of the project, then application of DEF STAN 00-970 Part 1, Sect 4, Paragraph 4.26.65 – 4.26.68 may be required.

View and Clear Vision Requirements

13. Windscreens and transparencies of a military derivative of a civilian aircraft will generally have been designed and certificated to the listed civil requirements, which will be similar to the military requirements in principle. If the Project Office considers the windscreens/transparencies design and construction to be critical to the aircraft's intended role, a compliance assessment of the existing aircraft in relation to the requirements DEF STAN 00-970, Part 1, Sect 4, Paragraph 4.17 is recommended. View and vision requirements that are related to ECS functions can be found in Section 2, Chapter 21 of this publication.

Seating

14. Seats designed exclusively for paratrooping, do not meet FAR or DEF STAN 00-970 requirements for passenger seating. Accordingly, seating designed for paratrooping shall not be approved as passenger seating.

15. There is no FAR requirement for troop seating. Should an aircraft certified for passenger seating be required for troop seating, it shall comply with the requirements of DEF STAN 00-970. Note that until DEF STAN Issue 3, Part 5 – *Large Civel Type Aircraft* is published, Project Offices should refer to DEF STAN 00-970, Issue 1, AL 14 for troop seating requirements. In addition to the DEF STAN 00-970 requirements, available space and stowage considerations will need to be taken into account.

Picketing

16. Provision shall be made for the aircraft to be picketed. DEF STAN 00-970, Part 1, Sect 3, Paragraph 3.12.4 states that the aircraft shall be capable of safely withstanding wind speeds of up to 148 km/h (80 kts) horizontally from any direction. Additional requirements exist for picketing on board ships. FAR 25 specifies a wind speed of 65 kts, horizontally. The Project Office may wish to specify a different wind speed based on the intended operating environment.

17. DEF STAN 00-970, Part 1, Sect 3, Paragraph 3.12.6 states that all flying control systems shall be safeguarded against damage in wind speeds up to 148 km/h (80 kts) by locks built into the aircraft or by irreversibility of the control operating mechanism. The Project Office may wish to specify a different criterion based on the intended operating environment.

Gravity Filling Orifices

18. All gravity filling orifices shall comply with ASCC AIR STD 25/11B.

GUIDANCE FOR LOCATION OF SPECIFICATIONS AND STANDARDS

DEF STAN 00-970

1. The Commercial Standards Search Engines located at the Aerospace Technical Standards Document Centre (ATSDC) Intranet website: http://wilap006.sor.defence.gov.au/specs/ provide an appropriate means for locating DEF STAN 00-970 in .pdf format. From the ATSDC website click on the 'Commercial Standards' link in the Main Menu. Then use the 'DSTAN' search engine to locate DEF STAN 00-970.

JSSG 2009

2. To obtain the most recent version of JSSG 2009, proceed to the 'Order Form' link on the ATSDC Intranet website. Follow the instructions to obtain a login and place an order.

Military Specifications

3. Most of the Military Specifications contained in this chapter can be located through the 'Assist Quick Search' search engine on the ATSDC Intranet website. However if a particular Specification or Standard cannot be located, then an order should be placed as per paragraph 2.

Society of Automotive Engineers

4. Information on the current status of Society of Automotive Engineers (SAE) Aerospace Recommended Practices (ARPs) or Aerospace Information Reports (AIRs) can be found by following the links on the SAE International website: http://www.sae.org/servlets/index Copies of any required SAE documents can be obtained by placing an order on the ATSDC website.

Aerial Refuelling Systems Advisory Group (ARSAG) Document No. 00-03-01

5. The latest version of ARSAG Document No. 00-03-01 can be found on the ARSAG website: http://www.arsaginc.com/index.htm by clicking on the link entitled 'Pressures and Defs'.

Aerial Delivery System Publications

6. DEF(AUST) 9009 *Air Transport by Fixed Wing and Rotary Wing Aircraft, Design and Restraint of Equipment* and DEF(AUST) 9010 Cargo Air Drop – *Design Requirements for Load Development and Aerial Delivery Equipment* can be located through the ATSDC Intranet website by following the links to Australian Defence Standards.

Air Standardisation Coordinating Committee (ASCC) Standards

7. The Air and Space Interoperability Council, (ASIC) previously known as Air Standardisation Coordinating Committee (ASCC)) is an active and productive international organisation that works for the air forces of Australia, Canada, New Zealand, the United Kingdom and the United States of America. Its principal objective is to ensure member nations are able to partake in joint and combined operations.

8. The ASIC objectives are achieved by the standardisation of doctrine, operational procedures, material and equipment. The current status of ASCC standards can be determined through the ASIC website: http://www.airstandards.com/ and clicking on the 'Documents' link. Copies of the ASCC standards can be located through the ATSDC website by clicking on the 'Australian Defence' Standards link.

Blank Page

SECTION 2

CHAPTER 11

AIRCRAFT STRUCTURAL INTEGRITY

INTRODUCTION

1. Effective and efficient management of structural airworthiness is essential to enable air operations to be conducted within an acceptable level of risk of structural failure and to preserve the asset to its Planned Withdrawal Date (PWD) without unforecast aircraft retirements. Safety of flight must be sustained while minimising life cycle costs and maintaining aircraft availability.

2. DI(AF) LOG 2-109 recognises that aircraft procured by the ADF are designed and certified to standards such as UK and US military standards and specifications, and civil FARs and JARs. The ADF accepts a range of structural design standards for type certification and continuing airworthiness. Preferred comparative standards and guides are used to supplement existing standards to assure safe and effective service. Comparative aircraft structural integrity standards include DEF STAN 00-970, FAR25 and FAR29, and comparative guides include MIL-HDBK-1530B and JSSG-2006. The Certification Structural Design Standard (CSDSTD) defines the primary standard and supplementary standard(s) against which an aircraft is certified for operation under ADF airworthiness control.

3. This chapter provides guidance on the application of structural airworthiness design standards within the ADF type certification program. Structural integrity design and verification requirements in the acquisition of both new and used aircraft are discussed. Relevant military and civil standards, as well as specific ADF requirements, are also considered.

APPLICATION AND TAILORING GUIDANCE

General

4. Whether acquiring new or used aircraft, carrying out structural modifications, making changes to operational roles or simply managing normal operations, the management of the aircraft's structural integrity must be guided by a program that ensures all relevant airworthiness issues are considered.

5. Aircraft are designed to approved airworthiness standards that set the requirements needed to provide an acceptable degree of safety by designing to an acceptably low risk of failure. These standards recognise that aircraft structures, including helicopter dynamic components, deteriorate throughout their service lives as a result of fatigue damage, environmentally induced degradation, stress corrosion cracking, accidental or battle damage and even the effects and interaction of repairs. The design process, whether for a new acquisition or for the modification of an existing aircraft, should seek to minimise accumulation of fatigue damage and environmental degradation during an aircraft's service life and provide an acceptable level of residual strength following accidental damage or unexpected failures. During design development, some compromise is usually required between reduced levels of stress and enhanced performance goals. There is also a well-established tendency for weight growth between design and production, and during an aircraft's service life, with a consequent increase in structural loading. It follows that the condition of structural and dynamic components and the actual usage of each aircraft must be closely monitored to verify the achievement of required standards of structural integrity.

6. The purpose of this chapter is to:

a. describe the ADF Aircraft Structural Integrity Program (ASIP), including a historical perspective;

b. provide guidance on various design standards including DEF STAN 00-970, US Military Specifications and Guides, and Civil Regulations (FARs, BCARs and JARs);

c. provide guidance on the application of ASIP to used aircraft; and

d. provide guidance on ASI management and engineering requirements for weapon system acquisitions and weapon system Through Life Support (TLS) contracts.

Scope

7. This chapter is applicable as follows:

a. ***Type of Aircraft.*** This chapter is directly applicable to piloted fixed and rotary wing aircraft.

b. ***Type of Structure.*** This chapter applies to all metallic and non-metallic structure and dynamic components unless stated otherwise. Gearbox systems, power generation and engine structures (excluding mounts) are not covered.

c. ***Organisations.*** This chapter applies to Acquisition Project Offices (POs), System Project Offices (SPOs), Authorised Engineering Organisations (AEOs), Logistics Management and TLS contracts, and Defence contractors involved in aircraft structure design activities.

Definitions

8. The definitions that are generally applied to the ASI management of ADF aircraft are listed in Annex A. Given that the ADF operates aircraft that are usually certified and operated by other organisations, adopting definitions that are common to a particular aircraft type may be appropriate. Accordingly, where variation of a definition in Annex A is considered appropriate for a particular aircraft, the Aircraft Structural Integrity Management Plan (ASIMP) is to include the relevant definition and source.

Policy

9. DI(AF) LOG 2-109 defines the objectives, outcomes, strategies and mandatory requirements of ASI management, and assigns responsibilities. AAP 7001.053(AM1) (Technical Airworthiness Management Manual, TAMM), lists the regulations for AEOs for structural integrity management in the ADF and provides guidance on the application of the regulations.

10. This chapter provides guidance on the standards pertaining to airworthiness in the design of structures with an emphasis on issues that must be examined during the acquisition of both new and used aircraft. The objective of ADF ASI management is to achieve the following outcomes:

a. constrain the risk of structural failure of an aircraft to an acceptable level,

b. achieve planned rates of aircraft availability,

c. avoid unforecast cost of refurbishment and/or replacement, and

d. achieve the PWD.

11. The basis for achieving these outcomes is good design, adequate verification and effective management.

12. DI(AF) LOG 2-109 requires projects to comply with ASI requirements through the provision of resources for structural integrity management in project allocations, as required by DGTA.

STRUCTURAL INTEGRITY MANAGEMENT PHILOSOPHY

Background

13. ***Military Airworthiness Authorities.*** Aircraft structural integrity management programs were initiated around the same time in both the USA and the UK in response to fatigue failures of various aircraft. During 1958 in the USA, the Aircraft Structural Integrity Program was established after fatigue failures of wing structure in B-47 aircraft. During the 1950s, the UK established a structural integrity policy in the wake of the Comet disasters resulting from fuselage fatigue. These structural integrity management policies were based upon the fact that repeated loads within the flight envelope could pose a threat to safety of flight due to fatigue. It was known that the time for fatigue damage to cause failure was subject to variability that needed to be allowed for in setting service lives of primary structural components. At that time both countries established structural integrity requirements based upon safe life and many

aircraft flying today were designed on that basis. Typically a safe life was established by conducting a fatigue test to a design spectrum on either a complete structure or major components and applying an appropriate factor to the test life to failure. This factor was referred to as the 'scatter factor' to allow for fatigue life variability. The most important research in establishing an appropriate value for the scatter in fatigue life of complete structures was carried out at the Defence Science and Technology Organisation (DSTO) using wings from Mustang fighter aircraft.

14. During the 1960s in the USA, it became evident that the original ASIP philosophy based on safe life was inadequate for structural components made from new high-strength D6ac steel, because it did not account for fatigue cracking arising from damage in the structure from manufacturing processes or from in-service maintenance of the aircraft. In 1969 the failure of an F-111 wing pivot fitting at only 100 flight hours on an aircraft type qualified to 4,000 hours led the USAF to adopt a damage tolerance approach. The USAF ASIP now reflects both durability and damage tolerance philosophies.

15. Adequate durability ensures the airframe will have an economic life greater than the design service life and consequently low in-service maintenance costs. Adequate durability is an economic criterion. Adequate damage tolerance ensures the structural safety of the airframe in the presence of undetected flaws or damage in critical structure. Adequate damage tolerance is a safety criterion.

16. The damage tolerance ASIP approach was applied to the design and modification of several aircraft and was formally established in MIL-STD-1530A(1) dated 26 February 1988, which has been superseded by MIL-HDBK-1530B. The USAF damage tolerance requirements are defined in JSSG-2006 (superseding AFGS-87221A dated 8 June 1990, superseding MIL-A-87221 dated 28 February 1985), which replaced MIL-A-83444 and provides guidance on the application of durability and damage tolerance requirements to aircraft structures.

17. The UK structural integrity philosophy, while still based on a safe life approach, includes inspection dependent locations, aircraft usage monitoring and operational loads monitoring. The UK design standard, DEF STAN 00-970 Issue 2, contains a comprehensive set of Design and Airworthiness Requirements for Service Aircraft. The requirements most directly related to structural integrity of fixed wing aircraft (combat aircraft) are located in Part 1, Section 3 (Structure) and Part 1, Section 4 (Design and Construction). The extant requirements for rotorcraft are located in Volume 2, Issue 1. A separate and updated section in DEF STAN 00-970 (designated as Part 7) for rotorcraft is to be published in the future. Similarly, sections for small and large civil type aircraft used in a military role (designated as Parts 3 and 5 respectively) are to be published in the future.

18. ***Civil Airworthiness Authorities.*** Large transport aircraft are typically designed with redundant load-path structural components to satisfy fail-safe requirements of civil regulatory authorities. In the 1970s, airworthiness authorities around the world (especially those of Australia and the UK) questioned the proposition that the fatigue and fail-safe requirements in force at the time justified indefinite operation of aircraft. The matter was brought to a head by the loss of a UK-registered B-707-321C aircraft in May 1977 due to failure of the right hand horizontal stabiliser from a fatigue crack in the rear spar, despite the fail-safe design of this component. Post accident inspections revealed a further 38 B-707 aircraft with fatigue cracks in stabilisers, requiring a fleet-wide modification to these components.

19. Boeing initially addressed the ageing aircraft airworthiness issue by conducting damage tolerance analyses (DTA) to define inspection requirements for Significant Structural Details (SSD), which would assure the structural integrity of civil transport type aircraft for the rest of their economic life. The result of the DTA was the issue of Supplemental Structural Inspection Documents (SSID) commencing in 1979.

20. The SSID provided a rational way to extend the operating life of ageing aircraft. In recent years, however, the incidence of a number of structural failures associated with ageing aircraft caused re-examination of the adequacy of this approach. The loss of a large section of the upper fuselage from a Boeing 737 of Aloha Airlines in April 1988 received worldwide media attention with the consequent pressure on regulatory authorities.

21. The airlines, manufacturers and civil airworthiness authorities set up an Airworthiness Assurance Working Group (AAWG). The AAWG established five ageing aircraft programs in 1988, which included:

a. modification and inspection program,

b. corrosion program,

c. maintenance program guidelines,

d. SSID updates, and

e. repair assessment.

22. The requirement to address widespread fatigue damage was a significant outcome from the AAWG.

23. ***ADF.*** The ADF acquires aircraft that are designed and certified to many different design criteria. This may present the ADF with a challenge when evaluating aircraft structural integrity requirements during the acquisition of new or used aircraft. To aid assessment on a comparative basis, the ADF has selected DEF STAN 00-970 as the ADF Structural Design Standard (ADFSDSTD).

Philosophy

24. Fatigue design criteria fall into three categories – safe life, fail-safe and damage tolerance. Damage tolerance, as defined in MIL-HDBK-1530B, is the attribute of a structure that permits retention of the required residual strength for a period of unrepaired usage after the structure has sustained described levels of fatigue, corrosion, and accidental or discrete source damage, such as unstable propagation of fatigue cracks, unstable propagation of initial or service induced damage, and/or impact damage from a discrete source. This can be accomplished through slow crack growth or fail-safe characteristics. Single load path structure must be designed with slow crack growth properties, whereas multiple load path structure can be designed with either slow crack growth or fail-safe properties. In general, most heavy transport type aircraft, whether civil or military, are designed on a fail-safe basis. Most military fighter, attack and trainer type aircraft are designed on either a safe life or damage tolerance basis. However, in reality many aircraft have components that fall into all three categories. DEF STAN 00-970 is based on a safe life approach, but allows an inspection-dependent approach (or safety by inspection) in certain circumstances. The FARs and JARs specify a damage tolerance approach for inspection and residual strength considerations, and allow a safe-life approach. Under the damage tolerance philosophy aircraft are managed on a safety by inspection basis.

25. The ADF, like many foreign military airworthiness authorities, has adopted an integrated, or program, approach to ASI management. The overall program to provide adequate ASI management for ADF aircraft is referred to as the Aircraft Structural Integrity Program (ASIP). The ADF ASIP is based upon MIL-HDBK-1530 with flexibility to adapt the program to reflect different original design standards. The program is based upon characterisation of the durability and damage tolerance features of the aircraft, although there is flexibility to adapt the principles of the program to a safe life approach.

26. The ASIP has grown out of the need to safely manage the structural integrity of aircraft throughout their entire life. This so called cradle-to-grave approach ensures that all structurally related activities from initial design and development through to retirement are adequately addressed. The program is therefore applicable to new aircraft system acquisition, aircraft systems acquired by the ADF but developed in other countries, used aircraft system acquisition, aircraft modified or directed to new operations, and ageing fleets.

27. Each ASIP has five parts spanning acquisition and in-service management. The key outcome of the ASIP at acquisition is to provide a basis for Design Acceptance (via specification, verification and certification) and ensure data is available for the maintenance of that certification basis during the in-service part of the ASIP.

28. The generation of the data requirements detailed in the five ASIP Parts – must be determined by the SPO in consultation with DAIRENG. It is worth noting, for example, that acquisition of an aircraft designed and certified under specific design criteria could still be considered a major structural development if the intended configuration or usage (role and environment) is significantly different from the certification basis, and the change adversely affects the structural life.

AIRCRAFT STRUCTURAL INTEGRITY PROGRAM

29. The certified structural design standard (CSDSTD) is the primary standard and supplementary standard(s) upon which the ASIP of a particular aircraft type is to be based. Where DAIRENG considers the proposed primary structural design standard is deficient, design requirements of recognised supplementary standards may need to be added to the primary standard and the CSDSTD becomes an amalgamation of the primary standard and the supplementary standard requirements. This situation will most typically arise when aircraft designed to a civil standard are acquired by the ADF and the intended or actual usage differs from the civil role.

Organisational Roles

30. ***DAIRENG.*** The role of DAIRENG is to set and regulate structural standards and provide a centre of expertise for the management of aircraft structural integrity. DAIRENG is responsible for establishing the standards by which adherence to the policies in DI(AF) LOG 2-109 is measured. Flowing from these standards is the procedural framework that defines the steps to be followed if the standards are to be met. Apart from its regulatory role, DAIRENG develops and manages implementation of each aircraft type ASIP on behalf of the CI manager, typically the SPO logistics management units, who are responsible for establishment and maintenance of an ASI management system. Within DAIRENG, ASI-DGTA is responsible for fixed wing aircraft and RWS-DGTA is responsible for rotary wing aircraft.

31. ***Role of ASIP Manager.*** Within DAIRENG, the ASIP manager is responsible, through the chain of command, for the development of the ASIMP and management of the implementation of the ASIMP. The ASIP manager is responsible for regular structural life assessments of each aircraft and provision of advice or support to SPOs, AEOs (service and commercial) and Force Element Groups (FEGs) on ASI issues, as necessary.

32. ***Role of SPOs.*** SPOs are responsible for implementing the relevant ASIP activities specified in this chapter for completion during the concept, acquisition and through-life phases of the life cycle. SPOs should ensure adequate consultation is undertaken with DAIRENG during the early part of these phases and, in consultation with Director General Aerospace Development (DGAD) staff, should ensure adequate provision is made in project funding for the completion of the relevant ASIP activities discussed in this Instruction.

33. ***ASI Aspects of Integrated Logistics Support.*** The Concept Phase represents that period during which the broad requirements for the through life support of the proposed weapon system are established and promulgated in the Integrated Logistics Support Plan (ILSP). DAIRENG will provide guidance on ASIP requirements to be incorporated into the ILSP. As a project enters the Acquisition Phase and more aircraft type specific information becomes available, the SPO should supplement the ILSP with more detailed activities from the ASIP, developed in conjunction with DAIRENG.

34. ***Statement of Requirement (SOR).*** DAIRENG is responsible for providing input on the ASI aspects of the SOR. This input is to include relevant DSTO contributions. ASIP Parts I to IV define the certification basis and provide the foundation for continuing airworthiness for the aircraft and each of their elements must be carefully considered during the acquisition phase. These elements establish, evaluate and substantiate the structural integrity (airframe strength, rigidity, damage tolerance and durability) of the aircraft structure. DAIRENG is to ensure that the SOR requires the manufacturer to address relevant ASIP elements, as discussed in paragraphs 35 to 39 of this Instruction.

ASIP PARTS AND ELEMENT DESCRIPTIONS

35. The ASIP is divided into five parts, as illustrated in the TAMM (Section 3, Chapter 11, Figure 11-1 of AAP 7001.053(AM1)). Each of these parts is further segmented into the elements that are essential for a successful ASIP. Linked to relevant ASIP elements are example specification clauses. Annex B provides a list of relevant standards and specifications including the applicable section. Annex C provides a cross-reference index table of all the relevant standards and specifications, by paragraph number, for each of the ASIP elements. Note that references provided in Annexes B and C are based on DEF STAN 00-970, Issue 1 and MIL-HDBK-1530. These references will be updated for DEF STAN 00-970 Issue 2 (and Issue 3) and MIL-HDBK-1530B in a future revision of this chapter. Where detailed mandatory requirements are not expressly contained within appropriate standards, as tailored or supplemented by this chapter, advice shall be sought from DAIRENG.

36. General requirements of the ASIP are as follows:

a. Establish, evaluate and substantiate the structural integrity (airframe strength, rigidity, damage tolerance and durability) of the aircraft structure or helicopter dynamic components;

b. Acquire, evaluate and utilise operational usage and aircraft structural condition data to provide continuing and regular assessment of the in-service integrity of individual aircraft structure/dynamic components;

c. Provide a basis for determining logistics and ADF planning requirements (maintenance, inspections, spares, rotation of aircraft, weapon system replacement and future requirements); and

d. Provide a basis to improve structural criteria and methods of design, evaluation and substantiation for future aircraft structure/dynamic components.

37. An effective ASIP consists of the following five distinct but interrelated functional parts:

a. ***Part I – Design Information.*** Development of those criteria that must be applied during design so that the specification requirements will be met and that must be applied during the life of the aircraft structure/dynamic components.

b. ***Part II – Design Analysis and Development Testing.*** Development of the design environment in which the airframe/dynamic components must operate and the analysis and testing of the response to the environment.

c. ***Part III – Full-Scale Testing.*** Flight and laboratory tests of the airframe and/or components to assist in determination of the structural adequacy of the design, reflect changes in usage or for possible economic life extension.

d. ***Part IV – In-Service Management Data Package.*** Development of a management data package. Generation of data required to manage in-service operation in terms of inspections, modifications, repairs, damage assessments and possible economic life extension.

e. ***Part V – In-Service Management.*** Those tasks that must be conducted by the ADF during in-service operations to ensure damage tolerance and durability throughout the useful life of individual aircraft, including possible economic life extension. The TAMM (Section 3, Chapter 11, Figure 11-2 of AAP 7001.053(AM1)) illustrates the primary flow of information required during in-service management.

38. These parts are each performed to a differing degree during the Concept, Acquisition, In-Service and Disposal phases of the weapon system life cycle and underpin the strategies for conduct of ASI management identified in DI(AF) LOG 2-109.

39. ASIP Parts I to III define the certification basis while Part IV provides the foundation for continuing airworthiness through maintenance of the certification basis. Part V, the in-service management function, is to ensure that the original certification basis continues to be valid for each aircraft in the operating role, configuration and environment.

PART I DESIGN INFORMATION

Structural Design Criteria

40. Except for aircraft specifically designed to meet an ADF requirement, the ADF is rarely in a position to specify the structural design or manufacturing standard to be applied by the manufacturer. Where the ADF is unable to specify the standard to be applied during the development of the aircraft or modification, the adequacy of the standard used is to be assessed. Significant deficiencies are to be redressed by including in the SOR the need for the manufacturer to provide additional substantiation through test or evaluation, as necessary. This requirement will often arise when the ADF procures an aircraft whose intended operation is different to that for which another recognised airworthiness authority has issued a Type Certificate. MIL-HDBK-1530B (Appendix A) provides some guidance on acquisition of new off-the-shelf aircraft. Requirements for small and large civil type aircraft used in a military role are to be published in DEF STAN 00-970 (Parts 3 and 5) in the future.

41. ***Damage Tolerance and Durability Design Criteria.*** A damage tolerant and durability design approach should be used to ensure structural safety, ensure life of type meets PWD, and to minimise in-service maintenance costs. Damage tolerance design approaches are used to ensure structural safety. Durability design approaches are used to provide airframes with minimised in-service maintenance costs and to ensure through-life aircraft availability. The structure should incorporate materials, stress levels and structural configurations that:

a. allow routine in-service inspection,

b. reduce the probability of loss of the aircraft due to propagation of undetected cracks, flaws or other damage to an acceptable level, and

c. minimise cracking, corrosion, delamination, wear and the effects of foreign object damage.

42. ***Corrosion Control and Prevention.*** As the length of service for an aircraft increases, environmental degradation becomes a major maintenance expense. The goal is to control the maintenance costs associated with corrosion and ensure that corrosion does not adversely affect safety of flight. A key aspect of this element is selection of the corrosion protection system. The continuing airworthiness of ageing aircraft is partly dependent upon the control of structural degradation due to the environment.

43. The contractor shall prepare a Corrosion Prevention and Control Program (CPCP), which defines the activities, including the consideration of appropriate materials and processes, finishes, coatings and films, necessary to ensure the airframe is suitably protected from environmental degradation effects for the entire life.

Structural Build Quality

44. Manufacturers will have their own manufacturing quality assurance (QA) programs, which will address the action and documentation required to address manufacturing anomalies. The ADF QA Plan will have to account for the manufacturer's QA program. The SPO is to ensure that all documentation, such as the manufacturer's Material Review Board (MRB) reports, for each build discrepancy and manufacturing anomaly, is obtained. SPOs are to ensure that DAIRENG reviews the QA Plan before it is approved and that the AEO is provided with copies of reports on manufacturing anomalies and the build quality of each aircraft. As a minimum, DAIRENG is to ensure the QA Plan contains adequate provisions for documentation of material discrepancies and manufacturing anomalies during the production of ADF aircraft. Particular attention is to be given to the structural build quality in the vicinity of fatigue critical areas. DAIRENG is to liaise with DSTO to perform an assessment of the influence of the actual build quality on the forecast structural life of the aircraft. The production build quality records of the fatigue critical areas for each aircraft delivered to the Commonwealth are to be documented in a Record of Production Build Quality (RPBQ). Annex D provides guidance as to the content requirements of a RPBQ.

Selection of Material, Processes and Joining Methods

45. The contractor shall identify the proposed materials, processes and joining methods to be used in each structural component and the rationale for the individual selection. The material processes and joining methods selections for fracture critical parts shall require approval by the Commonwealth.

Design Service Life and Design Usage

46. The required design service life and design usage will be established through close coordination between the SPO and DAIRENG, DSTO, DGAD and the FEG. Design mission profiles and mission mixes that are realistic estimates of expected service usage, will be established. Commonwealth specified usage will often not be sufficient in itself for a contractor to determine an aircraft LOT. Supplementary spectra, such as asymmetric loads and ground loads spectra, used by the contractor are to be agreed by the Commonwealth.

47. Commonwealth provided design service life and usage will also be used for evaluation of aircraft or modifications designed to service lives and usage spectra other than specified by the ADF. This is usually the case for the acquisition of new aircraft, where the ADF provides no input into the initial design, used aircraft, and for structural modifications to existing aircraft.

Non-Destructive Inspection

48. Non-destructive testing and inspection requirements should be considered early in the design development and the appropriate tools and methods integrated into the overall risk management.

PART II DESIGN ANALYSES AND DEVELOPMENTAL TESTS

49. The objective of this part is to determine the environment that the airframe must operate in and to perform preliminary analysis and testing (based on this environment) to design the airframe or modification to meet the required strength, damage tolerance and durability requirements.

Design Service Loads Spectra

50. The purpose of the design service loads spectra is to develop the distribution and frequency of loading that the structure will experience based upon the design service life and typical usage. Load and stress spectra need to be developed to support analysis and testing.

Loads Analysis (External)

51. The contractor shall comply with the detailed requirements for load analysis as specified in the contract specifications. The loads analysis shall consist of determining the magnitude and distribution of significant static and dynamic loads that the aircraft may encounter. This analysis consists of determining the flight loads, ground loads, power-plant loads and weapon effects. The analysis may also include the effects of temperature and aeroelasticity, if appropriate. A comprehensive flight loads program to verify the loads is essential.

Design Chemical/Thermal Environment Spectra

52. As aircraft age, the structural degradation due to environmental effects can have a significant effect on the attainable life. The environmental spectra should characterise the operational environment in terms of severity and duration.

Material and Joint Allowables

53. The contractor shall use as appropriate the materials and joint allowables defined in DEF STAN 00-932, Metallic Materials Data Handbook, MIL-HDBK-5, Metallic Materials and Elements for Aerospace Vehicle Design and MIL-HDBK-17, Plastic for Aerospace Vehicles. DEF STAN 00-932 and MIL-HDBK-5 can be used for guideline purposes for contractor generated data. When new materials are used, properties shall be justified by reference to experimental data that must be approved by the Commonwealth. The generation and analysis of test data for new material shall follow the guidelines presented in Chapter 9 of MIL-HDBK-5. Allowables for composites shall be derived based upon the requirements for composites and adhesive bonding in MIL-STD-1587. Other data sources may also be used but will require approval by the Commonwealth.

Stress Analysis

54. Stress analysis consists of the analytical determination of stresses, deformation (stiffness) and reserve factors (or margins of safety) resulting from the external loads and temperatures applied to the structure. Stress analyses are used for strength, fatigue and damage tolerance analyses. The determination of the local stress is also used for the selection of structurally significant items and the determination of significant loading actions. Stress analyses have to be revised for structural modifications, changes to loading conditions and significant changes to aircraft weight.

Durability and Damage Tolerance Analysis

55. The nature and extent of fatigue life substantiation undertaken by a manufacturer will be influenced by the structural design standard. Accordingly, the adequacy of proposed fatigue life substantiation is to be assessed by DAIRENG in light of the intended ADF usage of the aircraft. Regardless of whether or not the aircraft is designed to a safe life philosophy, a durability and damage tolerance assessment (DADTA) is required.

56. DAIRENG is to ensure that for all aircraft being procured the SOR adequately specifies the requirement for a damage tolerant design, which will ensure structural safety through the consideration of undetected flaws existing in critical structural components, despite the design, fabrication and inspection efforts expended to eliminate their occurrence. In addition, demonstration is required that durability structural design approaches have been used to minimise in-service maintenance costs and improve operational readiness and airworthiness throughout the design service life of the aircraft and during possible economic service life extension. The nature and extent of durability and damage tolerance substantiation undertaken by the manufacturer will be determined by the structural design standard. SPOs are responsible for ensuring that DAIRENG defined requirements in this regard are actioned.

Aeroacoustic Durability Analysis

57. The structure is to be designed to resist sonic cracking throughout the life. An aeroacoustic durability analysis is to be carried out for an assumed aeroacoustic environment to demonstrate that aeroacoustic effects have been addressed in the design process and that the structure is suffiently resistant.

Vibrations Analysis

58. The vibration analysis should predict the resultant environment in terms of vibration levels in various areas of the aircraft. The analysis should show that the structure is resistant to vibration cracking throughout the life. For rotorcraft, particular reference should be made to ground resonance.

Flutter Analysis

59. The flutter analysis should determine the characteristics of the aircraft for flutter, divergence and other related aeroelastic instabilities. The analysis should substantiate the ability of the aircraft structure to meet the specified flutter airspeed margins and damping requirements for all design conditions. Analysis should include design failure conditions as well.

Mass Property Analysis

60. Mass property analysis of the structure must be established. The weight distribution is needed because it affects all aspects of aircraft usage. Weight growth during the life of the aircraft can lead to significant structural problems and possible operational limitations if it is not controlled.

Weapons Effects Analysis

61. The objective of the weapons effects analysis is to determine the capability of the structure to survive the effects of weapon damage. Consideration should be given to evaluating the battle damage tolerance, repairability, construction modularity, accessibility and fail safety of the design, and to the influence of battle damage on material selection.

Design Development Testing

62. The objectives of design development testing are:

a. to establish material and joint allowables;

b. to verify analysis methodologies;

c. to obtain allowable stress levels, material selections, fastener systems, and determine the effect of environment spectra; and

d. to obtain early evaluation of the strength, durability and damage tolerance of critical structural components and assemblies.

PART III FULL SCALE TESTING

63. The objective of this part is to assist in determining the structural adequacy of the basic design through a series of ground and flight tests. Military design standards require verification of design through testing to representative design loads and usage. However, the civil design standards place the onus on analysis supported by test *where necessary*. Therefore, where ADF aircraft have been certified to a civil standard, the design verification rationale must be carefully considered. Considerations which may affect the testing requirements include the inspectability of the structure (large open type structure typical of civil transport aircraft improve inspectability) and the intended operational usage.

Static Tests

64. The static test program should consist of a series of tests conducted on an instrumented airframe that simulates loads from critical flight and ground conditions. The aim of the static test program is to verify the static strength analyses and the design ultimate strength capabilities of the airframe. Static tests will also help to establish the amount of weight growth potential in the structure.

Fatigue Tests

65. Design validation testing on aircraft procured by the ADF will generally have been conducted before the aircraft type enters ADF consideration. In this case, fatigue testing will usually have been based on assumed operational usage that may not reflect ADF intended or actual usage. Accordingly, additional scatter factors may need to be applied to the fatigue life established by this testing. This will establish the safe life of the airframe/dynamic components. Additionally, there is a requirement to conduct damage tolerance testing to determine crack growth information that can be used for damage tolerance assessment. Limitations of the design validation test, relative severity of intended or actual ADF usage, or substantial variations in build state, may impose large scatter factors on the test life. Furthermore, damage tolerance testing may not have been conducted as part of the design validation testing. In such cases a follow-on full-scale fatigue test, termed a Fatigue Life Substantiation Test, may be warranted. Similarly, the need to significantly extend the aircraft service life may require additional testing be conducted. DEF STAN 00-970, Issue 2 (Leaflet 37) provides guidance on fatigue testing.

66. ***Fatigue Test Article.*** In order to ensure the Fatigue Life Substantiation Test is representative, acquisition of a full-scale fatigue test article is to be considered as part of the ADF production run to ensure it represents the structural configuration and build quality of the fleet. SPOs are responsible for ensuring DAIRENG advice on this requirement is sought and sufficient resources provided in project allocations for the implementation of any follow-on structural testing.

67. ***Durability Tests.*** Durability tests of the airframe should consist of repeated application of the flight-by-flight design spectrum. For Fatigue Life Substantiation Tests, a spectrum representative of ADF operational usage shall be applied. The objectives of the full scale durability tests are to:

a. demonstrate the economic life of the airframe/dynamic components;

b. identify the critical areas of the structure not previously identified by analysis or component testing;

c. provide a basis for establishing special inspections and modification requirements; and

d. for Fatigue Life Substantiation Tests, verify the life of post-production modifications.

68. The test duration is a function of many considerations including the design service life, the desire to determine life extension capabilities, the severity of the loading spectrum relative to typical usage, the applicable scatter factor and the desire to validate repairs, modification or structural changes.

69. ***Damage Tolerance Tests.*** The purpose of conducting damage tolerance tests is to determine crack growth characteristics and validate damage tolerance analyses. Damage tolerance tests are sometimes, but not always, conducted at the completion of the durability test using the same test article. Damage growth testing can be conducted prior to or following the end of the production fatigue test, using, if necessary, artificially induced damage to initiate damage growth.

Flight and Ground Operations Tests

70. Loads measurements shall be made, usually by strain gauge methods, on an early production aircraft. A later production model of typical production configuration should also be used to measure flight and ground loads. These measured loads are used for:

a. verification of the structural loads and temperature analysis used in the design of the airframe/dynamic components,

b. evaluation of loading conditions which produce the critical structural load and temperature distribution, and

c. determination of new critical loading conditions.

71. Flight and ground tests are also carried out to support follow-on durability and damage tolerance analysis and testing.

Aeroacoustic Durability Tests

72. Measurements should be made of the acoustic environments on a full scale aircraft to verify or if required modify the initial design aeroacoustic loads/environment. If deemed applicable, a sonic durability test should be conducted on a representative airframe or major components to demonstrate full life.

Flutter and Vibration Tests

73. Flutter and vibration tests should be conducted to verify the accuracy of the flutter vibration analysis. Both ground and flight vibration tests should be conducted. Major structural modifications may affect the dynamic characteristic of the airframe and additional ground and flight vibration tests may be required. Ground vibration tests are conducted at low load levels and caution must be exercised if extrapolating to flight levels.

Interpretation and Evaluation of Results

74. Each structural problem identified in the tests described in the previous paragraphs should be analysed to determine the cause, corrective actions and fleet implications. Structural modifications or changes resulting from these deficiencies must be substantiated through analysis or additional testing. MIL-HDBK-1530B (paragraph 5.3.10) discusses the interpretation and evaluation of results. Where structural failures have been deemed unrepresentative, DAIRENG should be advised and confirmation sought.

PART IV IN-SERVICE MANAGEMENT DATA PACKAGE

Final Analysis

75. The preliminary analyses carried out in Part II should be revised as appropriate to account for significant differences between the analysis and test, which were revealed during the full scale tests and flight tests. The appropriate final analyses (stress, damage tolerance, fatigue and others) should be used to develop inspection and repair criteria. The analyses can be used to develop inspection and maintenance intervals and to develop repair procedures. MIL-HDBK-1530B (paragraph 5.4.1) discusses final analyses. DEF-STAN 00-970, Issue 2 does not directly address this element; however, Leaflets 35 to 37 of DEF-STAND 00-970, Issue 2 do discuss analysis and test.

Aircraft Structural Integrity Documentation Package

76. The Aircraft Structural Integrity Documentation Package (ASIDP) should summarise the final analysis and other relevant structures information that will provide the basis for ADF type certification and provide rapid visibility in service of important characteristics, limitations and capabilities. Guidance as to the minimum content requirements for an ASIDP is provided in Annex E.

Aircraft Structural Integrity Management Plan (ASIMP)

77. ***Purpose and Content.*** The vehicle for documenting the strategies for the ASI management of a specific aircraft type is the ASIMP. The ASIMP is a proactive plan that addresses the ASIP activities required to be undertaken over the short, medium and long term of an aircraft type service life with particular emphasis on the next three to five years. As an aircraft progresses through the different phases of the life cycle, the ASIMP will reflect the activities necessary to ensure that structural integrity does not reduce below that established at introduction to service. A separate ASIMP is not to be produced for different models of an aircraft type. However, the ASIMP is to clearly identify the differences between models and any special ASI management requirements unique to a particular model. Annex F provides guidance on the content and structure of an ASIMP. The ASIMP content and structure do differ for a fixed wing aircraft and rotary wing aircraft and these differences are defined in Annex F.

78. ***ASI Projects.*** ASIMPs are required to identify and address current or foreseen ASI deficiencies by referring to ASI projects. ASI projects can include any or all of the following:

a. changes to the method of collecting usage data;

b. structural testing requirements;

c. aircraft structural tear downs;

d. special inspection programs to obtain structural condition information beyond that routinely gathered;

e. corrosion recovery programs;

f. repair/replacement and/or modification action; or

g. DSTO research tasks.

79. ASI projects are to be planned and agreed by the ASIP manager, the relevant AEO and, where appropriate, DSTO. Generally, ASI projects dealing with structural degradation problems such as corrosion would be managed by the relevant AEO and those dealing with fatigue problems, such as a durability and damage tolerance assessment (DADTA) requirement, would be managed by DAIRENG. However, in each case project management of an ASI task is to be decided between the AEO and DAIRENG.

80. ***ASIMP Approval Process.*** The ASIMP forms an integral part of the ADF airworthiness management policy (DI(G) OPS 2-2) and technical airworthiness regulations (AAP 7001.053(AM1), Regulation 3.5.4). Accordingly, each ASIMP is to be authorised by DAIRENG, following review by the relevant AEO and approval by the OIC of ASI-DGTA or RWS-DGTA.

81. ***Aircraft Acquisition ASIMP Requirements.*** An ASIMP is to be produced and reviewed for all aircraft types being considered for acquisition. A draft ASIMP is to be part of the Tender Deliverable Requirements List and is to provide the basis for ASI management of the aircraft. ASI tender deliverable requirements are to include the following (guidance is to be sought from ASI-DGTA or RWS-DGTA if this listing is to be tailored);

a. draft version of the ASIMP Volume 1 (and Volume 2 if required);

b. an initial aircraft structural life assessment;

c. structural verification plan (or ASI verification is to be adequately embedded in the aircraft certification plan); and

d. sufficient substantiation and evidence that the aircraft is going to achieve the required LOT.

82. An alternative to the draft ASIMP tender deliverable requirement is an Aircraft Structural Integrity Report (ASIR). An ASIR is essentially an abridged ASIMP. The purpose of the ASIR is to provide the Commonwealth with confidence in the ability of the Contractor to be able to address through life ASI management issues for the aircraft presented for tender. The ASIR is to include a detailed description of the aircraft structural certification basis, the critical structure (including analyses) and the systems (usage monitoring, fatigue management and environmental degradation management for example) required to support the through life ASI management of the aircraft. Guidance for the content and structure of an ASIR is to be sourced through consultation with ASI-DGTA or RWS-DGTA.

83. The ASI tender deliverable requirements developed by the Contractor(s) are to be reviewed by ASI-DGTA or RWS-DGTA and authorised by DAIRENG. Subsequently, observations and feedback of the implications to the required structural LOT (safety, availability and cost of ownership) for each aircraft type being considered for acquisition will be provided to the PO. Once an aircraft has been selected for acquisition the PO is to ensure the ASI tender deliverable requirements are included in the Contract Deliverable Requirements List. The ASI contract deliverable requirements are further discussed in paragraphs 102-105 of this chapter. Guidance on the structure and content of an ASIMP and a structural verification plan (SVP) are provided in Annexes F and G, respectively.

Operational Loads Measurement

84. An operational loads measurement (OLM) system aims at direct measurement of parameters necessary to define the actual loads experienced by the aircraft structure, for a given aircraft configuration, role and environment. Helicopters pose particular problems in this area because of the difficulties associated in monitoring loads on the rotary lift system. The objective of an OLM program is to obtain time history records of these parameters so that the actual load or stress spectra may be determined for the critical areas of the aircraft structure under representative operations. A representative sample (typically 10 to 20 percent) of operational aircraft shall be instrumented to measure such pertinent parameters as velocity, accelerations, altitude, fuel usage, temperature, strains, rotor RPM, pitch and roll rates, etc. An accurate environmental spectrum must also be determined for aircraft utilising composite structures. Data acquisition is to commence with delivery of the first operational aircraft. Accordingly, the SPO and/or

PO is to ensure the SOR includes provisions for the installation of an appropriate operational loads and environment monitoring system together with the provision of ground based data analysis and recording systems and software. Variation of this requirement requires TAA approval. SPOs are to ensure adequate provision is made in the project allocations to satisfy this requirement.

85. It is essential that strain sensors used for OLM be calibrated. These strain sensors should be replicated on production tests and subsequent follow-on fatigue tests to allow direct comparisons to be made.

Health and Usage Monitoring

86. A health and usage monitoring system (HUMS) monitors structural locations and dynamic components deemed to be critical by the original equipment manufacturer (OEM) from a fatigue or economic point of view. This is achieved through the monitoring of the aircraft usage, through recording of flight parameters and/or strain data.

87. An aircraft is assessed for acquisition based on the suitability to satisfy the ADF expected usage requirement. Past experience has indicated that initial service usage often produces fatigue damage at a greater rate than that predicted prior to acquisition. Aircraft usage also typically changes during the life from that originally planned due to varying capability requirements. The result is often an aircraft operating at either a higher than anticipated risk or with an increased operating cost (for example decreased inspection intervals). Unless the usage of each aircraft is monitored from introduction to service, a conservative approach must be adopted when retrospectively evaluating the fatigue damage accrued during the unmonitored period. This can severely restrict the operational availability of aircraft later in the life cycle.

88. It is therefore essential that a fleet-wide HUMS capable of collecting, storing and reporting aircraft usage is in place when an aircraft enters service. There is no standard monitoring system used in the ADF. Instead the most appropriate system for a particular fleet is to be selected based on both the size and cost of the fleet, and variability in usage. These considerations define a hierarchy of possible monitoring systems of increasing accuracy and complexity:

a. ***Simple Parametric Approach.*** The simplest monitoring system involves recording only several significant parameters, such as flying hours or flight cycles for each aircraft. This is particularly appropriate for long-range transport aircraft where the operational role is well defined.

b. ***Extended Parametric Approach.*** The above system can be expanded to record other significant parameters that are significant to fatigue damage, particularly when operational roles vary.

c. ***Fatigue Meter.*** For the majority of military aircraft, usage varies significantly such that a ‘fatigue meter’ is required. The ‘fatigue meter’ does no more than register counts in the vertical axis at the aircraft centre of gravity. The accumulation of these counts helps define the load spectrum. To relate component stresses to loads, it is necessary to record some other parameters, for example, weight and stores configuration. On ADF aircraft, fatigue meter counts are usually recorded after each flight along with mission type. Hence, a flight-by-flight sequence is obtained for each monitored aircraft. However, the fatigue meter has limitations. It is good for measuring loads in the centre fuselage and inner wing where there is good correlation between ‘g’ levels and stresses in the structure, but the fatigue meter takes no account of rolling or yawing, high angle-of-attack flying or the effects of wing-sweep, nor does it provide data to measure the loading in structure which is not related to ‘g’, for example the aft fuselage or ground loads.

d. ***Advanced Recording Devices.*** Modern sophisticated flight recorders record both parametric and strain data. Consequently, structural loads can be derived directly from the strain data and validated using the parametric data. In addition, the parametric data provides the ability to reconstruct the flight profiles of the aircraft to investigate aircraft incidents.

89. DAIRENG is to ensure that the HUMS adequately reflects the role of the aircraft and the characteristic structural degradation regimes. DAIRENG is also to ensure that operational staff are aware of the information collected from the HUMS and the applicable management procedures and processes, and that the requirements for routine reporting are implemented. SPOs are to ensure adequate provision is made in project allocations for the development and implementation of an appropriate HUMS. SPOs are to ensure that the ASIMP documents the HUMS for the aircraft.

90. Chapter 19 of this Instruction (titled ‘Health and Usage Monitoring Systems’) provides specification guidance and certification requirements for a HUMS. The scope of chapter 19 includes the acquisition of a new aircraft with a

HUMS fitted and for the retrofit of existing aircraft with a HUMS. Chapter 19 also details the management systems that must be put in place by SPOs to support a HUMS and provides guidance as to the requirements for HUMS validation.

Routine Structural Life Monitoring Program

91. A structural life monitoring program is to be in place by the time a newly acquired aircraft enters operational service. The minimum requirement of this program is the periodic calculation of fatigue damage accrual for individual tail numbers. Provision is to be made for including the effects of other forms of structural/dynamic component degradation (including the assessment of structural build quality discussed earlier) and their influence on the life of the structure. A system of routine reporting of the structural life remaining on individual aircraft and/or aircraft components, and the ability of the fleet to achieve PWD is to be included in this program. SPOs are to ensure that the ASIMP contains details of the routine structural life monitoring program as endorsed by DAIRENG. DAIRENG is to ensure that the program provides sufficient feedback to operational staff for unit management purposes. In addition, DAIRENG is to also ensure that DSTO is routinely involved in the review of the program and its output.

Additional Data Requirements for Used Aircraft

92. When used aircraft are considered for acquisition, it must be recognised that their previous operation and structural integrity management may have been different than ADF practices or philosophy. Usage, maintenance, fatigue and any other relevant data from previous operators and the OEM shall be obtained.

PART V IN-SERVICE MANAGEMENT

93. In-service management defines those tasks that must be conducted by the ADF during in-service operations to ensure damage tolerance and durability throughout the useful life of individual aircraft including possible economic life extension. The in-service management is not specifically addressed in any of the design criteria because it is the responsibility of the ADF to ensure that a sound in-service management program is in place to assure the continued structural airworthiness of the fleet.

Routine Structural Life Assessment Reporting

94. DAIRENG is responsible for conducting routine structural life assessments as part of an overall ASIMP management cycle and for implementing the results as appropriate.

Operational Loads Measurement

95. The nature and frequency of operational loads measurement of an aircraft type will have been determined during Part IV In-Service Data Management. The SPO is to ensure that the OLM program is maintained throughout the In-Service Phase or that TAA approval is obtained for suspending the OLM capability. Generally, suspension of an OLM program should only be considered where sufficient evidence exists that the information obtained from the initial program adequately defines the loads environment and that the HUMS will detect any change in operational usage that may affect the loading environment. Notwithstanding the adequacy of a HUMS, the necessity for re-introducing an OLM program is to be specifically examined as part of the review of the structural life assessment program or when a change in aircraft role is proposed or detected. AEOs are responsible for maintaining the integrity of the OLM system installed on aircraft.

Usage Monitoring Data

96. During the Acquisition Phase, the usage monitoring aspect of the HUMS developed for the aircraft will have been based on the intended utilisation and the structural life management philosophy adopted for the aircraft type. Invariably, the usage monitoring program will be a fundamental element of the structural life monitoring program. Accordingly, review of the appropriateness of the usage monitoring program will be required in concert with a review of the structural life monitoring program. DAIRENG is responsible for the management of usage monitoring of ADF aircraft at all stages in the life cycle. During the In-Service Phase, DAIRENG is to ensure that the usage monitoring program provides feedback on the usage of individual aircraft, and the fleet of an aircraft type, to:

a. assess if each individual aircraft is being operated within the defined usage spectrum of the fleet and hence, assess if the certification basis remains valid;

b. enable structural life assessments to be based on actual individual aircraft usage; and

c. provide historical data on which to base predicted usage spectra for future acquisitions.

Structural Degradation Control Program

97. An essential element of an aircraft ASIP is the control of those factors that influence structural degradation. Accordingly, programs are to be implemented that provide adequate surveillance of the aircraft structure and operational environment, to enable the factors that influence structural degradation to be monitored and corrective action to be taken. The factors that are to be considered during the development of a structural degradation control program are detailed in the ASI guidance chapter of AAP 7001.053(AM1).

98. A corrosion assessment, prevention and control program is one example of the type of program that is required to prevent unforecast structural integrity problems. Another is a fatigue life conservation program that may involve flight limitations, aircrew awareness briefs and raising maintenance personnel awareness of fatigue sensitive structure. Whilst such programs should be established during the Acquisition Phase, most threats to the aircraft structure arise during the In-Service Phase. Accordingly, DAIRENG is to ensure adequate programs are in place when an aircraft transitions to In-Service. The adequacy of the programs is to be reviewed and updated, as necessary, as part of the ongoing ASIMP management cycle. The ASIMP is to reflect the scope of the structural degradation control program for each aircraft type.

Structural Deterioration Records

99. Structural repair action can consist of rework within negligible damage limits, installation of repairs contained in the aircraft Structural Repair Manual (SRM) and design and installation of non-standard repairs (note that the decision to not repair or to replace the damaged part are both repair actions). Each of these repair actions can influence structural life, especially if conducted without knowledge of previous repair action in the vicinity. Accordingly, records are to be kept of any repair action performed on aircraft primary structure and should be kept on secondary structure; records are not required to be kept for repairs to tertiary structure. The nature and level of detail of the records kept is to reflect the significance of each repair.

ADDITIONAL REQUIREMENTS PERTAINING TO USED AIRCRAFT

100. When used aircraft are being considered for acquisition, recognition must be made that their previous operation and structural integrity management may have been at variance with ADF practices or philosophy. Accordingly, particular care must be exercised in assessing the degree of conformity to ADF standards. Therefore, apart from the requirements outlined in the other paragraphs in this section, DAIRENG is to ensure that the relevant SPO and/or AEO is aware that, before used aircraft are operated under ADF airworthiness control, the following requirements are to be completed:

a. Previous usage, maintenance, repair and modification records of each individual aircraft are to be obtained, examined and an assessment made of the reliability and comprehensiveness of those records.

b. A physical examination of the condition of critical components, including inspections for structural degradation, is required to assess the effects of previous usage, repairs, modifications and environmental degradation. The scope of actual inspections to be conducted will largely be governed by the assessment of aircraft maintenance records and the competency of the previous operator maintenance and ASI programs.

c. The accrued fatigue damage on each aircraft is to be determined using appropriate scatter factors to account for unreliability of previous usage history and deterioration of the structure from the as manufactured condition.

d. Where possible, a high time structural tear-down article (of similar build configuration to either the newly acquired or current in-service fleet) should be obtained to assist in forecasting structural integrity problems. This activity does not remove the requirement for consideration of the purchase of a fatigue test article, especially if the used aircraft are not supplementing an existing fleet in ADF service.

101. MIL-HDBK-1530B (Appendix A) provides some guidance on acquisition of used aircraft and potential aging aircraft issues and Appendix B contains further guidance on ageing aircraft.

WEAPON SYSTEM ACQUISITION AND THROUGH LIFE SUPPORT CONTRACTS

102. Current DMO policy is to engage Through Life Support (TLS) Contractors for the complete management and support of weapon systems, both for weapon systems currently in-service and for those being considered for acquisition. Under this arrangement, certain elements of the ASI management responsibility will be transferred from ASI-DGTA and RWS-DGTA to a competent contractor. There are various services and data deliverable requirements (plans and reports) associated with ASI management and engineering activities. The ASI management and engineering requirements for DMO TLS contracts are to be incorporated into the Contract Deliverable Requirement List (CDRL) as Detailed Service Descriptions (DSDs) and Data Item Descriptions (DIDs).

103. DMO is to approach and work together with ASI-DGTA and RWS-DGTA when developing DSDs and DIDs specific to ASI management and engineering activities. ASI-DGTA and RWS-DGTA will be able to provide tailored DSDs and DIDs to DMO on request and are responsible for reviewing all DSDs and DIDs associated with ASI management and engineering activities. DAIRENG has the authority to approve the pertinent DSDs and DIDs, prior to their inclusion in all TLS contracts.

104. A sample DSD providing guidance to DMO for Engineering Support Services (ASI management aspects) is attached at Annex H. The scope of this DSD is to encompass all ASIP management tasks identified as the responsibility of the contractor. Subordinate to this DSD are DIDs that document the ASI management and engineering requirements of the contractor. Sample ASI management and engineering DIDs have been provided for the following data deliverable requirements:

a. Record of Production Build Quality – Annex D;

b. Aircraft Structural Integrity Documentation Package – Annex E;

c. Aircraft Structural Integrity Management Plan – Annex F;

d. Structural Verification Plan – Annex G;

e. Deeper Maintenance Report – Annex I;

f. Routine Usage Status Reports – Annex J;

g. Usage Assessment Report – Annex K;

h. Structural Condition Assessment Report – Annex L; and

i. Fatigue Assessment Report – Annex M.

105. DMO may combine the requirements of ASI DSDs and DIDs with equivalent Engine Structural Integrity (ESI) DSDs and DIDs in order to create a single DSD or DID for a single Contractor responsible for both ASI and ESI Program management (refer to Section 4, Chapter 1 of this Instruction for ESI DSDs and DIDs). DMO must seek guidance from ASI-DGTA and RWS-DGTA when combining ASI and ESI management requirements into a single DSD or DID.

FURTHER DEVELOPMENT OF SECTION 2 CHAPTER 11

106. This chapter is still under development and areas to be addressed in future amendments include:

a. Guidance on the concept of usage monitoring/OLM design, certification and in-service management.

b. Guidance on test versus analysis for structural substantiation.

c. Update of Chapter 11 (including associated annexes and DSD/DIDs) to reflect revised ASI requirements as necessary (ie. DEF-STAN 00-970 Issue 3, MIL-HDBK-1530C, environmental degradation management).

d. Inclusion of additional guidance (in the form of sample DIDs) on ASI type certification requirements for aircraft acquisition and through life support contracts.

e. Improved integration of DSD/DID philosophy and requirements into the body of Chapter 11.

Annexes:

A. Definitions to be applied to ADF ASI Management

B. Standards and Specifications

C. ASIP Part and Element Standards and Specification Reference Table

D. Sample DID for Record of Production Build Quality

E. Sample DID for Aircraft Structural Integrity Documentation Package

F. Sample DID for Aircraft Structural Integrity Management

G. Sample DID for Structural Verification Plan

H. Sample DSD for Engineering Support Services – ASI Aspects

I. Sample DID for Deeper Maintenance Report

J. Sample DID for Routine Usage Status Reports

K. Sample DID for Usage Assessment Report

L. Sample DID for Structural Condition Assessment Report

M. Sample DID for Fatigue Assessment Report

Blank Page

DEFINITIONS TO BE APPLIED TO ADF ASI MANAGEMENT

Allowable Load (or Stress). The maximum load (or stress) value used for design purposes, taking into account material factors.

Applied Load (or Stress). The load (or stress) value relating to a specific design case.

Block. A specified sequence of loads applied to a fatigue test. A block may incorporate a series of load cycles representing flight and ground loads and ground-air-ground cycles. A block usually reflects an equivalent number of flight hours.

Certification Fatigue Life. The Certification Fatigue Life is the fatigue life established through testing or a form of validation acceptable to the DAA and Airworthiness Board. This fatigue life will reflect the limit of certification testing undertaken and is used for fleet planning purposes.

Certification Structural Design Standard (CSDSTD). An aircraft's CSDSTD is that which the ADF has approved by the process of type certification.

Damage Tolerance. Damage tolerance is the ability of the airframe to resist failure due to the presence of flaws, cracks, or other damage for a specified period of unrepaired usage.

Design Limit Load. This is the greatest load that is expected to occur during the specified life in any particular design case.

Design Ultimate Load. This is the product of the design limit load and the ultimate factor, normally 1.5.

Durability. The ability of the airframe to resist cracking (including stress corrosion and hydrogen induced cracking), corrosion, thermal degradation, delamination, wear, and the effects of foreign object damage for a specified time.

Equivalent Flight Hours. The unit of time used in block loading during fatigue testing.

Factor of Safety. The factor of safety is a design factor used to provide for the possibility of loads greater than those anticipated in normal conditions of operation and for uncertainties in design.

Fail-Safe. Fail-safe means that the structure has been evaluated to assure that catastrophic failure is not probable after fatigue failure or obvious partial failure of a single, principal structural element.

Life of Type. The upper limit of service life (in AFHRS, landings or cycles) which has been qualified either by test or calculation, or set as a requirement.

Load Factor. The load factor is the ratio of a specified load to the total weight of the aeroplane; specified load may be expressed in terms of any of the following: aerodynamic forces, inertia forces or ground reaction.

Mission Mix. The composition of the missions flown over a specified period based on a percentage of total operations for that period.

Mission Profile. The altitude-time profile representative of typical operations for the mission code.

Planned Withdrawal Date. The date which has been promulgated for removal of the aircraft type from service.

Reserve Factor. Reserve Factor is defined as the Allowable Load (or Stress) divided by the Applied Load (or Stress).

Residual Strength. Residual strength is the minimum internal member load which the structure is required to sustain with damage present without endangering safety of flight.

Safe Factored Life. The calculated safe life having applied the appropriate reduction factor to account for statistical variances in design and testing.

Safe Life. Safe life means that the structure has been evaluated to be able to withstand the repeated loads of variable magnitude expected during its service life without detectable cracks.

Safe Life Management. Based on a safe life evaluation, this philosophy requires the component to be retired from service before the likelihood of failure becomes unacceptable.

Safety by Inspection. A process for assuring continued structural airworthiness by repeated inspection of critical locations at designated periodicity to detect significant defects prior to imminent failure.

Safety by Inspection Management. Safety by inspection means that the risk of failure is constrained by a program of inspections which regularly assess the integrity of the item.

Scaling Factor. A factor used to relate the analytical predictions to actual test result data.

Scatter Factor. A factor used to account for the variances in design and testing procedures to produce a specified level of confidence.

Screening. The process of checking fatigue data for errors in input data against a range of acceptable values.

Spectra. A plot of g-level (or other parameter such as stress or load) values against the number of exceedances at that level, usually normalised per 1000 hours.

Structural Integrity. The ability of all constituent parts of an aircraft's structure to withstand normal operating loads within approved flight limitations without collapse or unacceptable deformation.

Structure – (primary). A structural assembly essential for carrying loads imposed by all flight manoeuvres, take-offs, or landings within the design limits of the aircraft, the failure of which may directly result in the structural collapse, loss of control or motive power, unintentional operation or inability to operate essential services, or cause injury to any occupant.

Structure – (secondary). Any structure carrying loads normally transmitted to the primary structure or an alternative load path, the damage to which may not directly impair the aircraft safety.

Structure – (tertiary). A structural member or assembly that is not primary or secondary structure and is normally unstressed or lightly stressed, the damage to which may not directly impair the aircraft safety.

Ultimate Load. An ultimate load is the limit load multiplied by the appropriate factor of safety.

Usage. The term used to define the manner in which an aircraft is operated, including the rate of flight cycle, landing, airframe hour accrual and mission utilisation rates.

STANDARDS AND SPECIFICATIONS

Standard or Specification	Title
DEF STAN 00-932	**Metallic Materials Data Handbook**
DEF STAN 00-970	**Design and Airworthiness Requirements for Service Aircraft**
Chapter 112	Reduction of Vulnerability to Battle Damage
Part 2	Structural Strength and Design for Flight
Chapters 200	Static Strength and Deformation
Para 5	Demonstration of Compliance with the Ultimate Strength and Proof Requirements for Complete Structures or Components
Leaflet 200/2	Static Strength and Design for Flight
Leaflet 200/4	Strength of Structures under Conditions of Heating and Cooling
Chapter 201	Fatigue Damage Tolerance
Para 3	Inspection Requirements
Leaflet 201/1	Fatigue and Damage Tolerance – Main Features of the Requirement
Leaflet 201/2	Material Selection
Leaflet 201/3	Substantiation of Fatigue Life
Leaflet 201/4	Substantiation of Damage Growth and Associated Inspection Procedures
Leaflet 201/5	Fatigue Damage Tolerance – Testing
Leaflet 201/6	Fatigue Damage Tolerance – Service Monitoring
Chapters 202	Symmetric Manoeuvres
Chapters 203	Asymmetric Manoeuvres
Chapters 204	Gust Loads
Chapter 401	Design Data for Metallic Materials
Leaflet 401/0	Design Data for Metallic Material – Reference Page
Chapter 402	Processes and Working of Materials
Leaflet 402/0	Processes and Working of Materials – Reference Page
Leaflet 402/1	Fusion Welding, Friction Welding and Diffusion Bonding
Leaflet 402/2	Adhesive Bonding of Structural Parts – Processes and Controls
Leaflet 402/3	Adhesive Bonding of Structural Parts – Recommended Design Practice
Leaflet 402/4	The Effects of Surface Finish and Protective Treatments on Fatigue Properties
Leaflet 402/5	Coatings of metals with plastic materials
Leaflet 402/6	Brazing and Soldering
Leaflet 402/7	Sealants and sealing
Chapter 403	Castings
Leaflet 403/1	Static Strength Approval for Castings
Chapter 409	Precautions against Corrosion and Deterioration
Leaflet 409/0	Precautions against Corrosion and Deterioration – Reference Page
Leaflet 409/1	The Penetration of Titanium Alloys by Solid Cadmium
Leaflet 409/2	The Stress Corrosion of Titanium Alloys by Fluorinated Sealants at Elevated Temperatures
Leaflet 409/3	Avoidance of Galvanic Corrosion at Bimetallic Contacts
Leaflet 409/4	Deterioration of Fibrous Materials
Chapter 500	Aeroelasticity
Para 5.1	Mass Distribution and Structure
Leaflet 500/1	Aero-Elasticity – Flutter Clearance Program
Leaflet 500/2	Aero-Elasticity – Main Surface Flutter
Leaflet 500/3	Aero-Elasticity – Flutter of Control Surfaces
Leaflet 500/4	Aero-Elasticity – Spring and Servo Tab Flutter
Leaflet 500/6	Aero-Elasticity – Stiffness Tests
Leaflet 500/7	Aero-Elasticity – Hydraulic Actuator Impedance
Leaflet 500/8	Aero-Elasticity – Still Air Resonance Tests

Standard or Specification	Title
Leaflet 500/9	Aero-Elasticity – Flight Flutter Tests
Chapter 501	Requirements for Structural and Equipment Exposure to Noise and Vibration
Leaflet 501/3	Requirements for Structural and Equipment Exposure to Noise and Vibration – Data Analysis and Assessment
Chapter 1015	Flight Tests- Structures
Leaflet 1015/1	Structures – General Information
Leaflet 1016/1	Flight Vibration Survey

Standard or Specification	Title
MIL-HDBK-1530	**General Guidelines for Aircraft Structural Integrity Program**
5.1.2	Structural Design Criteria
5.1.2.1	Damage Tolerance and Durability Design Criteria
5.1.2.1.1	Damage Tolerance
5.1.2.1.2	Durability
5.1.2.2	Battle Damage Criteria
5.1.2.3	Repairability
5.1.3	Damage Tolerance and Durability Control
5.1.4	Selection of Materials, Processes and Joining Methods
5.1.5	Design Service Goal and Design Usage
5.1.6	Nondestructive Testing and Inspection (NDT/I)
5.2.1	Material and Joint Allowables
5.2.2	Loads Analysis
5.2.3	Design Service Loads Spectra
5.2.4	Design Chemical/Thermal Environment Spectra
5.2.5	Stress Analysis
5.2.6	Damage Tolerance Analysis
5.2.7.	Durability Analysis
5.2.8.	Aeroacoustic Durability Analysis
5.2.9	Vibrations Analysis
5.2.10.	Flutter Analysis
5.2.11	Mass Property Analysis
5.2.13	Weapons Effects Analysis
5.2.14	Design Development Testing
5.3.1	Static Tests
5.3.2.1	Selection of Test Articles
5.3.2	Durability Tests
5.3.3	Damage Tolerance Tests
5.3.4	Flight and Ground Operations Tests
5.3.5	Aeroacoustic Durability Tests
5.3.6	Flight Vibration Tests
5.3.7	Flutter Tests
5.3.9	Interpretation And Evaluation Of Results
5.4.1	Final Analysis
5.4.2	Strength Summary
5.4.3	Force Structural Maintenance Documentation
5.4.4	Loads/Environment Spectra Survey
5.4.5	Individual Aircraft Tracking
5.4.5.2	Tracking Analysis Method
5.5.1	Loads/Environment Spectra Survey

Standard or Specification	Title
AFGS 87221	**General Specification for Aircraft Structures**
3.1	Detailed Structural Design Requirements
3.2.4	Weight Requirements
3.2.5	Weight Distribution Requirements
3.2.14	Service Life and Usage requirements
3.2.16	chemical, thermal and climatic environments requirements
3.2.19	Detailed Materials And Processes Requirements
3.3	Design and Construction Parameters Requirements
3.4	structural loading requirements
3.4.1	Flight Loading Conditions Requirements
3.4.2	Ground Loading Conditions Requirements
3.6	Vibration Requirements
3.9	Structure Survivability – Nonnuclear Requirements
3.10.4	Stresses And Strains Requirements
3.11	Durability Requirements
3.11.12	Corrosion Prevention Requirements
3.12	Damage Tolerance Requirements
3.12.1	Flaw Sizes And Inspection Requirements
3.13.1	Data Acquisition Provision
4.1	Detailed Structural Design Verification
4.2.4	Weight Verification
4.2.5	Weight Distribution Verification
4.2.14	Service Life and Usage verification
4.2.16	Chemical, Thermal And Climatic Environments Verification
4.2.19	detailed materials and processes verification
4.3	Design and Construction Parameters Verification
4.4	Structural Loading Condition Verification
4.4.1	Flight Loading Conditions Verification
4.4.2	Ground Loading Conditions Verification
4.5	Durability Testing Verification
4.6, subpara (a)	Vibration Analysis
4.6, subpara (b)	Ground And Flight Vibration Testing
4.7	Aeroelastic Stability and subpara (a) Addresses Analysis
4.9	Structure Survivability – Nonnuclear Verification
4.10.4	Stresses And Strains Verification
4.10.5	Static Strength Verification
4.10.5.1	Development Tests – Strength
4.11	Discusses Durability Verification
4.11.1.2.1	Development Tests – Durability
4.11.1.2.2a	Durability Testing
4.11.12	Corrosion Prevention Verification
4.12	Damage Tolerance Verification
4.12.1	Flaw Sizes And Inspection Verification
4.12.2	Residual Strength And Damage Growth Limits (and Test Article Selection)

Standard or Specification	Title
FAR Part 23	Small Aircraft (less than 12,500 lb)
FAR Part 25	Large Aircraft
FAR Part 27 and 29	Rotorcraft
JAR Part 25	Aeroplanes
BCAR Section D	(Large) Aeroplanes
BCAR Section K	Light Aeroplanes
BCAR Section G	Rotorcraft
MIL-A-8860	General Specification for Airplane Strength and Rigidity (USN).
MIL-A-8861	General Specification for Airplane Strength and Rigidity, Flight Loads
MIL-A-8862	General Specification for Airplane Strength and Rigidity, Landing and Ground Handling Loads
MIL-A-8863	Airplane Strength and Rigidity, Ground Loads For Navy Procured Airplanes
MIL-A-8865	General Specification for Airplane Strength and Rigidity, Miscellaneous Loads
MIL-A-8866	General Specification for Airplane Strength and Rigidity, Repeated Loads and Fatigue
MIL-A-8867	Airplane Strength and Rigidity, Ground Tests
MIL-A-8870	General Specification for Airplane Strength and Rigidity, Flutter and Divergence
MIL-A-8892	General Specification for Airplane Strength and Rigidity, Vibration
MIL-A-8893	General Specification for Airplane Strength and Rigidity, Sonic Fatigue
MIL-D-8708	Demonstration Requirements for Airplanes
MIL-I 6870	Inspection Program Requirements, Nondestructive, for Aircraft and Missile Materials and Parts
MIL-S-8698	Structural Design Requirements – Helicopters
MIL-STD-210	Climatic Information to Determine Design and Test Requirements for Military Systems and Equipment
MIL-STD-1515	Fastener Systems for Aerospace Applications
MIL-STD-1568	Materials and Processes for Corrosion Prevention and Control in Aerospace Weapons Systems
MIL-STD-1587	Materials and Process Requirements for Air Force Weapon Systems *(Including Composite Material Requirements)*
MIL-STD-2069	Requirements for Aircraft Nonnuclear Survivability Program
MIL-HDBK-5	Metallic Materials and Elements for Aerospace Vehicle Structures
MIL-HDBK-17	Plastic for Aerospace Vehicles
MIL-HDBK-336	Survivability, Aircraft, Nonnuclear (Volumes 1 and 2)
AFSC DH 1-2	General Design Factors
AFSC DH 1-7	Aerospace Material
WL-TR-94-40152/3/4/5/6	Damage Tolerance Design Handbook

Blank Page

ASIP PART AND ELEMENT STANDARDS AND SPECIFICATION REFERENCE TABLE

PART I – DESIGN INFORMATION									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Structural Design Criteria	Part 2	5.1.2 5.1.2.1 5.1.2.2 5.1.2.3	3.1 4.1						MIL-A-8860 MIL-A-8861 MIL-A-8862 MIL-A-8865 MIL-A-8866 MIL-A-8870 MIL-A-8892 MIL-A-8893 MIL-S-8698 BCAR Section G – Rotorcraft, FAR Part 27 and 29 - Rotorcraft
Durability and Damage Tolerance Design Criteria	Leaflet 201/1, paras 3, 4 and 5; Leaflet 201/3; Leaflet 201/4	5.1.2.1 5.1.2.1.1 5.1.2.1.2 5.1.3	3.11 4.11 3.12 4.12						BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft
Corrosion control and prevention	Chapter 409, paras 6-22; Table 1; Leaflets 409/0-409/4	5.1.2.1.3	3.11.12 4.11.12	609	609	609	4-1.10	4-1,8	BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft

PART I – DESIGN INFORMATION									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Structural Build Quality	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	3.3 4.3	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Selection of Material, Processes and Joining Methods	Chapter 401; Leaflet 401/0; Chapter 402; Leaflets 402/0 – 402/7; Chapter 403; Leaflet 403/1; Leaflet 201/2	5.1.4	3.2.19 4.2.19	601, 603, 605, 613, 615	601, 603, 605, 613	601, 603, 605, 613, 615	1-2,4.9; 3-10,2; 3-1,2;4-12,2/4	1-2,4.8; 3-10,2; 3-12,2; 4-1,2	MIL-STD-1568 MIL-STD-1587 MIL-HDBK-5 AFSC DH 1-2 AFSC DH 1-7 MIL-STD-1515 MIL-HDBK-17 BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft
Design Service Life and Design Usage	Leaflet 201/1 paras 3, 4 and 5; Leaflets 201/3 – 201/4	5.1.5	3.2.14 4.2.14						BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft
Non-Destructive Inspection	Chapter 201, para 3; Leaflet 201/4	5.1.6	3.12.1 4.12.1						MIL-I 6870 BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft

PART II – DESIGN ANALYSES AND DEVELOPMENTAL TESTS									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Material and Joint Allowables	Chapter 401	5.2.1	3.2.19 4.2.19	613 615	613	613	4-1,2.3	4-1,2	DEF STAN 00-932 MIL-HBK-5 MIL-HDBK-17 MIL-STD-1587 BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft
Loads Analysis (External)	Part 2 Chapters 200, 202, 203 and 204	5.2.2	3.4 4.4	333 335 351 397 367 349 427	333 335 351 397 367 349 427	333 335 351 397 367 349 427 1503 1505 1507	3-2,2.2 3-2,4.2 and appendix 3-2,5.2 and appendix 4 3-2,4.1 3-2,4.2 3-2,2.7 7-2 and appendix	3-2,2.2 3-2 4-2.2 4-8 3-2,5.2 3-2,4.1 3-2,4.3 3-2,2.7 7-2,2	BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft
Design Service Loads Spectra	Leaflet 201/1 paras 3, 4 and 5 Leaflet 201/3 Leaflet 201/4	5.2.3							BCAR Section G – Rotorcraft FAR Part 27 and 29 - Rotorcraft

PART II – DESIGN ANALYSES AND DEVELOPMENTAL TESTS									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Design Chemical/ Thermal Environment Spectra	Does not contain detailed mandatory requirements. Some information in Leaflet 200/4.	5.2.4	3.2.16 4.2.16		Appendix C				BCAR Section G – Rotorcraft FAR Part 27 and 29 – Rotorcraft MIL-STD-210
Stress Analysis	Does not contain detailed mandatory requirements. Some information in Chapter 200	5.2.5	3.10.4 4.10.4	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	MIL-STD-210
Durability and Damage Tolerance Analysis	Leaflet 201/1 paras 3, 4 and 5 Leaflet 201/3 Leaflet 201/4	5.2.6 5.2.7	3.11 4.11 3.12 4.12	571	571	571	3-1,5.2 and appendix	3-1,3.4 and appendix 2	BCAR Section G – Rotorcraft FAR Part 27 and 29 – Rotorcraft WL-TR-94-40152/3/4/5/6
Aeroacoustic Durability Analysis	Leaflet 501/3	5.2.8	3.5 4.5	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	MIL-A-8870 MIL-A-8893

PART II – DESIGN ANALYSES AND DEVELOPMENTAL TESTS									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Vibrations Analysis	Leaflet 501/3	5.2.9	3.6 4.6	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	BCAR Section G – Rotorcraft FAR Part 27 and 29 – Rotorcraft MIL-A-8870 MIL-A-8892
Flutter Analysis	Chapter 500 Leaflet 500/1 Leaflet 500/2 Leaflet 500/3 Leaflet 500/4	5.2.10	4.7	629	629	629	2-10, 8	2-10, 6	BCAR Section G – Rotorcraft FAR Part 27 and 29 – Rotorcraft MIL-A-8870 MIL-A-8892
Mass Properties Analysis	Does not contain detailed mandatory requirements. Some information in Chapter 500, para 5.1	5.2.11	3.2.4 4.2.4 3.2.5 4.2.5	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Weapons Effects Analysis	Chapter 112 Leaflet 112/1	5.2.13	3.9 4.9	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	MIL-HDBK-336 MIL-STD-2069

PART II – DESIGN ANALYSES AND DEVELOPMENTAL TESTS									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Design Development Testing	Does not contain detailed mandatory requirements. Some information in Chapter 200 para 4 and 5 Leaflet 200/2 Leaflet 201/5 para 2 Leaflet 201/4, para 2	5.2.14	4.10.5.1 4.11.1.2.1	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	MIL-A-8870 MIL-A-8892 MIL-A-8893

PART III – FULL SCALE TESTING									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Static Tests	Does not contain detailed mandatory requirements. Some information in Chapter 200 para 5	5.3.1	4.10.5						BCAR Section G – Rotorcraft FAR Part 27 and 29 – Rotorcraft MIL-A-8867
Fatigue Tests									
Test Article	Leaflet 201/5, para 4.2 Leaflet 201/5	5.3.2.1	4.11.1.2.2a 4.12.2		571	571			BCAR Section G – Rotorcraft FAR Part 27 and 29 – Rotorcraft
Durability Tests	Leaflet 201/1, para 5	5.3.2 and sub-paras	4.11.1.2.2		571	571	para 3-1, 5.2 and appendix	para 3-1, 5.2 and appendix	
Damage Tolerance Tests	Leaflet 201/5, para 4.5	5.3.3	4.12.2						

PART III – FULL SCALE TESTING									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Flight and Ground Operations Tests	Chapter 1015 Leaflet 1015/1	5.3.4	3.4.1 3.4.2 4.4.1 4.4.2						BCAR Section G – Rotorcraft FAR Part 27 and 29 – Rotorcraft MIL-D-8708, para 3.5.3, 3.4.5, 3.7.1.2, 3.7.2.1 and 3.12 MIL-A-8860, para 3.10 and 3.14 MIL-A-8861 MIL-A-8862 MIL-A-8863, para 4.3 MIL-A-8865, para 4 MIL-A-8866, para 4 MIL-A-8867
Aeroacoustic Durability Tests	Chapter 501, para 4 Leaflet 1016/1	5.3.5	4.5 4.5.1, sub-para b	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	MIL-D-8708, para 3.12.6 MIL-A-8860, para 3.10 and 3.13 and 3.14

PART III – FULL SCALE TESTING									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Flutter and Vibration Tests	Chapter 500; para 7 Leaflet 500/1, paras, 5, 6, 7, 9; Leaflet 500/7 Leaflet 500/8 Leaflet 500/9 Chapter 501, para 4 Leaflet 1016/1	5.3.6 5.3.7	4.6, sub-para b 4.7 sub-para b (ground tests), sub-para c (flight test)	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	MIL-D-8708, para 3.12.6 MIL-A-8870 MIL-A-8892
Interpretation and Evaluation of Results	Does not contain detailed mandatory requirements	5.3.9	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	

PART IV – IN-SERVICE MANAGEMENT DATA PACKAGE									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Final Analysis	Does not contain detailed mandatory requirements. Some information in Chapter 201	5.4.1	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Strength Summary	Does not contain detailed mandatory requirements	5.4.2	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Aircraft Structural Integrity Management Plan	Does not contain detailed mandatory requirements	5.4.3	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Operational Loads Measurement	Chapter 201, para 4 Leaflet 201/6, para 3	5.4.4	3.13.1	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Usage Monitoring	Chapter 201, para 4 Leaflet 201/6, para 2	5.4.5	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	

PART IV – IN-SERVICE MANAGEMENT DATA PACKAGE									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Routine Structural Life Monitoring Program	Chapter 201, para 4 Leaflet 201/6, para 2	5.4.5.2	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Additional Requirements for Used Aircraft	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	

PART V – IN-SERVICE MANAGEMENT									
Element	**DEF STAN 00-970**	**MIL-HDBK-1530**	**AFGS-87221A**	**FAR Part 23 – Small Aircraft**	**FAR Part 25 – Large Aircraft**	**JAR Part 25 – Aeroplanes**	**BCAR Sect D – (Large) Aeroplanes**	**BCAR Sect K – Light Aeroplanes**	**Other Standards or Specifications**
Routine Structural Life Assessment Reporting	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Operational Loads Monitoring	Does not contain detailed mandatory requirements	5.5.1	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Usage Monitoring Data	Does not contain detailed mandatory requirements	5.5.2	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Structural Degradation Control Program	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	
Structural Deterioration Records	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	Does not contain detailed mandatory requirements	

SAMPLE DID FOR RECORD OF PRODUCTION BUILD QUALITY

1 IDENTIFIER: DID-RPBQ

2 TITLE: RECORD OF PRODUCTION BUILD QUALITY

1 DESCRIPTION

3.1 The Record of Production Build Quality (RPBQ) contains the production build quality records of the fatigue critical components of an aircraft, which could reduce, prevent or significantly affect the aircraft's future inspection program, rework or repair. An RPBQ is required for each aircraft delivered and the fatigue article aircraft (if applicable).

3.2 The Commonwealth will use the RPBQ for each aircraft to assess compliance of the delivered build quality of each aircraft with the acceptable initial flaw sizes and defect tolerances associated with the significant non-conforming manufacturing process, fabrication and assembly as supplied by the Contractor (or aircraft manufacturer). The RPBQ will also be used to support the subject aircraft in-service Aircraft Structural Integrity Program, as described in the ASIMP.

2 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 This Data Item is related to the following DID:

Aircraft Structural Integrity Management Plan (ASIMP), DID-ASIMP

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of the RPBQ which is required by the Contract/Statement of Work.

5 RPBQ CONTENT REQUIREMENTS

5.1 The RPBQ for each subject aircraft (including any fatigue article aircraft, if applicable) shall contain the production build quality records, which is to include the associated actions for all non-conforming hardware.

5.2 The RPBQ shall contain the description and disposition of fatigue critical items that meet one or more of the following criteria:

a. The item may significantly change the way the structure could be repaired.

b. The item may significantly change the way the aircraft would be serviced or maintained.

c. The item may significantly affect the post delivery inspection program for structural components.

Blank Page

SAMPLE DID FOR AIRCRAFT STRUCTURAL INTEGRITY DOCUMENTATION PACKAGE

1 IDENTIFIER: DID-ASIDP

2 TITLE: AIRCRAFT STRUCTURAL INTEGRITY DOCUMENTATION PACKAGE

3 DESCRIPTION

3.1 The Aircraft Structural Integrity Documentation Package (ASIDP) will be used by the Commonwealth to support the Type Certification Program conducted in accordance with the Approved Type Certification Plan, and the in-service Aircraft Structural Integrity Program for the subject aircraft, as detailed in the Aircraft Structural Integrity Management Plan (ASIMP).

3.2 The ASIDP also documents the results of the Structural Verification Program, conducted in accordance with the Approved Structural Verification Plan.

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following documents are related to this DID to the extent described herein:

Aircraft Structural Integrity Management Plan (ASIMP),	DID-ASIMP
Structural Verification Plan (SVP),	DID-SVP
Type Certification Plan	

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of the ASIDP as required by the Contract/Statement of Work.

4.2.2 The ASIDP shall include a title page containing, as applicable: document number; volume number; version number; security markings or other restrictions on the handling of the document; date of issue; document title; Contract number; organisation for which the document has been prepared; and, the name and address of the preparing organisation.

5 ASIDP CONTENT REQUIREMENTS

5.2 Type Certification

5.2.1 The ASIDP shall contain or reference all the structural integrity and design information and documentation required for type certification of the subject aircraft by the Commonwealth for those entries of the Certification Basis Matrix (provided as part of the Type Certification Plan) where the Commonwealth is identified as the certifying authority.

5.2.2 For each item of documentation provided, or referenced, the ASIDP shall indicate the entries in the Certification Basis Matrix against which that documentation is provided.

5.3 Structural Verification

5.3.1 The ASIDP shall contain a summary of the structural integrity documentation raised during the Contractor's Structural Verification Program.

5.3.2 The ASIDP shall identify each item of documentation used in the verification of the tasks in the Structural Verification Plan (refer to DID-SVP).

5.4 In-Service Support

5.4.1 The ASIDP shall contain the documentation and data required by the Commonwealth to conduct the in-service Aircraft Structural Integrity Program (ASIP) for the subject aircraft, in accordance with the procedures detailed in the Aircraft Structural Integrity Management Plan (ASIMP).

5.4.2 The ASIDP shall include, as a minimum, the following data and documentation relating to the delivered subject aircraft configuration:

a. Structural testing and loads data, including details of all finite element models developed for the determination of internal loads, stress analysis and aeroelastic analysis.

b. Structural design criteria for the aircraft, including the static load cases, the associated loads and the methods used to determine these loads.

c. Structural stressing reports.

d. Fatigue analyses performed on the aircraft components, including the fatigue design methodology used, associated S/N and crack growth data and any associated software used in the fatigue analysis.

e. Full-scale, component and coupon static and fatigue tests performed, including test load requirements, test spectra, test loads development procedures, and deficiencies and failures identified and test results.

f. Available aerodynamic loads and performance data, including wind tunnel test data and computer generated loads data.

g. Flight test data available for the aircraft, including flight measured loads, strain and performance data, calibrations performed and weapons release data (if applicable).

h. Propulsion loads and performance data.

i. Mass and centre of gravity breakdown of the aircraft in the configurations to be supplied to the Commonwealth.

j. Fatigue life monitoring and usage techniques developed for the aircraft, including details of the methodology (eg. S/N and/or crack growth data used) and details and listing of associated software.

k. All reports concerned with the validation of the Usage Monitoring and Operational Loads Monitoring systems identified in the ASIMP.

l. Environmental Degradation (including Corrosion Control) documentation.

m. Material properties, coatings and fastener systems data, including:

(1) details of the heat treatment and production standards used on all steels, aluminium and titanium alloys, and other non-ferrous alloys in structural components of the subject aircraft;

(2) details of the standards and specification used to select and apply organic paint systems and inorganic coating processes; and

(3) details of the standards and specifications used to select, assemble and maintain the subject aircraft fastener systems.

5.5 Document Control

5.5.1 The ASIDP shall also include a table detailing the following information for each document included or referenced in the package:

a. Document Reference Number;

b. Document Title;

c. Document Revision Number (if applicable);

d. Document Type; and

e. The Configuration Item to which the document applies.

Blank Page

SAMPLE DID FOR AIRCRAFT STRUCTURAL INTEGRITY MANAGEMENT PLAN

1 IDENTIFIER: DID-ASIMP

2 TITLE: AIRCRAFT STRUCTURAL INTEGRITY MANAGEMENT PLAN (ASIMP)

3 DESCRIPTION

3.1 The Aircraft Structural Integrity Management Plan (ASIMP) provides a basis for the Commonwealth's conduct and management of an in-service Aircraft Structural Integrity Program (ASIP) for the subject aircraft, to achieve the required design service life.

3.2 General requirements of the ASIMP are as follows:

a. To articulate the Certification Structural Design Standard (CSDSTD), which provides a basis for establishing, evaluating and substantiating the structural integrity of the aircraft structure (including the airframe strength, stiffness and damage tolerance and durability) to ensure the risk of operations remains within that defined in the CSDSTD.

b. To be the authoritative source of the instructions for continuing airworthiness (ICAs), by either; referencing the documents that define the TAR-authorised Safety-by-Inspection (SBI) program and/or life limited items, or defining these details in Volume 2 of the ASIMP.

c. To detail weapon system specific in-service management systems (particularly usage monitoring, structural condition data recording, fatigue management and environmental degradation management systems) required to provide continual assessment against the basis established, including the roles and responsibilities of the various agencies involved.

d. To define the allowable extent of structural degradation, in terms of cracking, corrosion or other structural damage, before impinging upon the structural warranty as defined in the Acquisition Contract.

e. To provide a basis for determining logistics planning requirements (eg. maintenance, inspections, spares, rotation of aircraft and future requirements).

f. To provide a high level plan detailing both the routine and development tasks required to ensure continued structural integrity.

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 A list of documents that form part of this Data Item are to be defined in this DID and should include, at a minimum, the following:

MIL-HDBK-1530B	Aircraft Structural Integrity Program, General Guidelines for
AAP 7001.053 (AM1)	Technical Airworthiness Management Manual (TAMM)
AAP 7001.054	Airworthiness Design Requirements Manual (ADRM)
SOI – Subject Aircraft	Statement of Operating Intent

4.1.2 This ASIMP DID is related to the following DSD/DIDs:

Engineering Support Services (ENGSERV),	DSD-ENGSERV
Aircraft Structural Integrity Documentation Package (ASIDP),	DID-ASIDP
Routine Usage Status Reports (RUSR),	DID-RUSR
Usage Assessment Report (UAR),	DID-UAR
Structural Condition Assessment Report (SCAR),	DID-SCAR
Fatigue Assessment Report (FAR),	DID-FAR

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of the ASIMP as required by the Contract/Statement of Work and Engineering Support Services DSD (refer to DSD-ENGSERV).

4.2.2 The ASIMP shall be unclassified. As such only unclassified information contained in the SOI shall be included in the ASIMP.

4.2.3 The ASIMP is to be reviewed and amended annually following Annual Planning. The annual update is to include, as a minimum, an updated ASIP Master Plan (refer clause 5.3). Required updates to the remaining sections are to be conducted at least once every three years.

4.2.4 Allowance is to be made for amendment and inclusion of data at the request of the Commonwealth. Once the draft ASIMP has been reviewed by the Commonwealth, a final version for DGTA approval is to be issued within 30 calender days.

4.2.5 The ASIMP must comply with the purpose and content described in AAP 7001.054.

4.2.6 The contractor shall seek and obtain DGTA approval of the ASIMP. ASI-DGTA or RWS-DGTA will provide guidance and limited assistance in the development of the ASIMP.

4.2.7 The layout of the ASIMP Volume 1 shall comply with clause 5 of this DID. The layout of ASIMP Volume 2 (if required) shall comply with clause 6 of this DID.

4.2.8 The detailed content of the ASIMP must inevitably reflect the requirements of the individual aircraft type. When preparing the ASIMP, the focus should be on articulating the design standard to be maintained and the systems, including roles and responsibilities, to maintain that standard.

5 ASIMP VOLUME 1 CONTENT REQUIREMENTS

5.1 General Volume 1 Structure and Content Requirements

5.1.1 The ASIMP Volume 1 shall consist of two sections. Section 1 is to document clauses 5.2 and 5.3, while Section 2 is to document clauses 5.4 to 5.16. Based on this description, the structure of the ASIMP Volume 1 is the following:

Section 1

- Chapter 1 – Introduction
- Chapter 2 – ASIP Master Plan

Section 2

- Chapter 1 – General Aircraft Description
- Chapter 2 – Aircraft Design Information
- Chapter 3 – Structural Verification
- Chapter 4 – Critical Structure
- Chapter 5 – Certification Information
- Chapter 6 – In-service Operations
- Chapter 7 – Usage Monitoring
- Chapter 8 – Condition Data Recording
- Chapter 9 – Fatigue Management
- Chapter 10 – Environmental Degradation Management
- Chapter 11 – Major Projects Information
- Chapter 12 – Structural Life Assessment
- Chapter 13 – Index of ASI Documents

5.2 Introduction (Section 1, Chapter 1)

5.2.1 This chapter is to provide an overview of the ASI management philosophy applicable to the subject aircraft, and high level details of the ADF approach to ASI management to set the scene for the specific subject aircraft ASI requirements. This chapter is to also include highlights of major ASI issues and provides details of the ASIP Manager for the subject aircraft.

5.3 ASIP Master Plan (Section 1, Chapter 2)

5.3.1 This chapter details the ASIP Master Plan, which lists what activities are required for the ASIP (tasks), justifies why each task needs to be performed, shows when each task needs to occur (schedule) and how each task is to be achieved (resources).

5.3.2 The quality of the ASIP is assured, in part, by routine planning which ensures that all AAP 7001.054 ASIP elements are addressed.

5.3.3 A Gantt chart should be included in this section, covering all high level ASIP tasks that are to be covered for the subject aircraft.

5.4 General Aircraft Description (Section 2, Chapter 1)

5.4.1 This chapter shall include a general description of the subject aircraft. The description should include historical development, the main operating features and roles and the physical and functional characteristics of the aircraft, with specific focus on the structure. This chapter should include general details on the structural arrangement, which should include supporting diagrams and pictures.

5.5 Aircraft Design Information (Section 2, Chapter 2)

5.5.1 This chapter is to provide details of the original aircraft structural design information, that is, the design standard(s) which form(s) the CSDSTD (the structural elements of the certification basis). In particular, the section shall identify the salient aspects of the CSDSTD that will enable AEOs, and others who design repairs or minor modifications for the type, to satisfy Regulation 3.5.4 of AAP 7001.053(AM1), which requires all structural repairs and modifications to conform to the CSDSTD. Accordingly, for each design element, a clear statement on the authoritative design standard, including the applicable revision status, and a reference to the appropriate source document that details satisfaction of the design requirement is to be included. This chapter is expected to reference sources of information with only salient aspects to be detailed herein. The elements that shall be addressed are:

a. **Aircraft design specification.** Provide details of the design specification(s).

b. **Certification structural design standard.** Provide summary details of the standard(s) that form the CSDSTD, including the revision status.

c. **Design philosophy.** Provide a brief description of the overarching design philosophy applied to the aircraft, specifically to what degree the structure is managed under a safe life, fail-safe and/or damage tolerance philosophy.

d. **Design service life and design usage.** A short summary of the design service life criteria and expected in-service design usage is required.

e. **Structural design criteria.** Provide details of the static strength criteria (load factors, minimum margin of safety where no test substantiation was carried out, etc.); crashworthiness design criteria; bird-strike design criteria; and fatigue requirements, including residual strength criteria. If the design standard was not met, the basis for certification is to be stated and an overview of the equivalent safety finding (civil) or deviations/waivers (military) from these standards provided. The agency that certified this element is to be stated.

f. **Fatigue analysis.** Provide details of any analysis carried out to substantiate the ability of the structure to comply with the specified design service life, the design spectra for this analysis and verification of the analysis results.

g. **Corrosion prevention and control.** State the corrosion prevention and control design standard(s) applied to the subject aircraft type. Details are to be provided on: design requirements for selection of material type, temper and form; manufacturing, surface finish and assembly processes and design features to exclude moisture and contaminating fluids and ensure suitable drainage. Provide an explanation of the processes to maintain corrosion prevention and control throughout the service life of the aircraft, including; the standards for the selection of corrosion

prevention finishes and corrosion prevention compounds; and the choice of structural and fuel tank sealants and surface finishes, including the requirements for their re-application.

h. **Structural build.** Data is required on acceptable flaws and defect tolerances associated with manufacturing, fabrication and assembly processes. Provide references to the permanent record of build quality, covering production non-compliances and how issues at production were processed. Critical structure is the key focus, with a summary to be included of any significant production non-conformities.

i. **Selection of and allowables for materials, joints and processes.** Provide details on the design standard(s) and design criteria.

j. **Non-destructive testing (NDT).** Provide details on: design standard, design criteria applied for critical structure; overall approach to assure adequate NDT of in-service structural components; the basis to assess NDT technique reliability; and an overview of the validation process applied to ensure that NDT procedures using new technology provide adequate reliability. NDT requirements peculiar to the subject aircraft are to be identified and the requirement for their uniqueness provided.

k. **Weapons effects.** Content should include design standard(s) and design criteria for ballistic damage; details of the design standard(s), and design criteria for battle damage repair. If the design standard was not met, the basis for certification is to be stated and an overview of the deviations/waivers from the standard(s) provided. The agency that certified this element is to be stated.

l. **Loads analysis.** Provide details on the design standard; design criteria, including flight and ground loads; Vn diagrams (with configuration details); airspeed-altitude diagrams; the loads validation process (eg. wind tunnel, simulation, flight test) and results of this. If the design standard(s) was not met, the basis for certification is to be stated and an overview of the equivalent safety finding (civil) or deviations/waivers (military) from the standard(s) provided.

m. **Service life, design and test spectra.** Provide a summary of the criteria used to determine the design service life and details of the usage spectra. This description shall cover, as a minimum, the planned usage, mission profiles and design service loads spectra as developed from the SOI and specification, as well as those used in the design of the manufacturer's baseline aircraft (if applicable). For test spectra, include details of the usage assumed, the source of loads information (eg. flight test, FEM etc.) and the development of the following: gust/manoeuvre loads, dynamic loading (buffet), ground and pressurisation loads. The testing information in this section relates to fatigue testing carried out for the subject aircraft type and any subsequent testing required for certifying the ADF subject aircraft type configuration.

n. **Stress analysis.** Content should include: design standards; design criteria; overview of analysis process (eg. FEM simulation, classical analysis, etc.); validation of analysis procedures, especially simulation (eg. comparison with data from flight test and/or design development testing); validation of analysis results; and differences to prior variants. If the design standard was not met, the basis for certification is to be stated and an overview of the deviations/waivers (military) from these standards provided. The agency that certified this element is to be stated.

o. **Aeroacoustic durability analysis, vibration and flutter.** Content for each should include: design standards (revision status to be stated); design criteria; analysis technique used and its validation (design analysis and development tests); verification of analysis results (for example, comparison with test results), and differences to prior variants. If the design standard was not met, the basis for certification is to be stated and an overview of the deviations/waivers (military) from these standards provided. The agency, which certified this element, is to be stated.

p. **Mass properties.** Provide details on: the centre of gravity envelope; weight information used in design (for example, maximum take-off weight, gross weight, maximum landing weight and zero fuel weight).

q. **Design development testing.** Content should include details of any supplemental development testing conducted, for example: to support a change of role, a performance enhancement or life extension.

5.6 Structural Verification (Section 2, Chapter 3)

5.6.1 This chapter shall include the following information:

a. **Static Tests.** A summary of any static tests (full-scale, sub-assembly and component), and the results of these tests, used to verify structural integrity of the subject aircraft, including static design margins and residual strength results/margins. Include details on the structural configuration tested.

b. **Fatigue Tests.** A summary of any fatigue tests (full-scale, sub-assembly and component), and the results of these tests, used to verify structural integrity of the subject aircraft. State any safety and scatter factors applied to the test results. Include details on the structural configuration tested.

c. **Other Tests.** The results of aeroacoustic, flutter and vibration tests made on full-scale and/or sub-assembly aircraft structures, in flight and on the ground, used to confirm the dynamic characteristics of the airframe.

d. **Analysis.** A summary of any anlysis or modelling used to support the structural verification of the subject aircraft. This shall cover new structure, any baseline structure that has been modified and any baseline structure for which the loads have been altered due to modifications.

e. **Interpretation and Evaluation of Results.** A summary of how existing verification results from the other variants support the subject aircraft role, configuration and environment. For regions of the structure which the manufacturer proposes be managed on either a safety-by-inspection or safe life basis, information on how analysis programs were validated must be included. Analysis programs include those used by the designer to set initial inspection thresholds, recurring intervals and the program supplied to the Commonwealth to track individual aircraft fatigue, be it for a SBI program or safe life.

f. **Documentation.** Documents which contain the test program, test description, test results and test interpretation shall be referenced in this section.

5.7 Critical Structure (Section 2, Chapter 4)

5.7.1 Provide an explanation of the definition of critical structure as applied to the subject aircraft and an explanation of the methods used to determine which items are critical, such as analysis, static test, fatigue test, flight test or in-service experience.

5.7.2 The ASIMP shall, as a minimum, contain information on the following:

a. A summary of structural details of the aircraft that are assessed as critical structure.

b. A summary of data supporting the assessment of all identified critical structure (whether from analysis, testing or in-service experience).

c. A summary of any elements of structure needed to bring the baseline subject aircraft to the Commonwealth required configuration, which are assessed as critical.

d. A summary of any elements of the baseline subject aircraft structure assessed as critical as a result of changes in the baseline aircraft necessary to bring the aircraft to the Commonwealth required configuration.

e. Reference the documents that contain the detailed, certified information from which the above summaries have been drawn, including the document(s) containing the Instructions for Continuing Airworthiness.

5.7.3 The details on the systems to manage primary or critical structure are not to be provided in this chapter (refer to the Fatigue Management and Environmental Degradation Management chapters). However,

historical details in support of individual locations deemed to be critical structure may be provided in this chapter.

5.8 Certification Information (Section 2, Chapter 5)

5.8.1 The ASIMP shall summarise the certification basis for the subject aircraft, including the amendment level of all applied airworthiness standards.

5.8.2 If the Commonwealth is acquiring a civil aircraft that has received prior certification from an internationally recognised Airworthiness Authority (eg. FAA, JAA or USAF) and is to be modified for ADF use, the following additional information is to be documented in the ASIMP:

5.8.3

a. Details of the original design specification of the baseline aircraft.

b. Details of the design standards applied to both the baseline subject aircraft and the modifications to the baseline subject aircraft to arrive at the certification basis for the post-modified subject aircraft configuration. If the standards are Contractor standards rather than airworthiness authority or military standards, then provide details of the approval of the Contractor standards by an airworthiness authority.

c. If the baseline subject aircraft are used or refurbished aircraft, then the Contractor should give details of the common structural standard to which the aircraft have been brought before conversion to the Commonwealth required configuration.

d. Details on any previous type certifications by other airworthiness authorities.

5.9 In-Service Operations (Section 2, Chapter 6)

5.9.1 This chapter shall include a summary of the aspects of the SOI relevant to ASI, including the revision status of the SOI. The chapter shall provide a clear definition of each distinct pattern of flying and the associated configuration and any other parameters relevant to fatigue consumption. The following shall also be included:

a. roles;

b. type of flight codes, including all information necessary to enable aircrew to categorise each mission when completing post flight documentation;

c. an outline of the process used to develop the type of flight codes;

d. mission mix, both forecast and historical (if unclassified);

e. fleet distribution (by base and operating Squadron(s)), including aircraft that have crashed, been retired or otherwise disposed of; and

f. information on other fleets, with identification of world leaders in respect of the relevant measures for fatigue accumulation (such as hours, landings, etc.).

5.10 Usage Monitoring (Section 2, Chapter 7)

5.10.1 The ASIMP shall, as a minimum, contain information on the following:

a. A description of the philosophy of the Usage Monitoring (UM) system and the Operational Loads Measurement (OLM) system for the aircraft, detailing how the systems support the assessment of fatigue and environmental degradation for the subject aircraft during its life-of-type.

b. A description of the type, extent, performance and role of the UM system. This shall briefly detail the elements of the system used to record, store and output the usage parameters that are deemed necessary in assessing the structural degradation of the subject aircraft. The parameters to be recorded and why those parameters were selected are to be articulated in this section.

c. A description of the type, extent, performance and role of the OLM system. This shall briefly detail the elements of the system used to record, store and output OLM data deemed necessary to support the fatigue degradation assessment of the subject aircraft. The locations chosen for recording OLM data, including diagrams as necessary, and the philosophy behind the selection of these locations is to be articulated in this section.

d. A brief description of the methods used to validate the UM and OLM systems.

e. A description of the calibration requirements of the UM and OLM systems.

f. A brief description of the methodology, and associated infrastructure, for processing UM and OLM data to provide inputs into fatigue management and environmental degradation management activities.

g. A description of the requirement for Routine Usage Status Reports (RUSR) and annual Usage Assessment Reports (UAR) – refer to DID-RUSR and DID-UAR.

5.11 Condition Data Recording (Section 2, Chapter 8)

5.11.1 Provide a description of the philosophy of the condition data system for the aircraft, where the system is used to record, store and process the condition data that describes the in-service structural degradation of the airframe and the repairs, rework and modification action carried out to address the degradation. Forms of structural degradation include corrosion, fatigue cracking, stress corrosion cracking and damage to composite structure due to impact, environmental attack or operational loading.

5.11.2 The ASIMP shall include the following details:

a. The forms of structural degradation that will be recorded during service.

b. The mechanism for capturing the structural degradation and the information that will be recorded, such as type, location, dimensions and proximity to critical structural locations or existing repairs.

c. The outputs to be provided and how these will be used to support the fatigue and environmental degradation systems described in the following sections (Fatigue Management, Environmental Degradation Management and Structural Life Assessments).

d. The proposed condition data recording system shall be compared against the requirements of Regulation 3.5.4 of AAP 7001.053(AM1). Where discrepancies exist, justification shall be provided.

e. Data analysis. This chapter should present relevant summary results of condition data recording programs, in support of assessments for both fatigue and environmental degradation. Relevant structural condition data from other operators (eg. tear down data) may be included.

f. A description of the requirement for an annual Structural Condition Assessment Report (SCAR) – refer to DID-SCAR.

5.12 Fatigue Management (Section 2, Chapter 9)

5.12.1 Describe the philosophy of the fatigue management system developed for the subject aircraft, including how it: meets the objective of fatigue management; utilises the necessary input data, and; meets the requirements of Regulation 3.5.4 of AAP 7001.053(AM1).

5.12.2 The ASIMP shall also include the following details:

a. A description of the fatigue management system for the subject aircraft. Provide a schematic that illustrates the key aspects of the system

b. A description of the methods used to validate the fatigue management system during certification and ensure it remains valid throughout the service life.

c. A description of the outputs from the fatigue management system.

d. A description of the methodologies and techniques used to generate the inspection intervals and/or safe factored lives summarised under the Critical Structure section that form the basis of the ICAs.

e. A description of the requirement for an annual Fatigue Assessment Report (FAR) – refer to DID-FAR.

5.12.3 **Specific management requirements.** In the case of individual structural items that are subject to specific management requirements, such as components where fatigue enhancement techniques (such as cold working and shot peening) have been used, details are to be provided in this chapter. The historical background to the identification of the individual locations should be provided in the Critical Structure section, with this chapter detailing the specific management requirements, including:

a. the structure to be managed;

b. the techniques to be used;

c. more detailed information, such as stress level at the treatment area in the absence of fatigue enhancement treatment; and

d. validation methods and results.

5.13 Environmental Degradation Management (Section 2, Chapter 10)

5.13.1 Describe the philosophy of the environmental degradation management system developed for the subject aircraft, including how it: meets the objective of environmental degradation management; utilises the necessary input data and; meets the requirements of Regulation 3.5.4 of AAP 7001.053(AM1). The objectives of environmental degradation management is to ensure that the strength, both static and fatigue, of all primary structure continues to meet the design standard. An environmental degradation management system utilises condition data and usage data to monitor, assess and adjust the environmental degradation management throughout the specified LOT.

5.13.2 The ASIMP shall also include the following details:

a. A description of the environmental degradation management system for the subject aircraft. Provide a schematic that illustrates the key aspects of the system.

b. A description of any Corrosion Prevention and Control Program (CPCP) developed to minimise corrosion problems throughout the specified LOT.

c. A description of any programs developed to minimise problems associated with the environmental degradation of composite structure and adhesively bonded structure throughout the specified LOT.

d. A description of the extent to which environmental factors are considered in the design of repairs provided in the Standard Repair Manual (SRM).

5.13.3 **Special Management Requirements.** In the case of individual structural items that are subject to specific management requirements, such as components where stress corrosion cracking continues to be a significant ongoing threat, details are to be provided in this chapter. The historical background to the identification of the individual locations should be provided in the Critical Structure section, with this section detailing the specific management requirements.

5.14 Major Project Information (Section 2, Chapter 11)

5.14.1 This chapter shall include a summary of major projects with a direct ASI relevance (such as fatigue tests or an acquisition project that has ASI implications, eg. new role equipment) and is to be separated into on-going, future and historical projects. This section shall describe the impact of the project on the ASI management of the subject aircraft type fleet and include a project outline, detail who is responsible for the project and a reference to the planning documentation for the project. For on-going projects, this section shall identify any tasks that arise out of the project that should be included in the ASIP plan. Where information is excessive, references to external documents containing the details of the project is recommended.

5.15 Structural Life Assessment (Section 2, Chapter 12)

5.15.1 A fundamental function of an Aircraft Structural Integrity Program (ASIP) is to conduct Structural Life Assessments (SLA). A SLA will establish the structural LOT, and compare it to the PWD. This section shall detail overall structural life management information, such as the design service life, the initially established structural LOT, the PWD and the economic LOT for this subject aircraft, where relevant.

5.15.2 The ASIMP shall also include the following details:

a. A description of how the specified design service life will be met and verified in order to gain an Australian Military Type Certification (AMTC).

b. A description of how the structural LOT will be continually monitored and verified throughout the specified LOT. This is to include how the outputs from the fatigue assessments and environmental degradation assessments are used in the SLA.

c. A description of the limiting factor or structural component that defines the achievable LOT.

5.16 Index of ASI Documents (Section 2, Chapter 13)

5.16.1 The ASIMP shall contain a list of documentation needed to support the in-service ASIP for the aircraft. For each document the list shall contain the number, title and version or approval date, as well as the source of any documents not available through normal Commonwealth channels. The documentation listed shall include all documents provided in the Aircraft Structural Integrity Document Package (refer DID-ASIDP).

Note: **Rotary Wing Aircraft.** The ASIMP Volume 1 structure and content for a rotary wing aircraft is different to the ASIMP Volume 1 for a fixed wing aircraft. The structure of the ASIMP Volume 1 for a rotary wing aircraft is the following:

Section 1

Chapter 1 – Introduction
Chapter 2 – Overall Plan
Chapter 3 – Usage Monitoring Plan
Chapter 4 – Condition Monitoring Plan
Chapter 5 – Plan to Manage Critical Structure
Chapter 6 – Plan to Manage Ongoing Projects
Chapter 7 – ASIP Review Plan

Section 2

Chapter 1 – General Aircraft Description
Chapter 2 – Aircraft Design Information
Chapter 3 – Structural Verification
Chapter 4 – Critical Structure
Chapter 5 – Certification Information
Chapter 6 – In-service Operations
Chapter 7 – Usage Monitoring
Chapter 8 – Condition Data Recording (and Environmental Degradation Management)
Chapter 9 – Power Train Structural Integrity Management
Chapter 10 – Major Projects Information

Chapter 11 – Index of ASI Documents

In addition to the guidance provided in this Annex, the PO or SPO is to seek guidance from RWS-DGTA pertaining to the specific content requirements for a rotary wing aircraft ASIMP Volume 1.

6 ASIMP VOLUME 2 CONTENT REQUIREMENTS

6.1 General Volume 2 Structure and Content Requirements

6.1.1 The ASIMP Volume 2 shall be divided into four chapters, as detailed in clauses 6.2 to 6.5. The structure of the ASIMP Volume 2 is the following:

Chapter 1 – Introduction
Chapter 2 – Background
Chapter 3 – Structural Inspection Program
Chapter 4 – Structural Life Limited Items

6.2 Introduction (Chapter 1)

6.2.1 This chapter provides the scope and content of ASIMP Volume 2, as well as providing a brief overview of the fatigue management requirements necessary to ensure continued structural airworthiness of the subject aircraft fleet.

6.3 Background (Chapter 2)

6.3.1 This chapter provides the detailed background behind the structural inspection program, the interrelationship of the UM system (eg. HUMS if applicable) and structural life limited components.

6.4 Structural Inspection Program (Chapter 3)

6.4.1 This chapter articulates the specific structural locations and the attendant inspection requirements that comprise the structural inspection program for the Commonwealth subject aircraft fleet. Specific inspection requirements for sub-fleets or individual aircraft are to be included in this chapter.

6.4.2 An example of the level of detail that is to be promulgated in this chapter for individual structural inspection locations is provided at Appendix 1. The salient aspects that are to be documented are the basis for the inspection program and the details of the inspection program as implemented in the Technical Maintenance Plan (or equivalent document).

6.4.3 For each individual structural location, the resource and manhour requirements for each inspection requirement are also to be provided. Sufficient detail is to be provided to enable the Commonwealth to determine the cost of the inspection of each structural location as an independent inspection activity, or as part of a major servicing.

6.5 Structural Life Limited Items (Chapter 4)

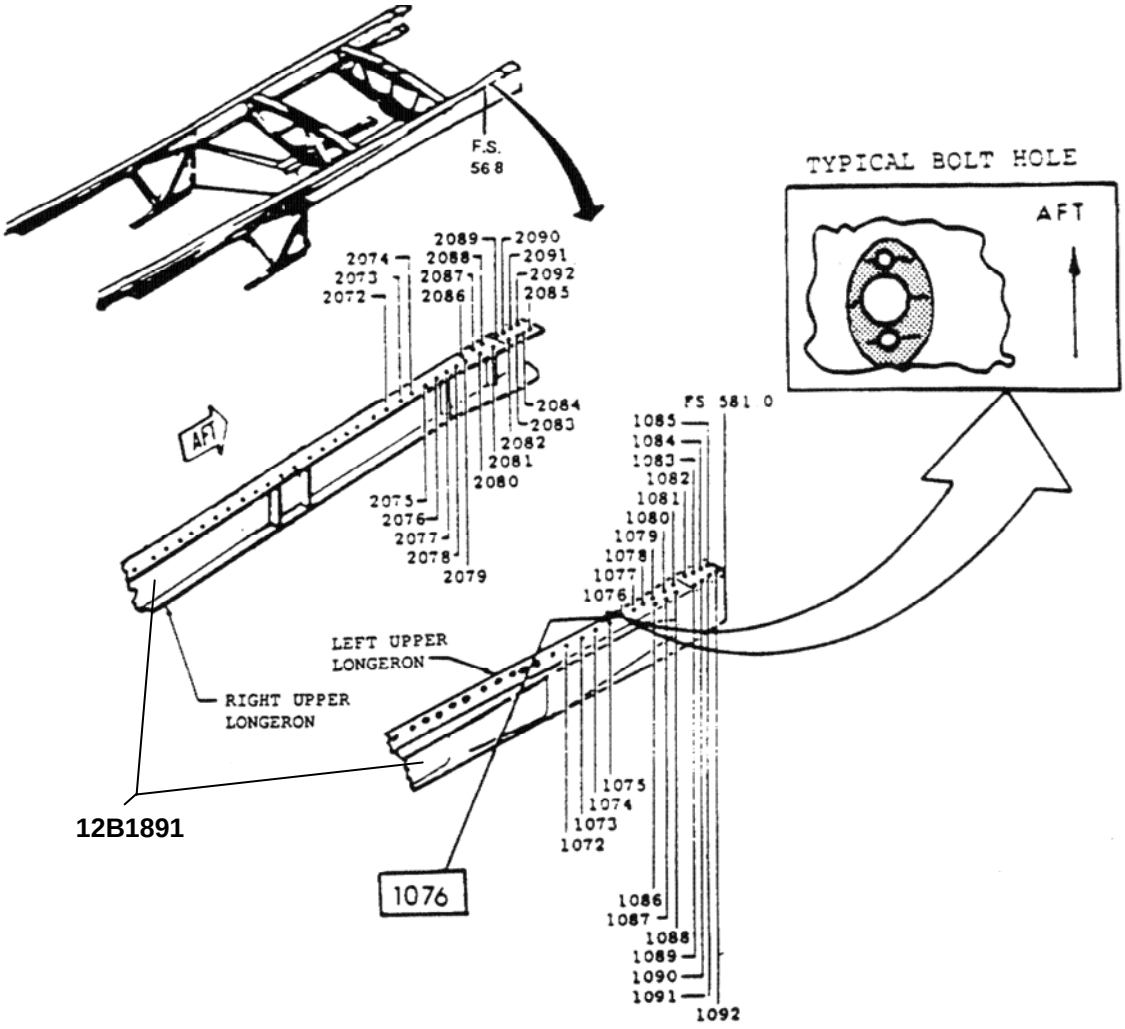
6.5.1 This chapter articulates the specific structural locations that are life-limited for the Commonwealth subject aircraft fleet.

Note: **Rotary Wing Aircraft.** For rotary wing aircraft acquisition projects, the PO or SPO is to seek guidance from RWS-DGTA pertaining to the requirement (and specific content) for an ASIMP Volume 2.

Appendix:

1. Example of the Level of Detail to be Provided for Structural Inspection Programs

EXAMPLE OF THE LEVEL OF DETAIL TO BE PROVIDED FOR STRUCTURAL INSPECTION PROGRAMS



CONTROL AREA:	PN 12B1891 Fastener Holes 1072-1092 and 2072-2092
CONTROL POINT:	Overwing Longeron Fastener Hole # 1076 at F.S. 568.3
PART NUMBER:	12B1891
APPLICABILITY:	F-111A, F-111C, F-111G

Figure 11F1–1 Location Identifier (eg DI 19)

Table 1.1–F1–1 Basis for Inspection

INTERVAL:	Maximum interval authorised for this location
PROCEDURE TYPE:	NDT technique
Andi:	Andi for associated NDT inspection
CRITIAL LOADING:	Provide details of critical loading case and, if appropriate, if LLS or 1.2MSS is utilised to set interval.
Acrit:	Crack size associated with critical loading case.
REFERENCE:	Provide reference for source of inspection interval and associated details. May be OEM report or an ASI-DGTA engineering review.
COMMENTS:	Provide any comments specific to management of this location eg. current analyses are insufficient for management of this location.
AMENDED INSPECTION BASIS (INDIVIDUAL AIRCRAFT)	List any aircraft that may have amended inspection intervals due to repairs or otherwise.

Table 1.1–F1–2 Inspection as Implemented by TMP

INTERVAL:	Actual interval called out in TMP
PROCEDURE TYPE:	NDT technique
INSPECTION LEVELS:	Servicing level to be listed.
PROCEDURE REFERENCE:	Reference to the –36 specific procedure

SAMPLE DID FOR STRUCTURAL VERIFICATION PLAN

1 IDENTIFIER: DID-SVP

2 TITLE: STRUCTURAL VERIFICATION PLAN

1 DESCRIPTION

3.1 The Structural Verification Plan (SVP) details the scope, objectives and schedule of activities to be performed by the Contractor in the Structural Verification Program to:

a. verify the structural design of the subject aircraft structural configuration;

b. evaluate the effect of the structural design on the structural life assessment of the subject aircraft; and

c. conduct any additional structural testing and analysis required to support the subject aircraft Type Certification Program.

3.2 The results and products of the Structural Verification Program are to be included in the Aircraft Structural Integrity Documentation Package.

2 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following documents are referenced in this DID:

Aircraft Structural Integrity Document Package (ASIDP), Type Certification Plan — DID-ASIDP

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of the SVP, which is required by the Contract/Statement of Work.

4.2.2 All certification data will be available to the Commonwealth for review but will remain the property of the aircraft manufacturer.

5 SVP CONTENT REQUIREMENTS

5.1 Requirements Verification

5.1.1 The SVP shall provide:

a. A description of the structural configuration of the subject aircraft.

b. Summaries of the test and analysis methods to be used to verify compliance of the subject aircraft with the structural design requirements of the subject aircraft specification.

c. A description of the additional structural testing, component testing and analysis that has been carried out, or is proposed to be carried out, to support the structural life assessment of the subject aircraft, including analytical and test scatter factors;.

d. A description of the flight loads verification program.

e. Summaries of the test and analysis methods to be used to verify the validity of the data collected by usage monitoring (UM) and operational loads monitoring (OLM) systems and any data processing software that is resident on the on-board systems, if applicable, including:

(1) a description of the methods to be used to calibrate all the sensors associated with the UM and OLM systems;

(2) a description of strain gauge installation procedures; and

(3) the methods to be used to qualify the on-board data recording and storage systems; and

f. summaries of the test and analysis methods and processes to be used to verify the validity of fatigue data processing systems to be used with the subject aircraft support program/facility, if applicable.

Note: The results of the Structural Verification Program are to be included in the Aircraft Structural Integrity Documentation Package, provided in accordance with DID-ASIDP.

5.2 Type Certification

5.2.1 The SVP shall include a description of the structural testing, component testing and analysis to be performed in support of the Type Certification Program, and shall indicate the entries in a Certification Basis Matrix, against which the testing and analysis is being performed.

5.3 Schedule

5.3.1 The SVP shall provide a schedule, consistent with the overall acquisition schedule, for the conduct of the Structural Verification Program and include:

a. the key activities to be carried out during the program;

b. the scheduling, sequencing and relationship of these activities; and

c. identification of key milestones.

5.4 Organisation

5.4.1 The SVP shall include a description of the organisation(s) responsible for the planning, conduct and reporting of structural verification activities.

5.4.2 The SVP shall identify the person(s) responsible for managing the Structural Verification Program and state their experience and qualifications.

5.4.3 The SVP shall identify the person(s) involved in the execution of each Structural Verification Program activity, including reporting responsibilities.

5.4.4 The SVP shall identify the scope of Engineering Authority assigned to persons involved in the Structural Verification Program.

SAMPLE DSD FOR ENGINEERING SUPPORT SERVICES – ASI ASPECTS

1 IDENTIFIER: DSD-ENGSERV

2 TITLE: ENGINEERING SUPPORT SERVICES – ASI ASPECTS

3 DESCRIPTION

3.1 This DSD describes the Engineering Support Services that shall be conducted by the Contractor's Engineering Support Element (ESE) in order to support the Aircraft Structural Integrity Management program and ensure the structural airworthiness of the subject aircraft fleet.

3.2 Aircraft Structural Integrity Management describes the program that is put in place to ensure that the airframe is able to operate safely, in accordance with the Statement of Operating Intent (SOI), for the life-of-type (LOT) of the aircraft.

3.3 This Engineering Support Services DSD is the hierachal document that defines the overall framework of the ASI management and engineering responsibilities of the TLS Contractor. The specific ASI management, engineering support and reporting requirements are documented in separate Data Item Descriptions (DIDs), which are subordinate to this DSD.

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following documents form part of this DSD to the extent described herein:

DI(G) LOG 8-15	Regulation of Technical Integrity of ADF Materiel
DI(G) OPS 2-2	ADF Airworthiness Management
AAP 7001.048	ADF Airworthiness Manual
AAP 7001.053 (AM1)	Technical Airworthiness Management Manual (TAMM)
AAP 7001.054	Airworthiness Design Requirements Manual (ADRM)
AAP 7001.060-4 (AM1)	CAMM2 Manual Authorised Engineering Organisation
AAP 7001.055	Support and Test Equipment Through Life Support Manual
AAP 7001.038-2-1	Maintenance Requirements Determination (MRD) CAPLOG Procedures Manual
SOI – Subject Aircraft	Statement of Operating Intent

4.1.2 The following Data Items are subordinate to this DSD and shall be delivered by the contractor:

Aircraft Structural Integrity Management Plan (ASIMP),	DID-ASIMP
Health and Usage Monitoring System Validation Plan (HUMSVP),	DID-HUMVSP
Routine Usage Status Reports (RUSR),	DID-RUSR
Usage Assessment Report (UAR),	DID-UAR
Structural Condition Assessment Report (SCAR),	DID-SCAR
Fatigue Assessment Report (FAR),	DID-FAR

4.2 Scope of DSD

4.2.1 This DSD describes the Engineering Support Services that the Contractor shall provide to support and ensure the structural airworthiness of the subject aircraft fleet. This DSD describes the following:

a. Engineering Support Services that the Contractor shall conduct;

b. Embedded Commonwealth personnel that the Contractor shall employ within their ESE; and

c. Constraints under which the ESE will conduct and manage the Engineering Support Services.

5 ENGINEERING SERVICES

5.1 Contractor Engineering Responsibilities

5.1.1 The Contractor shall manage and conduct all Engineering Support Services for the subject aircraft system, with the exception of Engineering Support Services that will be an ADO responsibility (refer clause 5.2).

5.1.2 The Contractor shall manage and conduct Engineering Support Services for the subject aircraft system in accordance with the Engineering Documentation listed at clause 5.3.

5.1.3 The Contractor shall arrange to develop and maintain a specification for the production and control of the reports required by clause 4.1.2. The specification shall be subject to review and acceptance by the Commonwealth.

5.1.4 DGTA provides overall program management of the reporting requirements. The Contractor is responsible for the project management of routine reporting and is to ensure tasking is in place in a timely manner for actioning of all requirements.

5.1.5 The Contractor shall establish a change process for the specifications developed in clause 5.1.3.

5.2 ADO Engineering Responsibilities

5.2.1 The Engineering Support Services to be conducted by the applicable ADO AEO are to be defined and listed in this part of the DSD.

5.3 Engineering Documentation

5.3.1 The Contractor's ESE shall conduct Engineering Support Services in accordance with:

a. the technical policies and publications listed in clause 4.1.1; and

b. the approved plans/specifications that form the set of required Data Items (refer clause 4.1.2).

5.4 Aircraft Structural Integrity Management

5.4.1 The Contractor shall be responsible for the establishment and maintenance of a system for the management of Aircraft Structural Integrity (ASI) for the subject aircraft.

5.4.2 The Contractor shall be responsible for the management and conduct of the subject aircraft ASI Program (ASIP).

5.4.3 In managing and conducting the subject aircraft ASIP, the Contractor shall, as a minimum, conduct the following routine activities:

a. Conduct annual planning to identify and prioritise ASIP tasks, responsible agencies and resources required.

b. Review and amend the subject aircraft ASI Management Plan (ASIMP) on an annual basis, and obtain DGTA approval of the ASIMP and associated ASIP in accordance with AAP 7001.053 (AM1).

c. Organise and chair annual, in-country ASI Working Groups (ASIWG), to which Commonwealth and contracted IV&V agents shall be invited.

d. Produce the written ASI submission to the annual subject aircraft Airworthiness Board (AwB), with input from ASI-DGTA, and deliver the ASI presentation to the AwB.

e. When requested, provide ASI advice to the subject aircraft Weapon System Management Committee.

5.4.4 The Contractor shall establish and maintain a robust, in-country organisation for the management and conduct of the subject aircraft ASIP.

5.4.5 The Contractor shall provide in-country access to adequate ASIP information (design, verification, and in-service usage/loads monitoring and condition) for the life of the aircraft.

5.4.6 The Contractor shall provide access to all design and certification data for the life of the aircraft.

5.4.7 The Contractor shall, upon request, provide access to data, processes, assumptions, executable software and other executable tools used in both the development and in-service modification of structural inspection intervals and structural life limits, sufficient to enable independent verification and validation.

5.4.8 The Contractor shall, upon request, release any defective, cracked or non-conforming product to the Commonwealth for independent forensic investigation and analysis.

5.4.9 The Contractor shall allow for the embedding of one Commonwealth employee (DSTO or ADF) in the in-country ASIP management organisation for periods of up to 24 months.

5.4.10 The Contractor shall accommodate DSTO and/or other contracted third party IV&V agencies acceptable to the Contractor and Commonwealth, throughout the life of the aircraft, as required by the Commonwealth.

5.4.11 The subject aircraft ASIMP is to be delivered as a System Acquisition Contract (SAC) Deliverable Item and will be approved by the relevant Commonwealth Authority in accordance with AAP 7001.053 (AM1). The subject aircraft ASIMP shall form part of the AEO application.

5.4.12 The in-service ASIMP shall be an evolution of the data and management plans delivered under the SAC.

5.4.13 If the Contractor believes that a new or significantly amended ASIMP from that delivered as part of the SAC is required to describe the evolution that this document shall undertake to meet the in-service requirements, the Contractor shall state this within their Engineering Management Plan (CEMP).

5.4.14 The subject aircraft ASIMP shall identify and describe (or explicitly reference) the Contractor's methodologies and associated processes for managing and conducting the subject aircraft ASIP.

5.4.15 The subject aircraft ASIMP shall describe (or explicitly reference) the Contractor's Organisation, Data, Facilities, Equipment and Tools that the ESE shall use to manage and conduct the subject aircraft ASIP.

5.4.16 The documents listed at clause 4.1.1 are standards, policy and regulations applicable to ASI and ASIP management. The Contractors shall describe how the ESE shall comply with the ASI and ASIP management requirements within the documents listed at clause 4.1.1.

5.4.17 The Contractor shall justify the need to deviate from any regulation or guidance, within the documents listed at clause 4.1.1 , which are relevant to ASI and ASIP management.

5.4.18 The ASIMP shall describe how the Contractor shall comply with all regulations in the AAP 7001.053 (AM1) relevant to ASI.

5.4.19 The ASIMP shall describe how the Contractor shall comply with the guidance documented in AAP 7001.054 for ASI. This shall include the ASIP management end objectives detailed.

5.4.20 Where necessary, the Contractor shall document subordinate ASIMPs and interfaces with other plans and supporting disciplines (such as Software, Human Engineering and Training) listed in the AAP 7001.054.

5.4.21 If the Contractor intends to comply with a document other than those listed at clause 4.1.1 then the Contractor shall identify the document and describe the relationship with the document listed and how it will be applied as part of the subject aircraft ASIP.

5.4.22 The Contractor shall describe any additional Operational Performance Monitoring and Diagnostics System ASI Management activities or requirements that shall be conducted in support of the subject aircraft system which are not covered in the document listed at clause 4.1.1. The Contractor shall describe the manner in which these additional activities will be managed and how they will form part of the subject aircraft ASIP.

5.5 Structural Condition Monitoring

5.5.1 The Contractor shall conduct, or arrange for the conduct as detailed in this DSD, structural condition monitoring for the subject aircraft and its associated support and reporting systems for condition data.

5.5.2 In conducting structural condition monitoring for the subject aircraft, the Contractor shall collect, record, store, assess/trend and report structural condition data and associated logistics data.

5.5.3 To meet the regulatory requirements detailed in AAP 7001.053 (AM1) and maintain airworthiness, the Contractor shall, as a minimum, conduct structural condition monitoring for all defects, inspections, repairs and modifications affecting critical structure.

5.5.4 The Contractor shall make provisions for the storage of all raw structural condition data as well as any processed data. Data shall be stored for the life of the contract and provided to the Commonwealth on request or as directed by this DSD and subordinate DIDs.

5.5.5 The Contractor shall provide a Deeper Maintenance Report (DMR) within one month of each Deeper Maintenance (DM) activity, in accordance with the requirements of the DID-DMR.

5.5.6 The Contractor shall conduct a Structural Condition Assessment (SCA) on an annual basis, and provide a SCA Report (SCAR) in accordance with the requirements of the DID-SCAR.

5.5.7 The SCAR shall be delivered in conjunction with the Usage Assessment Report (refer DID-UAR).

5.6 Usage Monitoring

5.6.1 The Contractor shall provide, or arrange for provision as detailed in this DSD, usage monitoring of the subject aircraft fleet.

5.6.2 In conducting usage monitoring for the subject aircraft, the Contractor shall collect, record, store, assess/trend, and report usage data as obtained from the Health and Usage Monitoring System (HUMS), the Operational Loads Measurement System (OLMS), EE500 sheets, EE360 sheets and CAMM2.

5.6.3 The Contractor shall make provisions for the storage of all raw HUMS and OLMS usage data. Data shall be stored for the life of the contract and provided to the Commonwealth on request or as directed by this DSD and subordinate DIDs.

5.6.4 The Contractor shall provide Routine Usage Status Reports (RUSR) on a quarterly basis in accordance with the requirements of the DID-RUSR.

5.6.5 The Contractor shall conduct a Usage Assessment (UA) on an annual basis and provide a UA Report (UAR) in accordance with the requirements of the DID-UAR.

5.6.6 The UAR shall be delivered in conjunction with the Structural Condition Assessment Report (SCAR).

5.7 Fatigue Management

5.7.1 The Contractor shall conduct, or arrange for the conduct as detailed in this DSD, fatigue management of the subject aircraft and its associated support and reporting systems, as directed in the subject aircraft ASIMP.

5.7.2 The Contractor shall maintain the integrity of the Fatigue Management System, including the HUMS and OLMS, and instigate any changes and improvements considered necessary to ensure the systems support

the generation of accurate fatigue damage accrual information for the subject aircraft. These changes cannot be made without the express permission of DGTA, who will retain approval and authorisation responsibility for the ASIMP.

5.7.3 The Contractor shall establish a change process for changes to the fatigue management system and its support elements.

5.7.4 The Contractor shall monitor the fatigue accrual and condition to enable structural LOT determinations and planned withdrawal date (PWD) feasibility assessments.

5.7.5 As required, the Contractor shall provide education and ongoing training to the aircraft operating Squadron(s) agencies performing HUMS and OLMS data collection.

5.7.6 The Contractor shall conduct a Fatigue Assessment (FA) on an annual basis, and provide a FA Report (FAR) in accordance with the requirements of the DID-FAR.

5.8 Health and Usage Monitoring System Validation

5.8.1 The Contractor shall conduct, or arrange for the conduct of, as detailed in this DSD, validation of the Health and Usage Monitoring System (HUMS) for the subject aircraft and the supporting systems.

5.8.2 In conducting the HUMS Validation (HUMSV), the Contractor shall validate the HUMS, the Operational Loads Measurement System (OLMS) and any other system used to determine the health and usage of the subject aircraft airframe, propulsion system or dynamic components.

5.8.3 The Contractor shall provide a plan for the HUMSV, in accordance with the requirements of the DID-HUMSVP (HUMSV Plan). The plan shall be subject to review and approval by the Commonwealth. *A DID-HUMSVP is provided in Section 2, Chapter 19 (Annex B) of the AAP 7001.054 ADRM.*

5.9 Employment of Embedded Commonwealth Personnel

5.9.1 Where the Commonwealth provided Embedded Personnel to be employed within the ESE, these personnel are to be employed in accordance with the associated personnel DSD for this Contract and the approved Duty Statement (agreed between the Contractor and the Commonwealth).

5.10 Constraints

5.10.1 Deployment of Contractor Personnel

5.10.1.1 Contractor Personnel shall be deployed on exercises and to an AO by exception only. It is not envisaged that any Contracted personnel within the ESE shall deploy to an AO.

5.10.2 CAMM2

5.10.2.1 The Commonwealth will provide the Contractor with on-line access to CAMM2, if CAMM2 is mandated as the primary lifing tool by the Commonwealth. The following requirements will then also apply.

5.10.2.2 CAMM2 shall be used as the primary tool for asset and maintenance management of the aircraft, spares and common-fit items.

5.10.2.3 The Contractor shall maintain the Engineering data within CAMM2 in accordance with AAP 7001.060-4 (AM1) CAMM2 Manual Authorised Engineering Organisation.

5.10.2.4 All CAMM2 System Management Centre (SMC) generated CAMM2 Action Notices (CANs) shall be complied with.

5.10.2.5 The Contractor shall warrant the data provided in CAMM2 in accordance with the associated Conditions of Contract.

5.10.2.6 The Contractor shall make available personnel, documentation, tools, data and access to the facilities required for DGTA to conduct internal and external CAMM2 audits.

5.10.2.7 Any tool supplied to augment CAMM2 shall be supplied and maintained by the Contractor. The Contractor shall provide the Commonwealth with the tools and training required to access this data.

5.10.2.8 The Contractor shall ensure that the AMS LSAR database is updated and maintained in accordance with the requirements of AAP 7001.038-2-1 Maintenance Requirements Determination (MRD) CAPLOG Procedures Manual.

5.10.3 Commonwealth Access to Data

5.10.3.1 The Contractor shall provide the Commonwealth with access on request to all ESE data considered to be part of the baseline data items. The Contractor shall provide the Commonwealth with the tools required to access this data.

5.10.3.2 The Contractor shall make available to the Commonwealth, access to the facilities, the personnel, documentation, tools and data required to conduct AEO compliance assurance audits in accordance with clause 5.1.

5.11 ESE Master Schedule

5.11.1 The Contractor shall maintain (and provide to the Commonwealth) a schedule of planned ESE activities, projecting future work effort for a period of not less than five years, or until the end of the Contract, when that is less than five years.

5.11.2 The Contractor shall provide to the Commonwealth a detailed schedule of planned ESE activities for a period of not less than one year, or until the end of the Contract, when that is less than one year.

5.12 Performance Measurement

5.12.1 The Contractor’s performance of Engineering Support Services shall be measured against a Contractor and Commonwealth agreed list of documented Health Measures, which shall be reviewed by DGTA at an agreed frequency. Performance measurement will focus on efforts made by the Contractor to improve structural airworthiness whilst optimising the availability and cost to the Commonwealth.

5.12.2 Engineering Support Services for the subject aircraft system that shall be measured include the following (tailor as appropriate):

a. Airworthiness compliance activities (ie. number of significant ASI related CARs raised).

b. Efficiency of the ASI program (including the ASI related inspection program).

c. Timely completion and quality of ASI reporting requirements (ie. Routine Usage Status Reports, Structural Condition Assessment Reports and Fatigue Assessment Reports).

d. Timely completion and quality of the required review of the ASIMP Volumes 1 and 2 (and subsequent issue of the revised document(s)).

e. Timely achievement of recommendations raised in ASI reporting documents (ie. Routine Usage Status Reports, Structural Condition Assessment Reports, Fatigue Assessment Reports, Ageing Aircraft Audits and Structural Life Assessments) or during ASI forums (ie. ASI Working Groups and Airworthiness Boards).

f. Reliability of usage monitoring and operational loads measurement systems and processes.

g. Capture rates of usage, operational loads measurement and condition data.

h. Number (and duration) of unscheduled aircraft non-serviceability events due to ASI related issues or inspection requirements.

i. Number of ASI related flight or life restrictions on the aircraft.

j. Aircraft time to make serviceable (TMS) due to corrosion repairs.

k. Costs of unscheduled ASI related repairs and/or refurbishment.

l. Success of any repair, modification and refurbishment carried out to improve safety, availability and/or cost of ownership.

Blank Page

SAMPLE DID FOR DEEPER MAINTENANCE REPORT

1 IDENTIFIER: DID-DMR

2 TITLE: DEEPER MAINTENANCE REPORT

3 DESCRIPTION

3.1 The Deeper Maintenance Report (DMR) provides a summary of the changes to and the status of each aircraft's structural condition post deeper level maintenance activities.

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 This Data Item is subordinate to the following DID to the extent described herein:

Structural Condition Assessment Report (SCAR), DID-SCAR

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of a DMR as required by the Contract/Statement of Work.

4.2.2 The Contractor shall develop and maintain a specification for the production and control of the DMRs. The specification shall be subject to review and approval by the Commonwealth.

4.2.3 The Contractor shall provide a DMR within one month of the completion of each Deeper Maintenance (DM) activity for all subject aircraft.

4.2.4 For all reports required by this DID, one hard copy of the report shall be provided to the SMM (of the aircraft operational Squadron(s)) and one electronic copy of the report shall be provided to the CENGR (of the subject aircraft SPO) and ASI-DGTA. The electronic copies shall be in an open format (such as Microsoft Word and Excel) that allows extraction and amendment of data and not a locked format (such as pdf).

4.2.5 The reports generated by this DID shall be input data for Structural Condition Assessments (refer DID-SCAR).

5 DMR CONTENT REQUIREMENTS

5.1 The DMR shall summarise the level and detail of structural work undertaken. The report shall be split into a minimum of three sections, with one for general comment and summary, a second for Primary Structural Elements (PSE) and the third for other structure. Within each section, sub-sections shall be used to identify individual damage sources such as corrosion, mechanical damage, fatigue cracking, delamination, etc.

5.2 The report shall provide a summary of the aircraft utilisation since the previous DM servicing and note any unique events that may have affected structural condition since the last DM servicing.

5.3 The report shall provide a summary of known and potential hotspots and any actions recommended for mitigating the risk of significant damage findings for these areas.

5.4 The report shall summarise corrosion findings, any mechanical damage or cracking by providing the following information (as a minimum) for both metallic and non-metallic elements:

a. Defect type and size.

b. Cause of defect (if known).

c. Any associated damage to other structure or component.

d. Location on aircraft.

e. Part number and serial number (if appropriate).

f. Material.

g. Surface finish (blueprint and after rework).

h. Method of repair, including reference.

i. Inspection requirement during which defect was found (if any).

j. Time in service (flight hours, landings and calender time).

k. Time since last inspection (if any).

l. Any unusual activity during defect removal (such as obvious preload, misaligned fastener holes or fractured fasteners); and

m. Any proposed new maintenance requirement as a result of repair action or finding.

5.5 For any PSE found with corrosion, mechanical damage or cracking, the report shall also provide a picture (photograph) of the following stages of repair:

a. Before defect removal.

b. After removal of corrosion or defect down to the good material.

c. After removal of any damaged part, or part thereof, before application of repair; and

d. After installation of repair but before top coat of paint applied.

5.6 The DMR shall list any structural modifications embodied or preventative repair actions taken during maintenance input that were not the result of actual findings during the DM servicing. Where a defect was found during the actioning of such work, then this shall be detailed as per clause 5.4 and clause 5.5.

5.7 The DMR shall list the results of any directed inspections that are required by Airworthiness Directives, Service Bulletins, internally generated Special Technical Instructions or the like.

5.8 The DMR shall list any repetitive inspections that are required as a result of structural rework actioned during the DM.

5.9 The DMR shall detail the results of any investigations actioned as a result of the defect finding. Where these investigations are not complete, an estimate of when it will be complete, along with reference and contact information, shall be provided. If a repair has been installed but only analysed for static requirements, then details of the fatigue and/or damage tolerance assessment to be performed shall be included. Data sufficient to track the requirement for these assessments shall be provided.

5.10 A supplementary DMR shall be provided with the findings for all outstanding items (once completed). This supplementary DMR shall be provided no more than 12 months after completion of the DM.

5.11 In the event of items/actions being outstanding following the provision of the DMR, a status report shall be provided quarterly, detailing the current state of all outstanding DMR follow-up items/actions. For any items closed or actions completed since the previous quarterly updated, a summary of the closed details shall be provided.

SAMPLE DID FOR ROUTINE USAGE STATUS REPORTS

1 IDENTIFIER: DID-RUSR

2 TITLE: ROUTINE USAGE STATUS REPORTS

1 DESCRIPTION

3.1 The Routine Usage Status Reports (RUSR) contain key airframe usage data to allow both the Commonwealth and the Contractor to monitor and manage fatigue usage within the aircraft fleet.

2 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following documents are referenced in this DID:

AAP 7001.053 (AM1)	Technical Airworthiness Maintenance Manual (TAMM)
SOI – Subject Aircraft	Statement of Operating Intent

4.1.2 The following DSD and Data Items form part of this DID to the extent described herein:

Engineering Support Services (ENGSERV),	DSD-ENGSERV
Usage Assessment Report (UAR),	DID-UAR
Fatigue Assessment Report (FAR),	DID-FAR

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of Routine Usage Status Reports as required by the Contract/Statement of Work and Engineering Support Services DSD (refer DSD-ENGSERV).

4.2.2 The Contractor shall develop and maintain a specification for the production and control of the reports as required by this DID. The specification shall be subject to review and approval by the Commonwealth.

4.2.3 The Contractor is to provide a Routine Usage Status Report (RUSR) at three monthly intervals. A draft report for Commonwealth review is to be issued within 30 calender days after the 20 January, 20 April, 20 July and 20 October. The final report is to be issued within 30 calender days after the end of January, April, July and October.

4.2.4 The report is to cover a period of three months unless specifically requested otherwise. The three month period is to run from the first day after the last reporting period to the end of the current reporting period.

4.2.5 The RUSR is to be documented in an Authorised Engineering Organisation (AEO) approved report. That is a report developed, reviewed and approved in accordance with the process and requirements specified in AAP 7001.053 (AM1) and the AEO's Engineering Management Plan (EMP).

4.2.6 The Contractor is to ensure that all data used for the production of the RUSR is available to the agency preparing the report.

4.2.7 The three monthly RUSR form the basis for the development of the annual usage assessment (refer to DSD-UAR).

5 RUSR CONTENT REQUIREMENTS

5.1 The RUSR is to analyse and present a summary of the quality of the aircraft fleet usage data collected since the last RUSR. This will include, but not limited to:

a. Comparison of EE500, EE360, Aircraft Operations (ACOPS), CAMM2 and HUMS data capture (such as airframe hours and number of full stop and touch and go landings) and provide comment on differences.

b. The number of HUMS unmonitored flights.

c. The level of fill in data used.

d. Identification of instances of spurious data; and

e. Identification of issues with the quality of recorded data.

5.2 The RUSR is to identify any periods of unusual usage such as aircraft on extended deployment or extended maintenance inputs.

5.3 The RUSR is to analyse and present the usage data for individual aircraft, the fleet and, if relevant, sub fleets identified in the Fatigue Assessment (refer to DID-FAR), recorded during the assessment period. Trend data is also to be presented for the current and all-time periods. Typical data to be presented includes:

a. AFHRs – both CAMM2 usage period and total.

b. The number of flights – usage period and total.

c. The number of landings, both full-stop and touch-and-go – usage period and total.

d. Mission types and mix comparison against the SOI – usage period, previous 12 months and total.

e. AFHRs in speed and altitude bands.

f. Fatigue Index or Damage accrual rates – usage period and total; and

g. Normal Acceleration data – usage period and total.

5.4 The RUSR is to provide an explanation for any apparent anomalies in recorded data.

5.5 The RUSR is to make comment on the usefulness and adequacy of the data available and the systems used in its preparation.

5.6 The RUSR is to identify any significant work carried out on the HUM or OLM systems during the reporting period. Any items or units replaced on these systems during the reporting period are to be identified. An assessment is to be made to determine if the work performed has had any noticeable effect on the data recorded or presented.

5.7 The RUSR is to make a comparison of the severity of aircraft usage during the reporting period against the approved aircraft usage baseline and provide comment on the adequacy of the current aircraft structural maintenance program to support the RAAF aircraft fleet usage.

5.8 The RUSR is to make recommendations, if required, to the appropriate agencies to ensure the required usage data (and quality) is collected and forwarded to the specified agency in a timely manner.

SAMPLE DID FOR USAGE ASSESSMENT REPORT

1 IDENTIFIER: DID-UAR

2 TITLE: USAGE ASSESSMENT REPORT

3 DESCRIPTION

3.1 The Usage Assessment Report (UAR) documents the annual usage assessment activity, being part satisfaction of the requirements for monitoring and assessing aircraft usage and structural life, as specified by AAP 7001.053(AM1).

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following documents form part of this DID to the extent described herein:

AAP 7001.053(AM1)	Technical Airworthiness Management Manual (TAMM)
SOI – Subject Aircraft	Statement of Operating Intent

4.1.2 The following DSD and Data Items are related to this DID to the extent described herein:

Engineering Support Services (ENGSERV),	DSD-ENGSERV
Aircraft Structural Integrity Management Plan (ASIMP),	DID-ASIMP
Routine Usage Status Reports (RUSR),	DID-RUSR
Fatigue Assessment Report (FAR),	DID-FAR

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of a Usage Assessment Report as required by the Contract/Statement of Work and Engineering Support Services DSD (refer to DSD-ENGSERV).

4.2.2 The Contractor shall develop and maintain a specification for the production and control of the reports as required by this DID. The specification shall be subject to review and approval by the Commonwealth.

4.2.3 The Contractor is to ensure that all data used for the production of the UAR is available to the Commonwealth. Any software required to read or process data supplied is to be made available by the contractor.

4.2.4 The UAR will contain a usage assessment of the subject aircraft fleet covering a period of 12 months, unless specifically noted otherwise or requested by DGTA. The 12 month period is to run from 1 July to 30 June.

4.2.5 A draft of the UAR is to be provided within 100 days of the end of the period noted in clause 4.2.4. In conjunction with the draft report, the contractor is to provide an electronic copy of all raw and processed usage data for the reporting period.

4.2.6 Allowance is to be made for amendment and inclusion of data at the request of the Commonwealth and Contractor undertaking clause 4.2.2. Once the data and draft UAR is deemed adequate by the Commonwealth, then the final report is to be issued within 60 calender days.

4.2.7 The UAR is to be documented in an Authorised Engineering Organisation (AEO) approved report. That is a report developed, reviewed and approved in accordance with the process and requirements specified in AAP 7001.053(AM1) and the AEO's Engineering Management Plan (EMP).

4.2.8 The annual usage assessment (and resultant UAR) is instrinsic to the conduct of the annual fatigue assessment (refer to DID-FAR).

5 UAR CONTENT REQUIREMENT

5.1 The UAR is to analyse and present a summary of the quality of the aircraft usage data collected since the last UAR, consistent with the data quality reporting in the Routine Usage Status Report (DID-RUSR).

5.2 The UAR is to state whether the data quality appears adequate for the purposes of the assessment. Comment should be made on any detected bias in the data, for example, a considerable proportion of fill-in data being used during the reporting period.

5.3 The UAR is to include a trend analysis (for the 12 month period and all time) of data quality and assess for indications of present or future variation outside of control limits.

5.4 The UAR is to analyse and present the usage data for individual aircraft, the fleet, and if relevant, sub fleets over both the usage period and for all time. The data analysis should also consider the effect of the data sample size and quality on the validity of the result. Usage data to be reviewed and trended should as a minimum cover all data presented in the RUSR.

5.5 The UAR is to review each data parameter, using statistical analysis where appropriate, to address the distribution of the data set for individual aircraft within the RAAF fleet, and for the aircraft fleet, and the change of relevant parameters with respect to previous recording periods.

5.6 The UAR is to analyse the data for variation in the mission profiles with respect to previous UARs and the SOI, for individual aircraft and the fleet.

5.7 The UAR is to perform an assessment of the aircraft usage severity in comparison with the baseline spectrum usage severity.

5.8 The UAR is to provide an explanation for any apparent anomalies or significant trend variations in recorded data.

5.9 The UAR is to list recommendations for any improvements that may be made to the usage data recording and collection.

5.10 The UAR is to make comment on the usefulness and adequacy of the data available and the systems used in its preparation.

SAMPLE DID FOR STRUCTURAL CONDITION ASSESSMENT REPORT

1 IDENTIFIER: DID-SCAR

2 TITLE: STRUCTURAL CONDITION ASSESSMENT REPORT

3 DESCRIPTION

3.1 The Structural Condition Assessment Report (SCAR) documents the annual structural condition assessment activity (for each individual aircraft and the RAAF fleet) in support of the continuing assessment of aircraft structural integrity, for the purposes of maximising the safety, minimising the cost of ownership and maximising aircraft availability. The SCAR also provides an opportunity to identify limitations with, and proposed improvements to, the in-service structural management programs.

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following document forms part of this DID to the extent described herein:

AAP 7001.053(AM1), Technical Airworthiness Management Manual (TAMM)

4.1.2 The following DSD and Data Items are related to this DID to the extent described herein:

Engineering Support Services (ENGSERV),	DSD-ENGSERV
Aircraft Structural Integrity Management Plan (ASIMP),	DID-ASIMP
Usage Assessment Report (UAR),	DID-UAR
Deeper Maintenance Report (DMR),	DID-DMR
Fatigue Assessment Report (FAR),	DID-FAR

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of a Structural Condition Assessment Report (SCAR) as required by the Contract/Statement of work and the Engineering Support Services DSD (refer to DSD-ENGSERV)

4.2.2 The Contractor shall develop and maintain a specification for the production and control of the SCAR, as required by this DID. The specification shall be subject to review and approval by the Commonwealth.

4.2.3 The Contractor is to ensure that all data used for the production of the SCAR is available to the agency preparing the Fatigue Assessment (FA). This data will be used in the FAR to establish any impact on the fatigue management of individual aircraft of the fleet due to specific damage occurrences within the reporting period and due to long term condition trends. Any software required to read or process data supplied is to be made available by the contractor.

4.2.4 The Contractor shall provide a SCAR on an annual basis. The report shall cover a period of 12 months, unless specifically noted otherwise or requested by DGTA. The 12 month period shall run from 1 July to 30 June. For trending purposes, the SCAR shall cover all-time data up to the end of the reporting period. The SCAR is to be delivered in conjunction with the Usage and Fatigue Assessment Reports (refer to DID UAR and DID-FAR).

4.2.5 The contractor shall provide a draft SCAR within two months of the end of the period noted in clause 4.2.4. In conjunction with the draft report, the contractor shall provide an electronic copy of all raw and processed condition data for the reporting period.

4.2.6 Allowance is to be made for amendment and inclusion of data at the request of the Commonwealth. Once the data is deemed sufficient by the Commonwealth, then a final certified report is to be issued within 60 calender days.

4.2.7 The SCAR is to be documented in an Authorised Engineering Organisation (AEO) approved report. That is a report developed, reviewed and approved in accordance with the process and requirements specified in AAP 7001.053(AM1) and the AEO's Engineering Management Plan (EMP).

4.2.8 The annual structural condition assessment (and resultant SCAR) is intrinsic to the conduct of the annual fatigue assessment (refer to DID-FAR).

5 SCAR CONTENT REQUIREMENTS

5.1 The SCAR shall contain a section that details the requirement for the assessment. The SCAR shall contain a section that describes the aircraft Structural Condition Management system, and any changes since the last SCAR.

5.2 The SCAR shall review and report on condition data and provide a summary of the data reviewed. Source data for this section shall include all relevant data that defines the structural condition of the aircraft. This includes data retrieved from the maintenance records such as the aircraft post Deeper Maintenance Reports (DMR) detailed in DID-DMR, inspection findings, details of repairs and modifications undertaken to primary structural elements and results from environmental degradation and condition management programs, such as the Corrosion Prevention and Control Program (CPCP) or its equivalent. The review shall include available and applicable condition data originating from other operators, both military and commercial (where applicable), and all relevant Technical Airworthiness Alert Information, such as service bulletins, service letters and Airworthiness Directives.

5.3 The SCAR shall review the collected condition data. Analysis shall be performed to identify any trends, both short and long term, in the data. The trending analysis should be presented separately for critical and non-critical structure.

5.4 To maintain airworthiness, the minimum requirements for data assessment and trending analysis for critical structure shall include:

a. identifying their susceptibility to corrosion;

b. identifying their susceptibility to multiple-site damage; and

c. identifying any evidence of, or potential for, adverse interaction of adjacent repairs.

5.5 Additional requirements for data assessment and trending analysis, to maximise availability and minimise cost of ownership, shall include as a minimum:

a. those requirements listed in clause 5.4, but for primary and secondary structure (on a cost benefit basis);

b. identifying susceptibility to degradation of adhesive bonds;

c. assessing and trending logistic costs;

d. assessing and trending maintenance costs; and

e. assessing and trending aircraft downtime (in days).

5.6 The SCAR shall consider and discuss factors that influence condition data, such as aircraft base locations, extended periods of deployment and routine maintenance activities.

5.7 The SCAR shall analyse and present a summary of the quality of the subject aircraft condition data collected since the last assessment. It shall also include an analysis of trends in data quality for the reporting period and all time, and assess for indications of present or future variation outside of control limits. Any issues with the quality of data recorded while aircraft were on significant deployments shall be recorded.

5.8 The SCAR shall state whether the data quality and quantity appears adequate for the purposes of the assessment. Comment shall be made on any detected bias or anomaly in the data, for example, data not being distributed over the entire period under study.

5.9 The SCAR shall review each data parameter, using statistical analysis where appropriate, to address the distribution of a particular parameter for individual aircraft within the subject aircraft fleet, and for the fleet as a whole, and the change of the relevant parameter with respect to previous recording periods.

5.10 The SCAR shall make comment on the usefulness and adequacy of the data available and the systems used in its preparation.

5.11 The SCAR shall identify any significant structural work carried out on the aircraft during the reporting period. Any structural rework as a result of an unacceptable condition shall be summarised. An assessment shall be made to determine if the work performed is likely to have any noticeable effect on the data recorded or presented.

5.12 The SCAR shall assess the nature and extent of any effect that the data collected and analysed in this report has on the assumptions and the resultant inspections for the baseline structural inspection program. Any variation to the baseline inspection program that is required as a result of the impact of the structural condition of the fleet shall be detailed in the SCAR, with appropriate justification.

5.13 The SCAR shall assess the nature and extent of any effect that the data collected and analysed in this report has on structural condition management programs other than the baseline inspection program. This shall include, but not be limited to, the CPCP (or its equivalent) and routine maintenance activities. This assessment shall consider the impact of the structural condition on design assumptions and results for the fleet as a whole and also the impact that any variation within the fleet, at either individual aircraft or at a sub-fleet level, has on the applicability of structural condition management programs.

5.14 The SCAR shall address the impact of current period and accumulated structural condition degradation with respect to both the structural and economic life-of-type (LOT) and the feasibility of achieving the planned withdrawal date (PWD).

Blank Page

SAMPLE DID FOR FATIGUE ASSESSMENT REPORT

1 IDENTIFIER: DID-FAR

2 TITLE: FATIGUE ASSESSMENT REPORT

3 DESCRIPTION

3.1 The Fatigue Assessment Report (FAR) documents the annual fatigue assessment activity, being part satisfaction of the requirements for ongoing monitoring and assessment of aircraft structural integrity as specified by AAP 7001.053(AM1).

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following document forms part of this DID to the extent described herein:

AAP 7001.053(AM1), Technical Airworthiness Management Manual (TAMM)

4.1.2 The following DSD and Data Items are related to this DID to the extent described herein:

Engineering Support Services (ENGSERV),	DSD-ENGSERV
Aircraft Structural Integrity Management Plan (ASIMP),	DID-ASIMP
Routine Usage Status Reports (RUSR),	DID-RUSR
Usage Assessment Report (UAR),	DID-UAR
Structural Condition Assessment Report (SCAR),	DID-SCAR

4.2 General Instructions

4.2.1 This DID provides instructions for the preparation of a FAR as required by the Contract/Statement of Work and Engineering Support Services DSD (refer to DSD-ENGSERV).

4.2.2 The Contractor shall develop and maintain a specification for the production and control of the reports as required by this DID. The specification shall be subject to review and approval by the Commonwealth.

4.2.3 The Contractor is to ensure that all data used for the production of the FAR is available to the Commonwealth. Any software required to read or process data supplied is to be made available by the contractor.

4.2.4 The FAR will contain a fatigue assessment of the Commonwealth aircraft fleet covering a period of 12 months, unless specifically noted otherwise or requested by DGTA. The 12 month period is to run from 1 July to 30 June.

4.2.5 A draft FAR is to be completed within 100 calendar days of the preparing agency receiving the draft UAR (and any amendments to the draft UAR).

4.2.6 The final FAR is to be released within 30 days of receipt by the preparing agency of the final UAR, providing the final UAR contains no new information beyond that previously discussed between the contractor, Commonwealth and the agency responsible for performing the FAR.

4.2.7 The FAR is to be documented in an Authorised Engineering Organisation (AEO) approved report. That is a report developed, reviewed and approved in accordance with the process and requirements specified in AAP 7001.053(AM1) and the AEO's Engineering Management Plan (EMP).

5 FAR CONTENT REQUIREMENT

5.1 The FAR is to contain a section that details the requirement for the fatigue assessment, describes the aircraft Fatigue Management System (FMS) and the status of the aircraft FMS, and any changes made to the system since the last fatigue assessment.

5.2 The FAR is to document an independent assessment of the aircraft usage severity in comparison with the baseline spectrum usage severity. The severity comparisons are to be cognisant of fatigue accrual rates and other parametric measures. Assessment of usage severity is to be confirmed (if possible) with fleet condition data (from the associated SCAR, refer to DID-SCAR).

5.3 The FAR is to address the extent that usage severity varies for individual aircraft, sub fleets or the Commonwealth fleet. The fatigue assessment is to assess the impact of variations in usage severity across individual aircraft, sub-fleets or the Commonwealth fleet.

5.4 The FAR is to include a review of the condition aspects that may affect the fatigue management system. The FAR is to report on condition data from critical structure during the period and provide a summary of the data reviewed. One aim of the condition data is to establish the impact on fatigue management due to individual damage occurrences and condition deterioration within the reporting period, and due to long-term condition trends.

5.5 The FAR shall address the impact of current period and accumulated aircraft usage and condition with respect to the structural LOT and the feasibility of achieving PWD.

5.6 The FAR shall comment on and establish the validity of the results of the aircraft fatigue assessment given the assumption made and taking into account the quality of the input data and any usage variations from the baseline. The FAR shall address the impact of the difference between current mission profiles and mix, and the mission profiles and mix of previous assessments. Further, the FAR shall make recommendations for improvements to data recording and processing if they will improve the fatigue assessment validity.

5.7 The FAR shall address the impact of aircraft usage and condition on the validity and effectiveness of the current maintenance program with respect to assuring ongoing airworthiness. Comment shall be made on the effect of the usage and condition for the period on the overall fatigue management of the aircraft. Any airworthiness issues, structural limit issues and inspection interval and location issues arising from usage, condition and structural configuration changes shall be identified.

5.8 The FAR shall list recommendations for any improvements that may be made to the aircraft Fatigue Management System and make comment on the usefulness and adequacy of the data available and the systems used in the preparation of the RUSR, UAR and SCAR.

SECTION 2

CHAPTER 12

AIRCRAFT / STORES COMPATIBILITY

INTRODUCTION

1. This chapter identifies the ADF's preferred design requirements for aircraft / stores compatibility (A/SC) and should be read in conjunction with AAP 7001.053 Sect 3 Chap 15. Use of different standards, and interpretation and tailoring of all standards must be discussed with ASCENG.

2. This chapter does not address certain aspects of the safety testing of explosive ordnance (EO) (such as rough handling, storage, and accelerated aging or transportation tests), tests of basic materials or piece parts, or the verification of the effectiveness of the EO. Such matters are the responsibility of GWEO (and in some cases DOS).

AIRCRAFT / STORES COMPATIBILITY DESIGN REQUIREMENTS

3. MIL-HDBK-1763, 'Aircraft/Stores Compatibility: Systems Engineering Data Requirements and Test Procedures', is the ADF's preferred 'standard' for A/SC activities. This HDBK identifies the majority of the ADF's preferred design standards, test requirements and methodology, and data delivery requirements. However, the ADF has some unique requirements and these are listed below and cross-referred to the applicable MIL-HDBK-1763 section.

4. Add AIR STD 20/34, 'Environmental Test Methods for Aircraft Stores', and DEF (AUST) 5168, 'The Climate Environmental Conditions Affecting the Design of Military Equipment', to Appendix C Part 111 para C.111.2.2.

5. Add AIR STD 20/36, 'Hazards of Electrostatic Discharge to Aircraft Stores', and AIR STD 20/43, 'Radiation Hazards to Aircraft Armament Electro-explosive Devices', to Appendix C Part 111 para C.111.3.

Draft Requirements (to be specified in conjunction with ASCENG)

6. ***Ground Safety Device.*** The store release system should be equipped with a positive safety device or devices to preclude functioning, dropping, launching, or ejecting of suspended stores or activation of ejector devices when the aircraft is on the ground even if the release or actuation system is energised.

7. ***Emergency Jettison.*** All aircraft carrying stores containing explosive ordnance should provide a functionally separate emergency jettison capability that should be demonstrated to present an improbable hazard to the releasing aircraft and ground based personnel and facilities.

8. ***Safety Templates.*** Safety templates should meet:

a. RCC STD 321-00 criteria.

b. In varying a stores mass and physical properties, a 5% variation in the specified Stores Coefficient of drag, and thrust for powered stores, should be assessed for impact on the safety templates.

c. Range monitoring systems that use a flight termination system (or systems) to determine safe operating areas should use at least two, independently redundant data systems to track any air vehicle or weapon under its control.

Blank Page

SECTION 2

CHAPTER 13

HUMAN FACTORS ENGINEERING

INTRODUCTION

1. The operational success of weapon systems, in part, comes from recognising that the roles and performance of the human components within those systems form part of the design process. This chapter provides guidance on the application of Human Factors Engineering requirements, from a technical perspective, for the design, maintenance and modification of ADF aircraft. Complimentary guidance on the Operational Airworthiness aspects of human factors is available from Wing and Squadron Aviation Safety Officers.

2. The DAR's primary role in HFE is to ensure that suitably qualified and empowered Subject Matter Experts (SMEs), usually operators and maintainers, have accepted the product's Human Machine Interface (HMI) design, backed, where necessary, by human factors' specialists. The guiding principle is that ultimately, the acceptability of the aircraft HMI (eg cockpit ergonomics, workload, design, maintainability, etc) is to be determined by the operators and maintainers themselves, for the entire operating envelope. Their input from early concept definition stages is therefore critical both for new designs and on-going design changes and may be documented in flight test reports or separate reports described by the Human Engineering Program Plan (HEPP).

3. The term 'Human Engineering' is not synonymous with 'Human Factors Engineering' (HFE). Human Engineering is the application of knowledge about human capabilities and their limitations only to system or equipment design. The term 'Human Factors Engineering' is more comprehensive, covering all biomedical and psychosocial considerations applying to the human in the system, to afford operators and maintainers the best possible opportunities in the operation of highly complex equipment. HFE therefore includes Human Engineering, HMI, perception and cognition, life support, personnel selection and training, training equipment, job performance aids, and performance measurement and evaluation.

4. HFE is therefore part of the mainstream design effort throughout the system life cycle and seeks to optimise the weapon system by integrating the human performance necessary to operate, maintain, support, and control the system in its intended operating environment. The scope of typical HFE effort in a major system acquisition life cycle is shown at Annex A.

5. When considering new designs or modifications, the System Program Office (SPO) should ensure that new designs or changes exploit known average human capabilities, and minimise performance requirements which exceed those capabilities. A system that requires extreme, uninterrupted concentration over long periods of time could not be relied upon to be effective in combat. All safe system designs should therefore not only take into account the limitations of people but also build in safeguards to mitigate 'worst credible scenarios' should the limitations be exceeded. Consequently, the application of HFE considerations in new design or modifications can be broadly separated into two areas:

a. HFE Considerations in Individual System Design. This covers the application of HFE in each aircraft system's design, to optimise normal and worst credible scenario operations (ie micro level considerations).

b. HFE Considerations in Systems' Integration. This ensures HFE consideration of the workloads placed on personnel when the integrated aircraft system is not operating as intended, in worst credible scenarios (ie macro level considerations).

6. These two separate but complimentary sets of considerations are now addressed in turn. The methodologies discussed will be the same whether the task involves a completely new design or a minor design upgrade. Further, this chapter also complements guidance provided on System Safety in Section 2 Chapter 1. HFE considerations are the third essential element of a successful System Safety Program, and must therefore be assessed together with hardware and software safety considerations, through the System Safety Program Plan and HEPP.

HFE CONSIDERATIONS IN INDIVIDUAL SYSTEM DESIGN

Human Engineering Program

7. The scope of HFE considerations are typically applied to programs through pragmatically tailored HEPPs. This document can be a beneficial management and coordination tool, however not all design changes will warrant a HEPP. Its need will be dependent on relative platform risks, technologies employed, design complexity, sensor usage, HFE coordination required, crew numbers and operating intent. Whatever the scope of the HEPP, effort and guidance provided in this chapter must be tailored to be proportional to risks within the weapon system's configuration, role and environment, and to integrate with the System Safety Program (refer to Section 2 Chapter 1). Every HEPP task must therefore be tailored toward maximising the crew's ability to operate all systems under worst credible scenarios. A sample HEPP DID is included at Annex B.

HFE Design Characteristics

8. Aircraft systems should provide work environments which foster effective procedures, work patterns and personnel health and safety, and minimise factors that degrade human performance or increase the possibilities for human error. However, given the role of the ADF, a sensible mix of safety and operational priorities must be found for each weapon system. The design of aircraft systems therefore typically reflects human engineering, physiological, life support and biomedical factors that affect human performance, including:

a. environmental conditions, such as:

(1) pressure, temperature, humidity, ventilation, lighting;

(2) noise, vibration, acceleration, shock, blast and impact forces; and

(3) thermal, toxicological, radiological, mechanical, electrical and other hazards.

b. provisions for minimising psychophysiological stress factors of mission duration and fatigue;

c. ergonomic considerations, such as visual display acuities and appearance, audio displays, controls, labelling, anthropometry, work space design, and HMI;

d. ease of maintenance;

e. provision for ingress, egress and on-board movement under normal, adverse and emergency conditions;

f. emergency systems and life support equipment for contingency management, escape, survival and rescue; and

g. provision of acceptable personnel accommodation, including body support and restraint during both normal and ejection conditions, seating, rest, and sustenance.

9. However, the application and tailoring of HFE design characteristics is dependent on the following factors:

a. The degree of system independence. HFE considerations must be designed into, and assessed for, each individual system as well as the total integrated system. Greater human tolerance at the system level may allow fewer characteristics to be applied at the lower levels and vice versa.

b. The level of new technology, complexity and system automation. Characteristics applied to new technology or highly complex and automated systems will typically require commensurate validation methods to confirm adequate mitigation of that complexity both during normal and worst credible scenarios. Additional tailoring of characteristics to inherent risks may therefore be required to ensure a pragmatic design scope.

c. The inclusion of Off-the-Shelf Equipment. There is little opportunity for the influence of HFE in these applications. Consequently, to highlight areas of future concern, the ADF should establish what HFE criteria was applied, its CRE acceptability, and the results of any workload assessment conducted (discussed later in this Chapter).

HFE Specialist Organisations

10. To assist ADF projects with the consideration of the above factors and characteristics there are numerous HFE specialist agencies available within the ADF. These agencies can be tasked to assist with advice or research, as listed below. Given the highly subjective nature of HFE analysis, some or all of their involvement is strongly encouraged, commensurate to platform risks.

a. **Aircraft Research and Development Unit (ARDU).** ARDU Flight Test Squadron's experienced and qualified test pilots and flight test engineers are a source of HFE advice on RAAF and Army aircraft, including aircraft design, cockpit and workload assessments, flight controls, flying qualities and HMI management.

b. **Aviation Medicine Institute (AVMED).** AVMED's human psychology and physiology cell, specifically adapted to aviation environments, can be used as a source of HFE advice on anthropometry, HMI and HEPs.

c. **Defence Science and Technology Organisation (DSTO).** The HFE research program at the Air Operations Division contributes towards the effectiveness of all human aspects within an aircraft system, including HMI design, application and interaction, and safe operation/workload under normal and worst case credible scenarios (through modelling if necessary).

d. **AMAFTU (Aircraft Maintenance and Flight Trials Unit).** Similar to ARDU, the RAN's flight test centre of expertise can provide experienced and qualified maintainers, test pilots and flight test engineers for advice on naval rotary wing aircraft and specialist functions. Advice can be requested on all aspects of HFE design, operation and maintenance including cockpit and workload assessments, shipboard landings, flight controls, flying qualities and HMI management.

e. **AMTDU (Air Mobility and Training Development Unit).** AMTDU provides training, engineering development advice in cargo aerial delivery (ie airland, airdrop and external lift) and usage procedures. Advice can be requested on flying qualities impacts, and loadmaster aspects of HFE load design, workload assessments and HMI management.

f. **Squadron or Wing Aviation Safety Officers (ASOs).** Trained in Crew Resource Management (CRM) and Aviation Risk Management (AVRM), these individuals are tasked by the parent units with the identification and mitigation of operational risks - mostly HFE-related. They are a source of local HFE advice and involvement in Human Factors' Working Groups and System Safety Working Groups (SSWG).

Human Factors Working Group

11. The establishment of a Human Factors' Working Group (HFWG) will enable the Project Office, SMEs and specialists to liaise efficiently, maximise the potential for identifying hazards, and analyse and mitigate hazards to acceptable levels. Further, HFWG tasks should be coordinated with the weapon systems' SSP, to avoid duplication, maximise efficiency, and actively integrate with the SSWG and its Hazard Risk Index (HRI) matrix. Further details on the System Safety Program and SSWG can be found in Section 2 Chapter 1.

Standards Application and Tailoring Guidance

12. The following paragraphs summarise ADF-preferred HFE standards. However, within the context of ADF acquisitions and sustainment, the application of HFE principles is usually not as simple as following a single standard. This is primarily due to most ADF acquisitions being of mature weapon systems with tailored modifications to meet specific ADF requirements. The ADF therefore typically relies on multiple HFE principles across multiple standards. Irrespective, HFE requirements should be tailored to be commensurate to inherent platform risks, CRE, and ensuring positive control of the Contractor's effort. Detailed synopses of HFE-related standards and guidance has been provided at Annex C.

13. **US Military Standards.** US military standards tend to be structured for their typical acquisition process, whereby the DoD generally has control over the entire product design cycle, through various iterations of conceptual design. Conversely, the ADF often requests Contractors to supply (with or without additional design) the required systems. The US DoD processes therefore may not transfer directly to the fixed price contracting methodologies typically used for ADF acquisitions.

14. The ADF-preferred US DoD HFE standard and complimentary guidance is MIL-STD-1472F and MIL-HDBK-46855. These provide HFE design criteria, principles and practices to be applied in the design of systems, equipment and facilities for a comprehensive HFE Program. While costly and inappropriate in many ADF applications without tailoring, they provide essential requirements in projects where there are significant HFE issues at stake (eg. cockpit layouts).

15. **UK Military Standards.** The ADF-preferred UK HFE military standard is DEF STAN 00-25. The standard aims to provide acquirers and designers with HFE data and process guidance, and post-design evaluation considerations. It is structured towards providing criteria for both individual systems, and overall system integration.

16. **Commercial Standards.** HFE design considerations for civil certified platforms can usually be found embedded within the various systems' design requirements (ie within FAR/JAR regulations), with some additional guidance provided by specific ACs. Together, they cover all the aspects and criteria of HFE. However, most commercial manufacturers still use MIL-STD-1472 for HFE certifications of airborne systems under the FAA. Consequently, the ADF-preferred commercial HFE standard is either the FARs/JARS themselves, and/or MIL-STD-1472F, depending on the scope of the new design. POs are therefore encouraged to seek early advice from DGTA.

HFE CONSIDERATIONS IN SYSTEMS' INTEGRATION

17. HFE issues have the potential to become most significant after equipment fielding and therefore operated by average-skill personnel. Hence, after all HFE design methodologies have been applied to individual systems and design integration is complete, a Human Factors Workload Assessment (HFWA) should be considered. The HFWA aims to validate that the integrated system design allows HMI and HFE-related duties to be carried out under the worst credible scenarios (ie multiple hazards at the same time) without reaching the task saturation limit for the average-skill crew complement. A sample HFWA CDRL DID is provided at Annex D.

18. Further, as part of the PO Transition Plan, the PO needs to ensure the transition of all HFE-related documents to the SPO, to allow for the consideration of original HFE concepts through Life-Of-Type (LOT). LOT considerations from the in-service organisation will then also include tailored Human Factors Workload Assessments to ensure HFE task saturation limits are not compromised, especially across interface, handling capacity and integration perspectives.

ASSOCIATED GUIDANCE AND INFORMATION

19. Synopses of the most common HFE-related standards, handbooks and guidance are provided at Annex C, however the following web sites are provided as a source of additional background information on HFE considerations and applications:

a. http://www.raes-hfg.com	Royal Aeronautical Society (RAeS) HFE Group
b. http://www.gainweb.org/	Global Aviation Information Network (GAIN)
c. http://www.flightsafety.org	Flight Safety Foundation
d. http://www.hf.faa.gov	FAA HFE Division
e. http://human-factors.arc.nasa.gov	NASA HFE Research and Technology Division
f. http://www.flightdeckautomation.com/fdai.aspx	Flight Deck Automation Issues
g. http://www.ashgate.com	Publisher of Aviation Human Factors Literature

Annexes:

A. Human Factors in the Lifecycle Acquisition Management Process

B. CDRL – 1 Human Engineering Program Plan (HEPP)

C. Human Factors Related Specifications and Standards

D. CDRL – 2 Human Factors Workload Assessment

HUMAN FACTORS IN THE LIFECYCLE ACQUISTION MANAGEMENT PROCESS

PHASE / ACTION	SOI ANALYSIS	INVESTMENT ANALYSIS	SOLUTION IMPLEMENTATION	IN-SERVICE MANAGEMENT (INCLUDING SERVICE LIFE EXTENSION)
MANAGE THE HUMAN FACTORS PROGRAM	• Identify Human Performance Deficiencies • Identify Opportunities to Improve Human Performance • Initiate Human Factors Goals and Objectives	• Designate HFE Coordinator • Generate a HEPP • Establish HFE Working Group • Develop the HEP	• Refine the HEP • Update HEPP if required	• Refine HEP • Update HEPP if required
ESTABLISH HUMAN FACTORS REQUIREMENTS	• Identify HFE and Human Resource Constraints	• Establish HFE Requirements in Acquisition Docs • Formulate Draft HFE Requirements for a System Specification • Generate Initial HFE Requirements for a SOW	• Revise HFE Requirements in the System Specification • Refine HFE Requirements in the SOW • Specify HFE Requirements for Source Selection	• Update HFE Requirements for System Modifications and Upgrades
CONDUCT HUMAN FACTORS SYSTEM INTEGRATION	• Identify Potential HFE Analyses and Trade-offs	• Provide HFE Inputs to Acquisition Docs • Initiate HFE Tasks and Activities • Coordinate HFE Tasks and Activities with ILS	• Revise HFE Inputs to Acquisition Documents • Continue HFE Tasks and Activities • Coordinate Results of Human Factors and ILS Analyses	• Monitor Results of HFE and ILS Activities
CONDUCT HUMAN FACTORS TEST AND EVALUATION		• Draft/Revise HFE Inputs for T&E Plans • Conduct Front-end Analysis • Prepare for a Human Factors Workload Assessment	• Revise HFE Inputs to T&E Plans • Participate in Developmental and Operational Testing • Conduct a Human Factors Workload Assessment	• Monitor HFE Test and Evaluation Activities • Conduct Post-Deployment Assessments • Ensure that original Human Factors Workload Assessment Baseline is not affected

Blank Page

CDRL-1 HUMAN ENGINEERING PROGRAM PLAN (HEPP)

Description/Purpose

1. The Human Engineering Program Plan is the single document which describes the contractors entire human engineering program, identifies its elements and explains how the elements will be managed.

Preparation Instructions

2. The following documents are referenced herein:

a. MIL-HDBK-46855 ‘Human Engineering Guidelines for Military Systems, Equipment and Facilities’, and

b. DI-HFAC-80740 ‘Human Engineering Program Plan’.

Content

3. The HEPP shall capture the requirements of MIL-HDBK-46855 and DI-HFAC-80740.

4. The following aspects of the HEP shall also be included in the HEPP:

a. Tailoring to be applied to all HFE regulations and guidance to be used.

b. A description of how sub-contractor HFE efforts will be integrated into the contractor’s efforts and reports.

c. System description:

(1) intended function,

(2) underlying principles for automation logic,

(3) underlying principles for crew procedures, and

(4) assumed crew characteristics.

d. The HFE Design Acceptance requirements,

e. Methods of compliance,

f. Intended interface and integration with:

(1) System Engineering - To identify and define system, equipment and facilities’ operations, maintenance, and control functions, and to allocate these requirements to human, machine or HMI combinations.

(2) Design and Development - Whether of equipment, procedures, work environments, and facilities associated with the system functions requiring human performance; and

(3) Test and Evaluation - To verify that design of equipment, procedures, work environments and facilities meet human performance and life support requirements and are compatible with overall system requirements.

g. Intended interface and integration with the System Safety Program, and:

(1) integration with System Safety Assessments and Analyses, and

(2) expected crew work-arounds to mitigate hazards;

h. operational, maintenance and environmental considerations;

i. Human Factors Workload Assessment requirements, conduct and tailoring;

j. HEP manpower resources, skills and training requirements;

k. HFE training requirements of the in-service organisation;

l. certification documentation available for viewing, and deliverables, and;

m. schedule of HFE activities.

HUMAN FACTORS' RELATED SPECIFICATIONS AND STANDARDS

1. The following provides synopses of the more common HFE-related standards and guidance documents.

2. US DoD Human Factors-Related Documents

a. **MIL-STD-1472F Design Criteria Standard for Human Engineering.** This remains as the most popular HFE standard and is even accepted by FAA in design certifications. It provides HFE design criteria, principles and practices to be applied in the design of systems, equipment and facilities so that:

(1) optimised performance by operator, control and maintenance personnel is achieved;

(2) skill and personnel requirements, and training time is minimised;

(3) required reliability of HMI combinations is achieved; and

(4) design standardisation within and among systems is fostered.

b. **MIL-HDBK-759C Handbook for Human Engineering Design Guidelines**. Designed to be used as a companion to MIL-STD-1472F. It provides guidelines and data on HFE design of military systems, equipment, and facilities.

c. **MIL-HDBK-46855 Human Engineering Requirements for Military Systems, Equipment and Facilities**. Defines requirements for applying HFE to development and acquisition cycles. It provides a process for the management of a development project under a comprehensive HEP. While costly and inappropriate in many ADF applications, this handbook is an essential requirement in projects where there are significant HFE issues at stake, for example, in cockpit layouts. The Contractor should follow a tailored MIL-HDBK-46855 application. However, full implementation may not be beneficial, or even possible, if the design of the tendered systems is largely fixed prior to acquisition by the ADF.

d. **DOD-HDBK-763 Human Engineering Procedures Guide**. Supplements MIL-HDBK-46855 and is designed to assist project managers and human engineers in the application of MIL-HDBK-46855 to a particular project. The handbook provides some guidelines for analysis, design, and test & evaluation procedures.

e. **DI-HFAC-80740A Human Engineering Program Plan**. Contains the format and content preparation instructions for a HEPP, related to section 4.2 of MIL-HDBK-46855.

f. **Air and Space Interoperability Council (ASIC) AIR STD 61/116/13 The Application of Human Engineering to Advanced Aircrew Systems**. (Joint effort between US, UK, Canadian, ADF and NZDF Defence agencies) Standardises methods for the integration of HE procedures within the design of advanced aircrew systems. The HEPP is based on the application of multiple relevant AIR STDs, the majority of which will be found in ASIC Working Party 10 (Aircraft Information Display and Aircrew Station Design) and ASIC Working Party 61 (Aerospace Medical and Life Support Systems).

3. UK MoD Human Factors-Related Documents

a. **DEF STAN 00-25 Human Factors for Designers of Equipment.** Aims to provide acquirers and designers with HFE data and process guidance, and post-design evaluation considerations. It is structured towards providing criteria for both individual systems, and overall integration. Additional references are provided for more detailed information.

b. **DEF STAN 00-970 Design and Airworthiness Requirements for Service Aircraft.** Provides comprehensive coverage of HFE requirements embedded within its various Chapters. Requirements are therefore not presented separately and have to be interpreted from text. For example, Part 1

discusses general and operational requirements, including human exposure to Noise and Vibration. Part 6 contains Aerodynamics, Flying Qualities and Performance requirements.

4. Commercial Human Factors-Related Documents

a. **JARs/FARs.** Minimum HFE requirements are embedded within the regulations within the broad headings of pilot skill, alertness, strength, workload, fatigue, minimum crew, controls, operation and arrangement, anthropometry, display visibility, cockpit lighting, personnel and cargo accommodations, emergency provisions, ventilation, heating and pressurisation, etc. Therefore, like DEF STAN 00-970, HFE requirements are not presented separately and have to be interpreted from text. Limited guidance is also available in some specific ACs like AC 25-11 for Electronic Display Systems and AC 20-88A for Marking of Power Plant Instruments.

b. **FAA Human Factors Design Guide (HFDG).** This guide is for the acquisition of COTS sub-systems, NDI, and Developmental Systems and is an exhaustive compilation of human factor practices and principles for the procurement, design, development, and testing of FAA systems, facilities, and equipment. It is focused on FAA ground systems. Most commercial manufacturers still use MIL-STD-1472 for HFE certifications of airborne systems under the FAA.

c. **FAA Policy Statement ANM-99-2, Guidance for Reviewing Certification Plans to Address Human Factors for Certification of Transport Airplane Flight Decks.** Provides guidance for reviewing the HFE components of the Certification Plan for Part 25 transport category aircraft, as well as defining what should be specifically included.

d. **FAA Policy Statement ANM-01-03, Factors to Consider when reviewing an Applicant's Proposed HFE Methods of Compliance for Flight Deck Certification.** Provides considerations for the review of an applicant's Human Factors or general Certification Plan. While tailored for Part 25 transport category aircraft, much of the guidance is general and may prove useful regardless of the make, model, or class of aircraft.

e. **FAA Flight Safety Digest – Human Factors in Aviation: A Consolidated Approach.** The Flight Safety Foundation ICARUS Committee's investigation of human factors-related aviation accidents has resulted in 18 findings and 10 recommendations for actions, which are detailed in this paper.

f. **FAA Flight Safety Digest: The Interfaces Between Flight crews and Modern Flight Deck Systems.** FAA's Transport Aircraft Directorate launched a study to evaluate the flight crew/flight deck automation interfaces of current generation transport category aircraft. This report is the culmination of that study.

g. **ICAO Circular 216 Human Factors Digest No.1 – Fundamental Human Factors Concepts.** Provides an introduction HFE, describing application of HFE to flight operations while encouraging the use of, and referencing, available sources of education and training.

h. **SAE ARP 1874, SAE ARP 4067 Design Objectives for CRT Displays for Part 25 and Part 23 aircraft respectively.** Recommend display system performance criteria for direct view CRT displays on the flight deck for transport and commuter category aircraft.

i. **SAE ARP 4032A Human Engineering Considerations in the Application of Colour to Electronic Aircraft Displays.** Provides recommendations concerning HFE issues in the application of colour to self-luminous display instruments. Although specifically intended for the application of colour to cathode-ray-tube (CRT) instrumentation, most portions are also compatible with other emerging electronic display technologies, whether they are self-luminous or light modulating devices, such as liquid crystal displays. However, it is not intended to address the heads-up display or night vision goggle issues.

j. **SAE ARP 4033 Pilot-System Integration.** Recommended crew interface and system integration approach for design development. Emphasises the fundamental need for a top-down design methodology with particular focus on clear operational performance requirements and functional integration.

k. **SAE ARP 4102/4 Flight Deck Alerting System.** Recommends design criteria that enhances safety of flight by providing early crew recognition of aircraft system or component status or malfunction, as well as of crew operational error.

l. **SAE ARP 4102/6 Communications and Navigation Equipment.** Recommends criteria for the control and display of communications and navigation equipment on the flight deck.

m. **SAE ARP 4102/9A Flight Management System (FMS).** Recommends HFE criteria and requirements to produce a fault tolerant FMS design for transport aircraft.

n. **SAE ARP 4102/15** Electronic Data Management System (EDMS). Recommends HFE criteria and requirements for EDMS use on the flight deck of transport aircraft.

o. **SAE ARP 4104 Design Objectives for Handling Qualities of Transport Aircraft.** Specifies design objectives for the handling qualities applicable to transport aircraft operating in the subsonic, transonic, and supersonic ranges. Objectives are not necessarily applicable to rotor or VTOL aircraft.

p. **SAE ARP 4107 Aerospace Glossary for Human Factors Engineers.** Provides accepted meanings of terminology used in reports, articles, regulations, and other materials dealing with aviation safety.

q. **SAE ARP 4153 Human Interface Criteria for Collision Avoidance Systems in Transport Aircraft.** Provides design and operational recommendations addressing HFE for airborne collision and avoidance systems.

r. **SAE ARP 4155 Human Interface Design Methodology for Integrated Display Symbology.** Recommended design approach is provided, emphasising the relationship between symbols, the information displayed, the context within which the symbols are displayed, and the tasks being supported.

s. **SAE ARP 4927 Integration Procedures for the Introduction of New Systems to the Cockpit.** Provides guidance to achieve the optimum integration of new aircraft systems which have an impact on cockpit layout or crew operating procedures. The process may also be used for the modification of existing cockpits.

t. **SAE ARP366 Autopilot, Flight Director, and Auto Thrust Systems.** Recommends criteria for the design and installation of Autopilot, Flight Director and Auto Thrust Systems. These three systems are highly interrelated and referred as an Integrated Flight Guidance System (IFGS).

u. **SAE ARP 5430 Human Interface Criteria for Vertical Situation Awareness Displays.** Provides HMI issue guidance for vertical situational awareness displays.

v. **SAE AS18012 Markings for Aircrew Station Displays**. Provides design requirements for the identification and configuration of letters and numerals for aircrew station displays.

w. **SAE ARD 50016 Head-Up Display Human Factor Issues.** Provides guidance for HFE issues related to the use of heads-up displays in civil transport aircraft. It also addresses issues with the interface provided by the heads-up display and other aircraft systems.

5. NATO Human Factors-Related Documents

a. **NATO STANAG 3994 Application of Human Engineering to Advanced Crew Systems.** Addresses the use of a HEPP during equipment procurement.

Blank Page

CDRL - 2 HUMAN FACTORS WORKLOAD ASSESSMENT

Description/Purpose

1. The Human Factor Workload Assessment (HFWA) validates that the integrated system design mitigations allow the operator to effectively perform his tasks without getting overloaded to human task saturation limits. Workload can be viewed in two different ways: forcing the operator to work harder; or increasing stress levels, difficulty and discomfort. Both cases will have considerable impact on operator's performance within the system under the worst credible scenarios. This impact needs to be quantified to validate design solutions.

Preparation Instructions

2. Contractor format allowable.

Contents

3. As a minimum, the HFWA should include:

a. objectives of HFWA;

b. integration of the HFWA into the HEPP and the SSPP;

c. skill level of crews upon which the assessment is to be based, and why;

d. identification of the worst credible hazard scenarios to be assessed and why these specific scenarios were selected;

e. assessment of mitigations to be adopted; and

f. recommendations and conclusions.

Blank Page

SECTION 2

CHAPTER 14

ROLE EQUIPMENT

INTRODUCTION

1. DEF STAN 00-970 and FAR/JARs do not fully addresses certification requirements for Role Equipment to be used on ADF aircraft. This chapter provides functional requirements, and where ADF policy or technical or operational imperatives dictate, deviations and alternate standards to supplement DEF STAN 00-970 and FAR/JARs.

2. Role equipment is any equipment, other than installed aircraft components, required to be operated in aircraft during flight, as distinct from equipment being carried as cargo. While the installation and use of role equipment in ADF aircraft is a requirement from time to time, the air and mission worthiness of aircraft could be compromised by equipment which is not compatible with aircraft systems. Additionally, some proposed role equipment may not be specifically designed for aircraft use, and therefore may not withstand the stresses imposed by the physical environment associated with aircraft operations. Before any role equipment can be approved for use, it must be evaluated to ensure that it will perform its intended function without adversely affecting the aircraft or being itself affected by the aircraft and associated environment. Obviously, incorrect operation of role equipment may not only affect the safety of aircraft and crew, but also the safety of the operator or end user.

3. Requirements for procurement of role equipment should not overstate test requirements and make the items unnecessarily expensive, or require tests that duplicate previous equipment certification tests (although these tests may still be undertaken at acceptance to verify compliance, if deemed appropriate). However, the approving authority must be satisfied that:

a. the equipment can be safely operated in an aircraft without affecting the airworthiness of the aircraft or any aircraft systems, and

b. the equipment will continue to perform its function in the most severe environment envisaged.

EFFECT ON AIRCRAFT AIRWORTHINESS

4. Role equipment must not unacceptably degrade the technical airworthiness of an aircraft. Factors to be considered when establishing the impact of role equipment on the airworthiness of an aircraft include:

a. electromagnetic emanations,

b. electrical compatibility, and

c. physical compatibility.

Electromagnetic Emanations

5. Electromagnetic emanations from role equipment, either conducted or radiated, have the potential to affect installed aircraft equipment. Accordingly, role equipment should be assessed in accordance with AAP 7001.054, Section 2, Chapter 2, *Electromagnetic Environmental Effects in Airborne Systems*, to ensure that the role equipment does not adversely affect Safety of Flight (SOF) or Mission Critical (MC) equipment on the aircraft. In addition, AAP 7001.054, Section 2, Chapter 18, *Carriage of Portable Electronic Devices*, may also provide guidance for some types of role equipment.

Electrical Compatibility

6. ***Electrical Wiring.*** Several types of electrical wiring, for example those with Polyvinyl Chloride (PVC) or Polyimide (Kapton) insulation, exhibit undesirable properties and are therefore either prohibited or heavily restricted for use in ADF aircraft. Similar restrictions apply to role equipment wiring. As such, AAP 7001.054, Section 2, Chapter 5, *Electrical Power Generation, Storage and Distribution*, should be consulted prior to fitting role equipment

to ADF aircraft. Wiring that connects role equipment to aircraft power outlets should be routed so as not to interfere with normal aircraft operations or to impede access to, or use of, the role equipment.

7. ***Bonding of Role Equipment.*** Where practical, all metallic components of role equipment should be electrically bonded to each other and to the airframe. This is required to protect the equipment and the aircraft against the effects of static electricity and lightning.

8. ***Battery Powered Equipment.*** Role equipment with installed batteries should be subjected to regular inspections to ensure the battery is physically sound and no leakage of electrolyte has occurred. If proper inspections are not included in the equipment servicing schedules, the requirement for a mandatory pre-flight inspection of batteries is to be included in the aircraft special (S) servicing for fitment of role equipment. Details of Aeromedical Evacuation (AME) Equipment technical inspections/servicings previously carried out, will be recorded in the GM 120, *Equipment Record Book*, which is required to accompany AME Equipment at all times (refer ADFP 703). Role equipment containing lithium batteries must be identified due to regulations pertaining to the carriage of lithium on ADF aircraft (Refer DI(AF) AAP 3504.001, Hazardous Goods Management).

9. ***Electrical Power Connections.*** Where role equipment is to be connected to an aircraft power supply (either directly or through some form of power conversion equipment), Military Specification electrical connectors should be used wherever possible. Where this is not practicable, a safety assessment of the connectors should be conducted, and steps taken to mitigate any inherent shortfalls.

10. ***Main Electrical Power Switch.*** Each item of electrically powered role equipment that will utilise aircraft power should be fitted with a single ON/OFF power switch in the appropriate power line. The switch should be guarded and there should be an indication that the power supply is switched on. Circuit breakers should not be used to fulfil this requirement unless they have been specifically designed for this purpose.

11. ***Overcurrent Protective Devices.*** Each item of electrically powered role equipment that will utilise aircraft power should be fitted with an overcurrent protective device. The protective device should be fitted as close as practicable to the entry point of power to the equipment. Appropriately rated circuit breakers are preferred, however fuses may be more appropriate in some circumstances. If a fuse is utilised, provision for storage of spares is required.

Physical Construction

12. ***Fastener Hardware.*** Fasteners must be suitable for the intended application and retain items securely without loss of joint integrity or separation of fastener parts when the equipment is subjected to vibration tests. Screwed fasteners must be either of the self-locking variety or must be lockwired.

13. ***Mounting and Securing.*** Suitable restraint devices should be provided which are capable of securing the role equipment against the minimum ultimate load factors (refer DI(AF) AAP 7279.010, Aerial Delivery Design Handbook and AMTDU for details). Note that the information detailed in DI(AF) AAP 7279.010 is appropriate for role equipment which is restrained in a manner similar to cargo, however SPOs should be aware that for non-standard and trial modifications where equipment is more permanently attached to the aircraft, the restraint of equipment should be designed in accordance with the aircraft ASIMP. Floor loading of the item should not exceed values for each aircraft type as detailed by AMTDU. Removable attachments, when not in use, should be securely stowed on the equipment.

14. ***Location.*** Equipment should be mounted in the aircraft in a location that will not impede normal and emergency ingress/egress. Additionally it should not impede access to aircraft emergency equipment and systems such as manual landing gear extension areas.

15. ***Oxygen Equipment.*** Where role equipment contains oxygen storage and/or distribution equipment, the requirements of AAP 7001.054, Section 2, Chapter 6, *Oxygen Systems*, should be addressed. Additional information relating to civilian installations is contained in CASA document CAAP 35-5(0).

16. ***Environmental Testing.*** The operating environment within an aircraft can be harsh, for example, dust, vibration, rapid decompression and so on. In the extremes of this operating environment, assurance is required that equipment failures will not impact the airworthiness of the aircraft or the safety of the occupants. MIL-STD-810 and RTCA/DO-160 detail various tests relating to the physical environment in which an item may be operated. MIL-STD-810 provides guidance in selecting and tailoring tests to satisfy the various conditions that equipment is likely to encounter. Guidance on role equipment environmental testing is included at paragraph 24 of this chapter.

ROLE EQUIPMENT PERFORMANCE

17. The previous section focused on ensuring that the role equipment would not impact the airworthiness of the aircraft. This section establishes requirements to ensure that the role equipment will perform as intended when installed in an aircraft, including:

a. electromagnetic compatibility,

b. electrical compatibility,

c. environmental qualification,

d. physical compatibility, and

e. ease of operation.

Electromagnetic Compatibility

18. An ADF aircraft can provide a potentially hostile electromagnetic environment for role equipment. There are three primary sources of electromagnetic interference to role equipment, as follows:

a. radiated electromagnetic interference from other aircraft systems;

b. radiated electromagnetic interference that originates externally to the aircraft (which can be particularly severe in a hostile operational environment); and

c. conducted electromagnetic interference via the role equipment's power or signal lines (if they interface with the aircraft).

19. Similar to aircraft equipment, the level of immunity required of any role equipment will be commensurate with the potential consequences of interference. The level of immunity will also depend on the role, configuration and operating environment of the host aircraft while the role equipment is installed. For example, if role equipment is to be operated in an operational (and therefore potentially hostile) electromagnetic environment, and the failure of the role equipment could have safety implications, then it may be necessary to test the equipment to a stringent immunity standard (eg. MIL-STD-461E). Conversely, role equipment with minimal consequences of failure, operated in a benign operational environment, might simply require source-victim testing to provide assurance that the role equipment is not affected by installed aircraft systems. AAP 7001.054, Section 2, Chapter 2, *Electromagnetic Environmental Effects in Airborne Equipment*, provides guidance on assessing the electromagnetic susceptibility (conducted and radiated) of installed aircraft equipment, and is equally applicable to role equipment.

Electrical Compatibility

20. ***Aircraft Electrical Power Sources.*** At least one of the following electrical power supplies will be available in ADF aircraft:

a. 12 Volt DC (thru DC - DC converter),

b. 28 Volt DC,

c. 115/200 Volt 400 Hz single or three phase AC, or

d. 240 Volt 50 Hz single phase AC (ADF VIP fleet only).

Where role equipment requires power from an external source, the use of one of the above voltage types is obviously preferred.

21. ***Battery Powered Equipment.*** Battery powered role equipment may use either rechargeable or non-rechargeable batteries. The operating life of the batteries should be considered in relation to the duration of missions on which the equipment is to be used. In some cases, equipment powered only by internal batteries, may require modification to facilitate use of an aircraft power supply to avoid the requirement to carry spare batteries on extended missions.

22. ***Electrical Power Connections.*** If equipment is not fitted with the appropriate mating connector for the aircraft power outlet, a modification may be necessary or, in some cases, an adaptor lead may be a more appropriate solution. Circular screwed electrical connectors conforming to MIL-DTL-5015 are preferred for use with all role equipment. Contacts in the electrical connectors may be either soldered or removable crimp type, with crimp contacts being preferred due to ease of replacement. Further guidance on determining specific part numbers of electrical connectors is detailed in AAP 7045.002-1, *ADF Aircraft Wiring and Bonding Manual*.

23. ***Overcurrent Protective Devices.*** Where circuit breakers are utilised as overcurrent protective devices they should not be used to fulfil the requirement for an ON/OFF switch unless specifically designed for this purpose.

Environmental Qualification

24. MIL-STD-810 and RTCA/DO-160 provide for a number of tests relating to the physical environment in which an item may be operated. MIL-STD-810 provides guidance in selecting and tailoring tests to satisfy the various equipment and end use requirements. Individual tests should be selected and tailored to satisfy the requirements for the equipment being tested. Listed below are the minimum tests which should be considered when determining the extent of testing, however additional tests may also be deemed necessary.

25. ***Low Pressure (Altitude) – MIL-STD-810F, Method 500.4 or RTCA/DO160, Section 4.*** This test is designed to assess the ability of the equipment to continue to operate in the event of either a rapid or gradual loss of cabin pressure in the aircraft. A sudden reduction in pressure can exploit weaknesses in equipment, leading to mechanical failure. High altitude pressures, whether arrived at gradually or due to sudden decompression, may cause electrical arcing between high voltage components and ground and may also reduce the ability of switches and circuit breakers to satisfactorily interrupt circuits. This test could be combined with low temperature operation or the thermal shock tests detailed below, if considered necessary. The time and pressure change rates should be tailored to represent the most severe operating conditions envisaged. This test is particularly applicable to pressure sensitive equipment.

26. ***High Temperature – MIL-STD-810F, Method 501.4 or RTCA/DO160, Section 4***. This test is designed to ensure that the item can continue to operate in the highest ambient temperatures likely to be experienced, without suffering physical damage or degradation of performance. It is particularly applicable to temperature regulated equipment.

27. ***Low Temperature – MIL-STD-810F, Method 502.4 or RTCA/DO160, Section 4.*** This test is designed to determine whether the item can operate at low temperatures, after a period of storage in that low temperature. Some effects that may be noticed are a reduced battery life and decreased flexibility of leads. Low temperatures could be experienced as a result of a decompression and/or failure of aircraft heating systems as well as operations in cold climates. This test is particularly applicable to temperature regulated equipment.

28. ***Temperature Shock – MIL-STD-810F, Method 503.4 or RTCA/DO160, Section 5***. This test will measure the effects of sudden changes in ambient temperature on equipment. This test is particularly applicable to temperature regulated equipment.

29. ***Humidity – MIL-STD-810F, Method 507.4 or RTCA/DO160, Section 6***. This test will measure the ability of the item to operate in a humid environment, after a period of storage in that environment. This test can be combined with the low temperature test to simulate the effect of transit and operation in high humidity and eventual movement to a cool low humidity environment. This test will reveal problems caused by corrosion and condensation on circuit components and should have humidity/temperature profiles designed to simulate worst case conditions.

30. ***Fungus – MIL-STD-810F, Method 508.5 or RTCA/DO160, Sect 13.*** This test is designed to determine the effectiveness of anti-fungal coatings on circuit materials and the likelihood of fungus growth effecting operation of the equipment. The cycles chosen should be representative of worst case conditions and should be conducted prior to the sand and dust test which may provide nutrients, which could compromise the validity of this test.

31. ***Sand and Dust – MIL-STD-810F, Method 510.4 or RTCA/DO160, Section 12***. This test should determine the effects of using the equipment in dusty conditions such as helicopter operations in dry areas. It is particularly applicable to equipment with exposed moving parts.

32. ***Explosive Atmosphere – MIL-STD-810F, Method 511.4 or RTCA/DO160, Section 9.*** This test should be tailored to suit any anticipated explosive atmospheres that may be encountered in or around aircraft. Low levels of electrical arcing produced by switches, etc. can ignite explosive vapours.

33. ***Vibration – MIL-STD-810F, Method 514.5 or RTCA/DO160, Section 8.*** This test should be tailored to suit the various vibration environments anticipated. When testing equipment, consideration should be given to including mounting hardware such as shock mounts, since these have occasionally been found to cause severe resonance in installed equipment. In addition to testing in the aircraft vibration environment, it may also be necessary to test in the road transport vibration environment to ensure reliable operation.

34. ***Shock – MIL-STD-810F, Method 516.5 or RTCA/DO160, Section 7.*** The operational shock test verifies that the equipment will continue to function after exposure to shocks experienced during normal aircraft operations. The crash safety test is to prove the integrity of mounts on equipment which could break loose in a crash or emergency.

35. ***AME Equipment Tests.*** Aeromedical Clinical Performance Tests (AMCPTs) should be conducted as necessary to ensure that clinical performance of the item is satisfactory in the aviation environment and to ascertain whether new or modified clinical procedures are necessary when using the equipment on AME missions. The requirement for AMCPTs will be dependant upon but not limited to the following factors:

a. Results of clinical tests.

b. Opinions of qualified military medical personnel with experience in AME work.

c. Results of laboratory clinical tests which indicate marginal performance and

d. The need to develop special mounting and/or securing devices to enable the item to be used effectively on AME missions.

Physical Compatibility

36. ***Mounting and Securing.*** Devices for mounting the item in an aircraft should not restrict the operation of the item. Removable attachments, when not in use, should be securely stowed on the equipment.

37. ***Electrical Connections on AME.*** With respect to AME Equipment, civilian medical agencies generally comply with the International Society of Aeromedical Services (Australia) with regard to standardisation of electrical power supplies and connectors. This standard contains the following requirements for electrical power:

a. Standard Receptacle – MS3102E20-19S (solder), MS3452L20-19S (crimp), Qty 3, Size 8 AWG socket contacts.

b. Mating Plug – MS3106E20-19P (solder), MS3456L20-19P (crimp.

c. Pin A – Earth (Common).

d. Pin B – Positive 12 Volts DC and

e. Pin C – Positive 24/28 Volts DC.

Ease of Operation

38. Operating role equipment while airborne can present difficulties not encountered on the ground, including operation in turbulence, vibration, low light, cramped conditions, and so on. The factors listed below may assist in obtaining satisfactory performance while airborne.

39. ***Control Locking Devices.*** Locking devices for equipment controls should be capable of retaining the control in any given setting. The locking and unlocking action should be easily and quickly accomplished and not affect the control setting.

40. ***Control Setting Stability.*** Controls should be designed so that the setting does not change when the equipment is subjected to its intended service conditions.

41. ***Rotary Switches.*** Rotary switches should have a positive mechanical indexing for each position. The indexing mechanism should be designed to minimise the possibility of the moveable element coming to rest between contact positions.

42. ***Toggle Switches.*** Toggle switches should operate in the vertical rather than horizontal plane with the OFF position being either the centre or bottom position.

43. ***Signal and Warning Devices.*** Signal and warning devices should satisfy the following requirements:

a. ***Audible Alarms***. Audible alarms should not be the only warning of malfunction as they may be impossible to hear in a noisy aircraft environment. If possible, audio warnings for critical functions should be audible under all operating conditions.

b. ***Mechanical 'Flag' Signals***. Mechanical 'Flag' signals should only be used to indicate ON-OFF type information.

44. ***Protection of Operating Controls.*** Operating controls should be protected from accidental damage or inadvertent operation by personnel brushing past the equipment. In the operating position all instrument readings, control settings and chart recorder outputs should be readily visible and accessible to the operator in the normal operating posture.

45. ***Marking Requirements.*** All controls should be marked to indicate function and position. The marking should be of a type that will not deteriorate or become illegible during normal use.

46. ***Special Tools.*** The requirement for special tools for installation and operation should be kept to a minimum. Where special tools are required, secure stowage provisions should be available on the equipment.

CONTINUED AIRWORTHINESS

47. A review system should be in place that will appraise the effects all new aircraft configuration changes may have on role equipment, or the role equipment may have on the modified aircraft. For example, EMI/EMC test plans should consider all role equipment that can be operated on the aircraft. In addition, any configuration changes to role equipment should be assessed to ensure they do not affect aircraft airworthiness.

SPECIFICATIONS AND PUBLICATIONS

48. The following is a list of specifications and publications which provide information relating to role equipment:

a. AS 2901-1986 – Medical Devices, Characteristics of Audible and Visual Alarms.

b. AS 3200.1.0-1998 – Approval and Test Specifications, Medical Electrical Equipment.

c. AS 3201 TO 3211 – Australian Standards which relate to Specific Items of Medical Equipment.

d. CAAP No: 35-5(0) – Design and Fitting of Oxygen Systems: Non Required Gaseous Oxygen Equipment.

e. CISPR 11 – 2004 Industrial, Scientific and Medical (ISM) Radio-frequency Equipment - Electromagnetic Disturbance Characteristics - Limits and Methods of Measurement.

f. MIL-STD-461E – Requirements for the Control of Electromagnetic Interference Characteristics of Sub-systems and Equipment.

g. MIL-STD-464A – Electromagnetic Environmental Effects Requirements for Systems.

h. MIL-STD-810F – Environmental Test Methods and Engineering Guidelines.

i. RTCA/DO-160E – Environmental Conditions and Test Procedures for Airborne Equipment.

j. STANAG 3204 – Aeromedical Evacuation.

k. ADFP 703 – Management Procedures for Medical and Dental Materiel.

l. DI(AF) AAP 3504.001 – Hazardous Goods Management.

m. AAP 7045.002-1 – ADF Aircraft Wiring and Bonding Manual.

n. DI(AF) AAP 7279.010 – Aerial Delivery Design Handbook.

o. DI(AF) PERS 57–3 – Approvals for Use of Aeromedical Evacuation Equipment.

p. ASIC AIR STD 61/115/19A Aero Medical Evacuation.

q. FAA Advisory Circular AC135-5 - Maintenance Program Approval for Carry-On Oxygen Equipment for Medical Purposes.

Blank Page

SECTION 2

CHAPTER 15

UNMANNED AERIAL VEHICLES

INTRODUCTION

1. Unmanned Aerial Vehicles (UAVs). This is one interpretation of the acronym 'UAV'. Other common variants include 'Uninhabited' or 'Unoccupied' in lieu of 'Unmanned', and 'Air', 'Aerospace', 'Aviation' or 'Airborne' in lieu of 'Aerial'. The FAA has recently adopted the term Remotely Operated Aircraft (ROA). UAVs operated within the ADF are subject to the same airworthiness regulatory requirements as conventional aircraft. However, neither DEF STAN 00-970, FARs, MIL-STDs or CARs prescribe comprehensive design requirements for UAVs, although each sponsoring agency has acknowledged the requirement. For example, CASA has drafted recommendations and guidance for UAV operations, design specification, maintenance and training (AC 101.1(0)).

2. Direct application of design requirements for conventional aircraft to UAV design is problematic, since they are primarily concerned with ensuring the safety of aircraft occupants. UAV design requirements, on the other hand, should be targeted primarily at ensuring the safety of other aircraft and ground-based facilities and personnel. The scope of design requirements for UAVs is therefore heavily dependent on the role in which the UAV is to be employed. This chapter provides airworthiness design requirements and operational considerations for UAVs employed by the ADF as State aircraft.

APPLICABILITY

3. This instruction is applicable to all new and existing UAVs being operated as State aircraft. In the context of this chapter, the term 'UAV' refers to the entire UAV system, not just the airborne component. As such, it also includes the ground control station and datalink, plus any ground-based launch and recovery systems.

4. Although they may be described as UAVs, model aircraft and 'smart' destructive weapons (except those carried as a payload on a UAV), are not covered in this chapter. The delineation between a model aircraft and a UAV is not rigid, however, a model aircraft is generally a small unmanned aircraft used for sport and recreation and operated within visual range below 400 feet.

AIRWORTHINESS DESIGN REQUIREMENTS

5. The scope of design requirements for a UAV is dependent upon the role in which the UAV is to be employed. This section provides a generic set of design requirements for all UAVs operated as State aircraft, supplemented with specific requirements for UAVs whose role includes operation over populous areas or in non-exclusive airspace.

Generic Design Requirements

6. All UAVs, regardless of role or operating environment, should conform to a minimum set of airworthiness design requirements. These requirements are aimed at ensuring that the UAV:

a. is adequately controllable, reliable and structurally sound (that is, safe to operate); and

b. will not inadvertently venture outside its assigned airspace and/or over populous areas.

The following set of design requirements is aimed at assuring an acceptable level of safety for UAVs operated under the ADF airworthiness system. For a UAV that is well away from populous areas and the sole aircraft operating in exclusive airspace, these requirements may be sufficiently comprehensive if the hazard presented by any design shortfall is shown to be offset by the low risk of collateral damage.

7. ***System Safety and Hazard Analysis.*** UAV operations should be as safe as manned aircraft, such that the hazard presented to persons or property in the air or on the ground, should be no greater than that posed by manned aircraft of equivalent class or category. Central to the ADF's assessment of the UAV's design integrity is the system safety and hazard analysis (SSHA). The SSHA is a mandatory requirement of designers, and must comprehensively examine all potential hazards through all flight phases, and throughout the entire operational spectrum required of the

UAV. It is only through such a comprehensive analysis that an assessment of each of the design requirements in the following paragraphs can be made. Annex A contains specific SSHA guidance for UAVs, to supplement the generic SSHA guidance provided at Section 2 Chapter 1 of this manual.

8. ***Air Vehicle Sub-system Requirements.*** The design requirements for each of the critical air vehicle components of the UAV system are as follows:

a. ***Structure.*** The structural design criteria for UAVs should normally conform to the equivalent design standards for conventional aircraft (for example, FAR 23 structural requirements). Where restrictions in role justify the application of reduced standards (for example, the UAV will not be flown in potential icing conditions), the role restrictions are to be clearly annotated in the flight manual.

b. ***Flight Control.*** The UAV flight control system is split between the air vehicle and the Ground Control Station (GCS). Within the air vehicle component, any single point of failure should not affect the ability to control UAV recovery. Provisions for possible reversion to degraded modes of operation should also be incorporated into the design, and the UAV should remain controllable in the event of a propulsion system failure. The criticality of each flight control system component should be clearly defined in the SSHA, and appropriate design and qualification rigour should be applied.

c. ***Safe Recovery Systems.*** The fitment of an automatic on-board system for safe recovery of the UAV, should positive control be lost, is a mandatory requirement for all ADF UAVs regardless of role. The two common safe recovery systems are the flight termination system (FTS) and the autonomous recovery system (ARS), and either is satisfactory in isolation (although preference should be given to UAVs fitted with both systems). The failure of any component associated with the safe recovery system should be immediately advised to the ground controller. Also, the capability to automatically engage the safe recovery system if the UAV inadvertently exits its assigned area should be pre-programmable. Specific requirements for each system are as follows:

(1) ***Flight Termination System.*** A FTS is an on-board system which is independent of the vehicle's propulsion and flight control systems, and provides a means to safely terminate the flight in all phases of flight operations (commonly a parachute). The FTS must be capable of being activated from the GCS and, if an autonomous recovery system is not fitted, then the FTS must be capable of being pre-programmed for automatic deployment when specific failure conditions occur (for example, loss of uplink signal or failure of an essential system).

(2) ***Autonomous Recovery System.*** An ARS engages a pre-programmed course of action to recover the UAV should specific failure conditions occur. For example, the ARS may direct the UAV to transit to a pre-designated recovery area, and then execute a recovery sequence (for example, spiralling slowly down to the ground). The ARS must be capable of being pre-programmed to engage when specific failure conditions occur, in particular loss of datalink signal. The GCS must have the capability to over-ride the ARS once it is activated, for example if the datalink is re-established.

d. ***Electrical.*** The electrical system should provide sufficient power and endurance to ensure safe operation and recovery throughout all phases of flight, including all conceivable emergency scenarios. Non-essential load shedding should be incorporated in the event of generator failure if the batteries are inadequate to effect safe recovery under worst-case role conditions. Changes in the health status of the electrical system (for example, generator failure) must be advised to the GCS. The electrical system should include spare load capacity (preferably 50%) for future expansion. To enable future flexibility in airborne equipment and payloads, electrical power characteristics should be in accordance with MIL-STD-704E. Unlike manned aircraft, PVC-insulated wire is acceptable, while polyimide-insulated wire is acceptable but not preferred.

e. ***Navigation.*** Navigation performance requirements for a UAV operating in exclusive airspace and away from populous areas are driven primarily by the UAV's operational requirements. However, for UAVs fitted with an ARS that relies on the navigation system, and no FTS, the navigation systems must be considered essential and therefore be designed to be appropriately reliable. A specific level of navigation accuracy is not an essential airworthiness requirement, provided the system is adequate to ensure the UAV remains within its allocated exercise area and that the ARS functions adequately.

f. ***Propulsion.*** The system safety analysis, tailored for the UAV's intended role, should define the reliability requirements for the propulsion system. Notwithstanding this, the UAV should remain controllable in the event of a propulsion system failure. The existence of a flight termination system (eg parachute) should not be accepted as a replacement for adequate propulsion system reliability. The probability of an uncontained engine failure should be identical to that for manned aircraft.

g. ***Payload.*** Some UAVs can accept a variety of payloads, for example daylight cameras, infrared cameras, and so on. Each of these payloads must be assessed for its impact on the technical airworthiness of the UAV, and a list of approved payloads included in the Flight Manual. The factors to be considered when assessing the payload for suitability are similar to the fitment of role equipment in manned aircraft, for example impact on weight and balance, suitability of mountings, impact on electrical system capacity, cooling requirements and electromagnetic compatibility.

9. ***Ground-Based Sub-system Requirements.*** The design requirements for each of the critical ground-based components of the UAV system are as follows:

a. ***Control Station.*** The GCS shall display clear and unambiguous aircraft systems and attitude information to the supervising controller, to enable safe operation, control and navigation. It should also include a diagnostic and monitoring capability for the status of the air vehicle, and should clearly advise of any degraded mode of operation due to any failure, including cases in which there is an automatic switching to a backup mode. Human factors should be paramount in the design of the GCS console, to minimise the potential for human error. In particular, instruments and controls should reflect the standard pilot's cockpit layout as closely as possible, as defined in DEF STAN 00-970 chapter 107. Any departures should be justifiable in terms of improved safety and should be clearly identified in the flight manual. The GCS is a safety-critical component of the UAV system, and accordingly appropriate design and construction standards should be employed. The existence of a FTS and/or ARS should not be used as justification for inadequate design rigour and qualification of the GCS.

(1) Where a UAV is exclusively computer controlled (ie without manual intervention), a full flight instrumentation presentation may not be necessary. Instead, presentation of power and performance may be adequate, provided any departure from assigned parameters results in an alarm or FTS operation.

b. ***Datalink.*** The SSHA should define the criticality of the datalink within the UAV system, and the design and qualification rigour should be appropriate to the criticality. At a minimum, any single failure of the UAV communications system (uplink or downlink) should not affect normal control of the UAV. Datalinks are susceptible to electromagnetic interference, and should be adequately protected from this hazard. The range and azimuth characteristics of the datalink should be comprehensively mapped throughout the operational envelope of the UAV and any limitations included in the flight manual. Datalink signal strength should be continuously monitored and appropriate datalink range cues should be provided to the GCS controller. Operating frequencies should be endorsed by the ADF spectrum management authorities. The existence of a FTS and/or ARS should not be used as justification for inadequate design rigour and qualification of the datalink system.

c. ***Launch and Recovery Systems.*** Some UAVs require an external launch aid, for example a rocket assisted take off (RATO). Others use ground-based recovery systems such as arrestor barriers or hook wires. In each case, the SSHA should clearly define the inherent hazards, and appropriate design steps should be taken to reduce the hazards to an acceptable level.

10. ***Qualification and Verification.*** Qualification and verification programs for each ground-based and air vehicle-based UAV sub-system, appropriate to each sub-system's criticality (as defined in the SSHA) should have been completed. All testing should be shown to be directly relevant to the ADF's intended configuration, role and operating environment. Evidence of appropriate electromagnetic environmental effects (E^3) testing should also be verified.

11. ***Type Record.*** Section 1 Chapter 4 of this manual details the type record requirements for ADF aircraft, and these are equally applicable to UAVs.

Additional Design Requirements for Operation Near Other Aircraft

12. The generic UAV design requirements in paragraphs 6 to 11 were based on the premise that the UAV would be operating in exclusive airspace. However, when the UAV's intended operating role does not preclude other military aircraft in proximity, or the UAV is to be operated outside military restricted airspace, additional precautions are necessary. The following additional design requirements, supplementing those generic requirements presented above, are necessary to assure an acceptable level of safety for UAVs not operating in isolation.

13. ***Operation within Military Restricted Airspace.*** If the UAV's intended operating role permits other military aircraft in its vicinity, the following additional requirements are necessary:

a. the system safety analysis should be expanded to account for the additional hazards presented by other military aircraft in the vicinity, and each of the generic requirements listed in paragraphs 6 to 11 revised accordingly;

b. anti-collision and navigation lights equivalent to those required for manned aircraft (eg FAR 23.1401) are to be fitted and controllable from the GCS while the vehicle is airborne, and are to be used at all times while airborne (unless strategic requirements dictate otherwise);

c. a means of immediate communication between the GCS controller and the nearest air traffic control (ATC) station, whether military or civilian, is to be provided; and

d. an altitude encoding transponder, meeting the requirements of FAR 91.215, is to be fitted and controllable from the GCS while the vehicle is airborne (eg resetting the transponder code).

14. ***Operation in Civilian Airspace.*** For an ADF UAV to operate in civilian airspace, CASA's requirements for UAVs should be met. The following requirements have been included in CASA's draft Advisory Circular 101.1(0):

a. the UAV should be fitted with a fail-safe flight termination system (the need for this feature will be given greater emphasis where operations will be within or near to controlled airspace);

b. provisions for full and immediate communications via two way radio between the supervising controller and the appropriate ATC shall be available, regardless of location;

c. position lights and anti-collision lights shall be fitted, and will normally be turned on at all times while the UAV is in motion;

d. for operation in controlled airspace, and where otherwise required by CASA, an operable SSR transponder shall be fitted (mode 3A and C) and the controller shall have the capability to turn it on/off, manually select codes and squawk in flight (CASA may approve operation without in-flight resettable SSR codes on a case-by-case basis);

e. CASA may require the UAV to be equipped with a collision avoidance system when required for use in the vicinity of manned aircraft (however, not all manned aircraft will have this equipment and therefore its applicability for UAVs will be selective);

f. CASA may require the GCS to have a recorder fitted to record UAV systems and navigational status, and radio and intercom voice communications;

g. the navigation systems should meet required navigation performance standards of the flight rules and the specific requirements for the airspace in which operations are to be conducted; and

h. only navigation systems meeting the requirements for 'sole means navigation' will normally be considered for flights under IFR and in controlled airspace.

Additional Design Requirements for Operation Over Populous Areas

15. The generic UAV design requirements in paragraphs 6 to 11 were based on the premise that the UAV would not be used near or over populous areas. However, if the UAV's intended operational role requires it to be used near or above populous areas, there is a real danger that a UAV systems failure could endanger ground-based personnel and facilities. A reasonable public expectation is for UAVs to pose no greater risk to them than conventional aircraft, and this should be the ADF's requirement before endorsing a UAV for this role. The following additional design requirements, supplementing those generic requirements presented in paragraphs 6 to 11, are necessary to assure an acceptable level of safety for UAVs operating near or over populous areas.

16. ***System Safety Analysis.*** In addition to the SSHA requirements at paragraph 7, the SSHA must specifically address the failure conditions that could lead to the UAV crashing, or being unable to reach a designated safe recovery area. If the existence of a flight termination system is to be used as a risk mitigator, the probability of failure of this system must also be comprehensively assessed, including multiple point and undetected failures.

17. ***Air Vehicle Sub-system Requirements***. The design requirements for each of the critical air vehicle components of the UAV system, in addition to those listed in paragraph 8, are as follows:

a. ***Structure.*** The potential for items detaching from the UAV in flight must be equivalent to that for conventional aircraft.

b. ***Flight Control.*** The UAV must remain controllable in the event of a propulsion system failure, so that the UAV can be guided to a safe landing zone. The criticality of the flight control system should be clearly defined as a result of the SSHA, and design and qualification rigour, equivalent to that on conventional aircraft, should be applied.

c. ***Safe Recovery.*** The fitment of a flight termination system, independent of the vehicle's propulsion and flight control systems, is an essential requirement for operating UAVs above or near populous areas. The FTS must be capable of being activated from the Ground Control Station (GCS) and must be capable of being pre-programmed for automatic deployment when specific failure conditions occur. The SSHA must comprehensively assess the potential failure modes of the FTS, both single and multi-point. Limitations in the deployment of the FTS (for example, minimum altitudes, drift rates, etc) should be accurately defined and clearly documented in the flight manual, so that appropriate risk mitigation strategies can be adopted. Should datalink be lost, the UAV must not automatically deploy the FTS, rather it must autonomously transit to a pre-determined safe landing area (away from the populous area) before deploying. The capability to program a number of safe landing areas should be available, commensurate with the size of the populous area being overflown.

d. ***Navigation.*** The navigation system performance should be determined by the SSHA. Primarily, it must always provide the GCS controller with sufficiently accurate location information to enable the UAV to be safely navigated away from the populous area. The size of available safe landing areas will be a determining factor in the required navigation system performance.

18. ***Qualification and Verification.*** Qualification and verification programs for UAVs operating near or above populous areas will inherently be more extensive than that required in paragraph 10. Similar qualification and verification requirements to conventional aircraft would normally be expected.

TAR REQUIREMENTS FOR TYPE CERTIFICATION

19. Section 1 Chapter 1 of this manual outlines the technical airworthiness requirements for ADF aircraft, and these are equally applicable to UAVs. The existence of a comprehensive certification basis underpins these technical airworthiness requirements, and Section 1 Chapter 2 provides guidance on producing and managing a certification basis. As with manned aircraft, prior certification by an airworthiness authority recognised by the ADF may be acceptable, but only to the extent that the existing certification basis can be shown to be relevant to the configuration being acquired, and the ADF's intended roles and operating environment. Annex B contains an example of how a modified version of FAR 23 could be used as a certification basis for a UAV. Guidance for establishing compliance with the certification basis is presented in Section 1 Chapter 3.

20. For UAVs that are to be operated uniquely under an ADF Special Flight Permit (for example, as part of a capability trial), the requirements in paragraph 19 may be unnecessarily onerous. In this case, the duration of the trial and the intended role for the UAV will influence the level of assurance required by the Commonwealth. For example, for a short-term UAV trial conducted over an unpopulated area in exclusive airspace, the data required would probably be minimal. On the other hand, an extensive trial of a large, high speed UAV to be operated in civilian airspace and over major cities would require substantially more supporting data. Annex C contains guidance on the requirements for substantiating data for a UAV to be operated uniquely under a SFP.

OPERATIONAL CONSIDERATIONS

21. The distinction between technical and operational airworthiness issues for a UAV is even less distinct than with conventional aircraft. The preceding sections examined the requirements necessary to assure a technically airworthy UAV system. Like conventional aircraft, appropriate operating procedures are necessary to assure overall safety. Unlike conventional aircraft, however, the lack of aircrew situational awareness demands that additional risk mitigation strategies be adopted for UAVs.

22. FAR 23.1585 (*Operating Procedures*) requires that information concerning normal, abnormal and emergency procedures and other pertinent information necessary for safe operation must be furnished. It provides a comprehensive list of topics to be included, and these are equally relevant to UAV operations. However, there are additional requirements for UAVs that also need to be included, and these are examined at Annex D.

References:

A. CASA Advisory Circular AC 101.1(0), *Unmanned Aerial Vehicle (UAV) Operations, Design Specification, Maintenance and Training of Human Resources*. (Draft, October 98)

B. NAVAIR Instruction 13034.2, *Flight Clearance Policy for Unmanned Aviation Services*. (Draft, May 99)

C. NAVAIR, *Range Safety Criteria for Unmanned Air Vehicles.* (Draft, 18 Mar 99)

D. FAA Notice 7610.71, *Department of Defense Remotely Operated Aircraft (ROA) Operations.* (19 Mar 99)

E. ABR 5291, *Unmanned Aerial Target Flight Instructions.* (Interim Edition Feb 99)

Annexes:

A. UAV SSHA Guidance

B. Example UAV Certification Basis

C. Special Flight Permit Technical Data Requirements

D. UAV Operational Considerations

UAV SSHA GUIDANCE

1. There is a difference in safety emphasis between manned aircraft and UAVs, since the former aims to maximise occupant safety whilst the latter aims to minimise collateral damage. Regardless, the underlying intention to produce a safe aircraft is the same, and therefore the system safety and hazard analysis (SSHA) requirements for UAVs are predominantly the same as for manned aircraft. The main difference is likely to be in the mitigation strategies adopted for identified hazards, since the intended role for a UAV can be used as an offset for a particular hazard. For example, a hazard that is unacceptable on a manned aircraft may be assessed as acceptable on a UAV that will always be operated well away from populous areas. It should therefore be evident that establishing the *intended role* for the UAV is a critical step in the SSHA process. Without this step, the UAV's role cannot be used to mitigate risk, and therefore the UAV would need to meet identical design requirements to manned aircraft.

2. Section 2 Chapter 1 of this manual contains SSHA guidance for manned aircraft, and this is equally applicable to UAVs. Realistically, however, UAV manufacturers are unlikely to employ similar rigour for a UAV, particularly one perceived to be employed in a low risk role. Notwithstanding this, a SSHA for a UAV is unlikely to be acceptable to the Commonwealth if it does not address at least the following minimum criteria:

a. for the airborne UAV system:

(1) a comprehensive hazard assessment of structures, flight controls, electrical, navigation and propulsion systems throughout all phases of flight (nominally launch, transit, mission and recovery);

(2) a thorough assessment of failure modes for the FTS and ARS (as applicable), in particular single and multiple point failure modes, potential undetected failure modes, and so on;

(3) an assessment of payload failure possibilities and consequences;

(4) an assessment of the probability of a system failure resulting in the UAV exiting its assigned exercise area;

(5) an assessment of the probability of a system failure resulting in the UAV crashing; and

(6) a comprehensive assessment of software failure modes and probabilities, in particular related to safety-critical software;

b. a hazard assessment of all ground-based UAV systems, including ground control station, datalink, launch and recovery systems, and so on;

c. justification for all low failure probabilities; and

d. evidence of mitigation of significant hazards (both software and hardware) in both the airborne and ground-based UAV system, appropriate to the UAV's intended role, configuration and operating environment.

3. For each of the requirements listed above, comprehensive coverage should be expected for all failure possibilities, including probability estimates, appropriate corrective actions and preventative measures. Direct applicability of the SSHA must be shown to the ADF's intended configuration, role and operating environment.

Blank Page

EXAMPLE UAV CERTIFICATION BASIS

1. A certification basis is a comprehensive set of airworthiness design requirements which must be met to assure the ADF that an aircraft configuration is airworthy for an intended role and operating environment. For conventional aircraft, FARs or DEF STAN 00-970 present a comprehensive set of airworthiness requirements, and therefore provide a convenient foundation for a certification basis. In time, similar sets of airworthiness requirements will be produced specifically for UAVs. In the meantime, the airworthiness requirements for conventional aircraft can also be used for UAVs, provided that suitable tailoring is incorporated to account for differences in role and configuration.

2. An example certification basis is included in the following table, based on FAR 23 requirements. FAR 23 was chosen because most military UAVs appear to be manufactured in the USA, and most UAVs are fixed wing and relatively small. These airworthiness requirements should be tailored to remove requirements that cannot be justified for the intended UAV operations. Conversely, airworthiness requirements should be added where similar requirements do not exist for manned aircraft (eg FTS, ARS, RATO launch systems, etc). Where a particular UAV does not meet an essential airworthiness requirement, it may be possible to procedurally mitigate the shortfall.

Table 15–B–1 Example UAV Certification Basis

Requirement	Applicable FAR References	Comments
UAV Category	23.3	Assess whether the UAV falls into the *normal*, *utility* or *acrobatic* category, and apply to all following requirements. Disregard all *commuter* category requirements.
Flight Requirements	23.21 - 23.53 23.55 23.57 - 23.71 23.73 - 23.77 23.141 - 23.231 23.233 - 23.235	 This requirement may be omitted for UAVs that solely use arrestor cables or parachutes for landing. These requirements may be omitted for UAVs that use a parachute as their sole means of landing. Disregard all references to stick force limits. The ability to taxi is not an essential UAV requirement.
Structural Requirements	23.301 - 23.395 23.407 - 23.473 23.477 - 23.505 23.507 23.509 - 23.511 23.521 - 23.537 23.571 - 23.575	 These requirements may be omitted for UAVs that use a parachute as their sole means of landing. These requirements may be omitted for UAVs that are not designed to be towed.
Design and Construction	23.601 - 23.703 23.723 - 23.733 23.735 23.737 - 23.757 23.787 23.863 - 23.871	 The undercarriage landing requirements may be omitted for UAVs that use a parachute as their sole means of landing. The undercarriage take-off requirements may be omitted for UAVs that use non-conventional take-off (eg RATO). This requirement may be omitted for UAVs that solely use arrestor cables or parachutes for landing. (a)1 and (a)2 only.
Powerplant	23.901 - 23.925 23.929 23.933 - 23.1091 23.1093 23.1095 - 23.1125 23.1143 - 23.1203	 Ice protection is an airworthiness requirement only if the UAV is to be used in potential icing conditions. Ice protection is an airworthiness requirement only if the UAV is to be used in potential icing conditions.

Table 15B–1 Example UAV Certification Basis (cont)

Requirement	Applicable FAR References	Comments
Equipment	23.1301 - 23.1401 23.1303 - 23.1305 91.205 23.1307 - 23.1309 23.1311 - 23.1322 23.1323 - 23.1367 23.1383 23.1385 - 23.1401 23.1416 - 23.1419 23.1431 - 23.1438 23.1459 23.1461 91.207 91.215	 These flight, navigation and powerplant instruments are located on the ground control station. These additional instrument and equipment requirements for IFR flight must be located on the ground station. Taxi lights and landing lights are not an airworthiness requirement. Ice protection is an airworthiness requirement only if the UAV is to be used in potential icing conditions. A Flight Data Recorder on the UAV is not an airworthiness requirement provided that all telemetry from the UAV is recorded on the ground station. Emergency locator transmitters are not an airworthiness requirement. However, if fitted, they must conform to these requirements. (ATC transponders)
Operating Limitations	23.1501 - 23.1522 23.1581 - 23.1589	Guidance on information that should be included in the UAV operating procedures is included in Annex D.
Emergency Recovery System	(no equivalent in FAR 23)	Airworthiness requirement for this system, applicable to the role of the UAV, should be inserted here.
Flight Termination System	(no equivalent in FAR 23)	Airworthiness requirement for this system, applicable to the role of the UAV, should be inserted here.
UAV Control Station	(no equivalent in FAR 23)	Airworthiness requirement for this system, applicable to the role of the UAV, should be inserted here.
Data Link	(no equivalent in FAR 23)	Airworthiness requirement for this system, applicable to the role of the UAV, should be inserted here.
Payload	(no equivalent in FAR 23)	Airworthiness requirement for this system, applicable to the role of the UAV, should be inserted here.

SPECIAL FLIGHT PERMIT TECHNICAL DATA REQUIREMENTS

1. A full type certification program may not be warranted for a UAV on short-term attachment to the ADF, for example participating in an ADF capability trial. In such cases, the ADF Airworthiness Authority may elect for the UAV to operate uniquely under a Special Flight Permit. However, the ADF would still require some assurance (beyond the UAV manufacturer's assertion) that the UAV was technically safe to fly in the intended role before endorsing the issue of a Special Flight Permit. That is, the ADF would require assurance that the UAV should:

a. remain in control and within its designated exercise area,

b. not pose an unreasonable threat to personnel or facilities on the ground, and

c. not pose an unreasonable threat to other aircraft within the exercise area.

2. The intended role of the UAV will have a significant impact on the level of assurance required by the ADF. This annex presents the ADF's data requirements for two example UAV trial scenarios, one inherently low risk and the other inherently higher risk. Most UAV trials would probably fall somewhere between these two extremes, and therefore appropriate tailoring of these lists should be used. The degree to which prior certification by a recognised airworthiness authority can be shown to be relevant to the intended role, configuration and environment, would also influence the ADF's assurance requirements.

Lower Risk Trial

3. If a UAV is to participate in an ADF trial with low inherent risks (for example, short duration, small UAV, well away from populous areas, exclusive use of airspace, etc), the following data would probably be required:

a. A complete description of the UAV system configuration, including air vehicle and land-based components.

b. A full list of all design and construction standards used for the UAV (copies of documents should be provided upon request).

c. A full list of all qualification and verification reports (copies of documents should be provided upon request).

d. All system safety analysis documentation.

e. The UAV flight manual.

f. An assessment of the probability of a critical UAV system failure leading to the UAV impacting the ground.

g. An assessment of the probability of a critical UAV system failure leading to the UAV exiting the exercise area.

h. Evidence that the intended payload(s) have been fully qualified for the offered UAV in the intended role.

i. An overview of the engineering management and logistics support arrangements that will be established to assure the continued airworthiness of the UAV and

j. Details of any prior certifications by a recognised Airworthiness Authority, including an assessment of their relevance to the ADF's intended role, configuration and environment, plus details of the evidence that was provided for the prior certification (eg basis for certification, and so on).

4. Based on the above data, the ADF should be able to gain adequate assurance that the UAV was designed, developed, constructed, and qualified with at least a basic level of rigour, and that appropriate engineering

management and logistics support arrangements will be available. Should the data not provide this assurance, the ADF may require additional data or may apply restrictions to the approved role.

Higher Risk Trial

5. If a UAV is to participate in an ADF trial with higher inherent risks (for example, high speed UAV, large airframe, near or over populous areas, within civilian controlled airspace, etc), the following data would probably be required:

a. A complete description of the UAV system, including the air vehicle and land-based components.

b. Basic drawings of the UAV, including dimensions, materials, physical features and so on.

c. A full list of design standards employed and evidence of compliance with these standards, including details of any tailoring.

(1) If proprietary or obscure design standards were employed, a comparison of that standard with an accepted ADF standard may be required.

d. A full listing of design documents for the UAV system, with the expectation that the ADF will require access to some or all of these documents.

e. A full list of all qualification and verification reports for the UAV system, with the expectation that the ADF will require access to some or all of these reports.

f. Evidence of qualification testing of the payloads, appropriate to the intended role of the UAV.

g. A copy of all system safety analysis (SSA) documentation for the UAV air vehicle and ground-based components.

h. Evidence of mitigation of significant hazards highlighted in the SSA (both hardware and software), in particular:

(1) Those failure modes leading to catastrophic failure of the UAV.

(2) Single point failure modes in critical systems and

(3) Failure modes in the flight termination system and/or automatic recovery system.

i. A copy of the flight manual, operating procedures, and so on.

j. A full safety history of the UAV system, including mishap history, corrective actions and so on.

k. A detailed assessment of the engineering management and logistics support arrangements that will be established to assure the continued airworthiness of the UAV.

l. A comprehensive list of ‘accepted technical risks’ that must be mitigated by operational procedures and

m. Details of any prior certifications by a recognised Airworthiness Authority, including an assessment of their relevance to the current intended role, configuration and environment, plus full details of the evidence that was provided for the prior certification (eg basis for certification, and so on).

UAV OPERATIONAL CONSIDERATIONS

1. FAR 23.1585 (*Operating Procedures*) requires that information concerning normal, abnormal and emergency procedures and other pertinent information necessary for safe operation of an aircraft must be furnished. It provides a comprehensive list of topics to be included, and these are equally relevant to UAV operations. However, there are some additional requirements, specific to UAVs, that also need to be considered. CASA Advisory Circular 101.1(0) requires that, prior to commencement of UAV operations, UAV operating personnel establish Local Operating Procedures for:

a. ground UAV operations,

b. flight plan filing procedures,

c. integration of UAVs into local traffic pattern,

d. UAV take-off and landing procedures,

e. local airspace restrictions,

f. noise abatement procedures,

g. right-of-way rules,

h. communications requirements,

i. ‘safe areas’ for UAV flight termination, and

j. UAV emergency procedures.

2. These requirements are equally applicable to ADF operations, and should be used as the basis for establishing UAV Standard Operating Procedures. The aim of this annex is to provide guidance on some of the additional factors that should be considered by UAV operators to maximise safety when establishing their operating procedures.

RISK MITIGATION

Vulnerabilities

3. The technical airworthiness review process will establish whether the UAV is technically adequate to perform the intended role. When establishing the complementary operational procedures, the following factors should be taken into account for all phases of flight (ie launch, transit, mission and recovery):

a. What are the main vulnerabilities of the zone in which UAV operations are to be conducted, in particular:

(1) What is the density of both civilian and service personnel on the ground?

(2) What is the density of facilities on the ground, and what are the hazards associated with these facilities (for example, fuel farms, politically sensitive facilities, etc)?

(a) While reference is made only to ‘facilities’ and ‘vehicles’ in this annex, the considerations are equally applicable to water craft if the UAV is to be operated over water.

(3) What is the potential density of civilian and military air traffic ?

b. Can operational procedures effectively overcome any significant technical limitations identified during the technical assessment ?

c. Could civilian personnel, vehicles or aircraft stray into the exercise area ?

d. How effective are the measures taken to ensure that civilian personnel, vehicles and aircraft do not stray into the exercise area ?

e. How effective are the measures taken to ensure that the exercise area is clear of civilian personnel, vehicles and aircraft before flying commences ?

f. What level of risk is acceptable to civilian personnel and facilities ?

g. Is a different level of risk acceptable to military personnel and facilities ?

4. For each of the vulnerabilities listed above, measures are needed to reduce, mitigate or (preferably) eliminate the risk. Where a safeguard is needed to reduce risk, an assessment of the potential failure modes for the safeguard are also needed.

Flight Over Populous Areas

5. Flight over populous areas presents the greatest source of UAV danger to personnel and facilities, and accordingly must be carefully planned. Draft CASA Advisory Circular 101.1(0) Section 6, for example, provides some basic guidance for operating UAVs over populous areas. It suggests that flights over populous areas will primarily be limited to large UAVs, although some small UAVs may be capable if appropriate design requirements are met. Central to the advisory circular is that emergency procedures must be established to ensure that the UAV can clear the area in the event of a failure. It does not, however, provide guidance on the types of emergency procedures that should be used.

6. If at all possible, ADF UAVs should not be operated over populous areas. Where such operations are not required, procedures should be established to prevent the UAV inadvertently straying over populous areas. If flight over populous areas is required, then the following risk mitigation factors should be considered:

a. Where possible, routes and altitudes should be selected to minimise the possibility of the UAV falling into congested areas (eg shopping centres, hospitals, schools) and vulnerable properties (eg fuel farms) in the event of a malfunction, particularly during higher risk phases of flight.

b. Emergency procedures should be established for likely UAV failure modes, that is, engine failure, loss of data link, loss of control, failure of navigation and airframe damage. Some UAVs are fitted with parachutes, and this may simplify the emergency procedures. However, a parachute should not automatically be assumed adequate for all failure modes, and additional emergency procedures may still be necessary.

Flight in Non-Exclusive Airspace

7. The FAA clearly assigns responsibility for airspace safety when UAVs are operating in Notice 7610.71, stating that ‘the proponent and/or its representatives shall be noted as responsible at all times for collision avoidance maneuvers with nonparticipating aircraft and the safety of persons or property on the surface’. Some considerations to mitigate risk may include:

a. ensuring that boundaries of the operational airspace are explicitly defined and recognised by other airspace users;

b. where the capability exists, that the airspace within and near the operational airspace is monitored for traffic that may conflict; and

c. controlling the airspace through scheduling or standard local procedures.

8. Draft CASA Advisory Circular 101.1(0) Section 5 provides extensive guidance for operating UAVs within controlled airspace. Primarily, it requires UAVs to be operated in accordance with the rules governing the flights of manned aircraft, including compliance with ATC regulations and equipment requirements applicable to the class of

airspace within which they intend to operate. The advisory circular should be consulted if UAV flight within controlled airspace is required.

Safety Supervision

9. An integral requirement for any UAV operation is for an individual to be assigned overall responsibility for UAV safety. This individual is responsible for monitoring and documenting the safety control measures of the planned test or operation, and is empowered to stop operations if control measures are not followed or if safety limits are exceeded. Where a UAV is to be operated by a contractor as a state aircraft (for example, as part of a capability trial), a suitable compromise may be for responsibility to be jointly shared by a contractor member and an ADF member. Concurrence by both members should be required for operations to commence, and either member should be individually empowered to stop operations if an unsafe condition evolves.

GENERAL GUIDANCE

Safe Recovery System

10. The safe recovery systems on a UAV are an essential component of the overall UAV safety system. However, safe recovery systems can introduce other hazards, and these must be taken into account when planning a UAV mission.

11. For UAVs equipped with parachutes, the landing footprint can be substantial if the parachute is deployed at high altitude in high prevailing winds (drift in excess of 10 km may be possible). When planning a mission, the operator must ensure that the UAV will remain within the designated exercise area even under the worst-case parachute deployment scenario. This is particularly important if the exercise area is located near populous areas. Calculations must also account for autonomous UAV manoeuvres prior to the parachute's deployment. For example, some UAVs are pre-programmed to climb and fly autonomously for many seconds upon loss of datalink, in the hope of regaining contact before deploying the parachute. This can add substantially to the worst-case drift scenario.

12. For UAVs that rely on an autonomous recovery system when datalink is lost, landing areas within adequate range must be established for all phases of flight. In addition, safeguards should be implemented to ensure that these safe zones are pre-programmed correctly into the UAV.

Pre-programmed (Autonomous) Mode

13. Some UAVs have the facility for pre-programming part or all of the mission profile, and then allowing it to be executed autonomously. In this mode, the UAV will continue to operate even when the datalink from the UAV to the control station is lost. While this mode has operational advantages (for example, it allows the UAV to venture out of line-of-sight with the ground station antenna), an error in pre-programming could have severe consequences. The operating procedures for the UAV should include the steps that will be taken to mitigate this risk. For information, CASA allows for autonomous flight provided UAV performance and designated ATC communications are continuously monitored by the UAV controllers, and that UAV system and crew are capable of immediately taking active control of the UAV.

Uncontrolled Flight

14. The potential exists, whether through system design shortfalls or through operator error, for the UAV to exit the assigned exercise area. It may even be possible, through multiple hardware or software failures, for control of a UAV to be lost without the emergency recovery mechanism deploying. In each of these situations, immediate action is required to ensure that the UAV does not pose a danger to other aircraft. UAV operating procedures should establish contingency plans for these scenarios, for example notifying any nearby ATC, advising ADF aircraft in the vicinity, diverting aircraft to locate the UAV, tracking progress from the ground, and so on.

Environmental Limitations

15. The design of some UAVs does not permit operation in environmental extremes, for example in dust storms or where there is potential for icing. While the flight manual should adequately address the UAV's environmental limitations, it is unlikely to establish fallback procedures should environmental conditions change while the UAV is airborne. UAV operating procedures should therefore address this issue.

Compensating for 'See and Avoid'

16. The lack of a 'see and avoid' capability raises a significant safety concern for UAV operation in the vicinity of other aircraft, particularly where operation in non-exclusive airspace is planned, or the exclusivity of airspace cannot be guaranteed. Even the fitment of an Airborne Collision Avoidance System (ACAS) does not fully mitigate the risk, since not all aircraft are fitted with this equipment. Possible strategies for UAV collision avoidance include the use of chase aircraft, adding bright colours to the UAV, radar surveillance of the area, the use of ground observers for low flying UAVs, plans to actively avoid conflicts which account for performance limitations of the UAV, and so on.

Unmanned Aerial Targets

17. Unmanned Aerial Targets (UATs) are a class of UAV that may require more extensive safety considerations, since their mission profile may include closer proximity to aircraft, facilities or personnel. In addition, evasive manoeuvres, tow lines, chaff, flares and damage from weapons, raise a number of additional safety concerns. ABR 5291 provides specific guidance for the Kalkara UAT, and may be used as a basis for SOPs for other UATs.

SECTION 2

CHAPTER 16

CRASH PROTECTION

INTRODUCTION

1. Aircraft that comply with contemporary Crash Protection requirements reduce the likelihood of crew and passengers suffering serious injuries in the event of a survivable crash. The ADF's draft policy on crash protection for ADF aircraft assigns the TAA with responsibility, inter-alia, for the following functions:

a. Defining and documenting the ADF's preferred crash protection standards for new aircraft acquisitions.

b. Informing SPOs of industry developments in crash protection that may affect in-service aircraft and

c. Assisting SPOs with the conduct of crash protection assessments for in service aircraft.

This chapter addresses the three policy requirements by presenting the ADF's preferred design standards for aircraft crash protection. These design standards present a baseline level of safety against which new and in-service ADF aircraft may be assessed.

2. As of March 2007 the ADF's crash protection policy has yet to be formally promulgated, although an advanced draft version now incorporates input from key stakeholders. The reader of this chapter must therefore be cognisant that the ADF's approach to managing aircraft crash protection is still evolving and that the guidance in this chapter may be superseded. SCI-DGTA assistance should be sought prior to applying the guidance in this chapter.

Aircraft crash protection design principles.

3. A successful crash protection strategy is one that protects occupants from serious injury in potentially survivable crashes while limiting capability reductions, implementation costs and additional maintenance overheads to acceptable levels. To optimise occupant protection, a systems approach to crash protection is necessary, encompassing the following five key crash protection principles:

a. **Aircraft crash resistance**. The ability of the aircraft structure to provide a protective shell for occupants in the event of a survivable crash is a key factor for occupant survival. The structure and equipment should be designed to allow deformation in a controlled, predictable manner so that forces imposed upon the occupants will be tolerable while still maintaining a protective shell. This aspect also relates to the restraint of mass items, to prevent parts of the aircraft becoming projectiles within the cabin during a crash (eg. engines/transmission/blades coming through the roof, internally mounted items dislodging, etc).

b. **Occupant retention**. Protection should be afforded to occupants by the aircraft's retention system, which comprises the seat and restraint system assembly. The retention system plays a major role in preventing occupant contact injuries associated with body parts flailing into aircraft structures.

c. **Cargo and equipment retention.** Restraint systems should be designed to control cargo and ancillary equipment displacements that are hazardous to occupants during a survivable crash.

d. **Post-crash emergency escape provisions.** Occupants should maintain the ability to rapidly evacuate the aircraft during non-crash ground emergencies, and after survivable crash conditions. The ability to escape is impacted by aircraft deformation, lighting, escape hatches, etc.

e. **Post-crash injury prevention.** The crash protection system should be designed to prevent post-crash environmental hazards that could seriously injure occupants. For hazards which cannot be prevented, the crash protection system should protect occupants from exposure to the hazards. Potential post-crash environmental hazards include fire, toxic fumes and submersion.

The following section assesses the extent to which common civilian and military crash protection standards address these five design principles. The subsequent sections provide guidance on how common crash protection standards should be applied to new aircraft acquisitions, and how they can be employed to assess the adequacy of in-service aircraft crash protection measures.

CRASH PROTECTION STANDARDS

4. The draft ADF crash protection policy makes numerous references to the concept of contemporary crash protection design standards. This section presents an assessment of whether common civilian and military crash protection standards may be considered 'contemporary'.

Civilian crash protection standards

5. The most common civilian crash protection standards are those adopted by the US Federal Aviation Administration (FAA). The FAA's Federal Aviation Regulations (FARs) parts 23 through 29 present airworthiness design requirements for fixed and rotary wing aircraft. While there are no regulations explicitly labelled 'crash protection', nevertheless numerous regulations cover the elements of crash protection such as seat crashworthiness, fire protection, emergency provisions and cargo retention. In addition, several Advisory Circulars (ACs) have been introduced by the FAA to document a means (but not the only means) of showing compliance with these key crash protection regulations. Annex A presents a summary of the key regulations and associated advisory material.

6. The level of safety inherent in the FAR crash protection requirements is widely accepted around the world, both by other airworthiness authorities and the travelling public. This is largely due to these FAR requirements being subject to ongoing review as a result of FAA research, industry working groups, pressure from special interest groups, and the post-crash analyses of the National Transport Safety Board. The current FARs are therefore assessed as presenting a set of contemporary crash protection standards, and present a convenient safety benchmark where the ADF is employing an aircraft in a civilian-like configuration, role and operating environment (CRE).

US Military crash protection standards

7. The US Joint Services Specification Guide, C*rew Systems Crash Protection Handbook* issued in 1998, presents guidance for the development of requirements and verification effort for crash protection, as well as the crash protective aspects of seating, restraint, and crew and passenger station design. While this handbook refers to various military and civilian standards, it primarily leverages off MIL-STD-1290A, *Light Fixed and Rotary-Wing Aircraft Crash Resistance*. This MIL-STD appears to be the prevalent crash protection standard for US military platforms and, despite the title, is also used for designing crash protection measures for large aircraft. However, it has not been updated since 1988, so its coverage of contemporary crash protection issues cannot be assured. The US Army has also published an *Aircraft Crash Survival Design Guide*, which provides further guidance on crash protection techniques. Annex A presents further information on the coverage of these standards and handbooks.

8. It is evident from the previous paragraph that the US DoD does not have a single up-to-date standard for crash protection. On the other hand, the US DoD handbooks and standards present an excellent holistic approach to crash protection, and in this aspect are superior to the civilian standards. Furthermore, these military documents recognise the likely differences in crash scenarios between military and civilian aircraft, and specifically cater for the military environment. While the US DoD handbooks and standards for crash protection may not be considered 'contemporary' standards because many years have elapsed since their last updates, neither should they be disregarded. Rather, they should be used as a guide, but supplemented by the FAA standards to ensure that modern advances in crash protection are addressed.

Other military and civilian standards

9. SCI-DGTA research into crash protection standards is ongoing. The next issue of this chapter will be expanded to include other military and civilian crash protection standards, if the standards are in widespread use. In particular, the European Aviation Safety Agency (EASA) approach to crash protection will be assessed in detail, since several recent ADF aircraft have been procured from Europe. The approach adopted by other military Airworthiness Authorities, for example the UK MoD, will also be assessed.

CRASH PROTECTION REQUIREMENTS FOR NEW AIRCRAFT

Civilian derivative aircraft

10. The ADF, like most militaries, recognises the advantages of acquiring existing civilian aircraft designs that largely meet our needs, and then adapting them to fulfil particular operational requirements. Furthermore, several recent military-specific aircraft (Tiger, MRH-90, 382J) have been designed primarily to civilian design standards. Civilian crash protection standards are therefore becoming commonplace for ADF aircraft.

11. Provided the ADF intends to employ an aircraft in a civilian-like CRE (eg the ADF's VIP aircraft), then contemporary civilian crash protection design standards provide an appropriate level of safety for the ADF. However, where the ADF intends employing a civilian aircraft design outside a civilian-like CRE, the FARs cannot automatically be assumed to present an appropriate level of crash protection. For all new acquisitions, an assessment of the differences between the intended ADF CRE and the civilian CRE (that is, the CRE assumed by an NAA when they issue a Type Certificate for the aircraft type) should be conducted. If the CRE differences potentially reduce the inherent level of crash protection for occupants, the FARs may need to be supplemented. Military standards are one way of supplementing the FARs.

12. The previous paragraph stated that contemporary civilian standards present an appropriate level of safety if the ADF is operating an aircraft in a civilian-like role. However, ADF project offices should not assume that new production aircraft will meet contemporary civilian standards. With very few exceptions, new production civilian aircraft will have been Type Certificated several years ago. Furthermore, until the recent introduction of FAR 21.101, liberal civilian 'grandfathering' principles permitted superseded standards (in some cases, from many decades ago) to continue to be applied to new variants of old aircraft designs. So, despite the ADF acquiring a new production aircraft, it may still fail to meet the ADF's policy requirement to meet 'contemporary' crash protection standards. This is less likely to be an issue for recent aircraft designs that have been issued a new Type Certificate (rather than an amendment to an existing Type Certificate). However, where a tendered aircraft is based on an older design, an assessment of the differences between the aircraft's crash protection design standards and contemporary standards will be required during the Tender Evaluation process. Where modifications to overcome crash protection shortfalls are possible, the costs should be factored into the Tender Evaluation and subsequently included in the project scope. Where modifications are impractical, a case must be presented for approval by the TAA and OAA (and perhaps the ADF AA, if the issues are sufficiently serious) prior to completion of the Tender Evaluation. An Issue paper is a suitable means for documenting crash protection analyses.

Military aircraft

13. The ADF occasionally procures aircraft that have been designed to military crash protection standards. As previously noted in this chapter, military standards do not necessarily reflect contemporary advances in crash protection measures. Furthermore, the military standards may not fully encompass ADF-unique aspects of CRE. The acquisition process should therefore include an assessment of the crash protection measures designed into the proposed aircraft. Key issues are as follows:

a. it may not be practicable (or even possible) to improve some key aspects of crash protection, such as impact protection, so the ADF must decide whether those shortfalls will be acceptable throughout the entire service life of the aircraft; and

b. some crash protection improvements may be retrofitted to an aircraft; these modifications should be identified early in the acquisition process and completed as part of the acquisition project.

The civilian and military crash protection standards discussed in this chapter provide a basis for assessing these two issues. The information in the next major section (Crash Protection Assessments for In-Service Aircraft) is also useful, since it presents guidance on how to assess the adequacy of crash protection measures on existing aircraft. Where modifications to overcome crash protection shortfalls are possible, they should be factored into the project scope. Where modifications are impractical, a case must be presented for approval by the TAA and OAA (and perhaps the ADF AA, if the issues are sufficiently serious) prior to acquisition. An Issue paper is a suitable means for documenting all crash protection analyses.

Aeronautical life support equipment

14. Aeronautical Life Support Equipment (ALSE) is fundamental to the fifth element of crash protection, namely post-crash injury prevention. Some ALSE elements (eg life rafts) are included in an aircraft's certification basis, and

therefore will inherently be encompassed within aircraft design standards such as the FARs. However, personal ALSE (for example personal locator beacons, immersion suits, etc) are not normally included in an aircraft's certification basis. Project offices must therefore ensure that personal ALSE is not omitted from any assessments of aircraft crash protection.

15. Aircraft acquisition project offices should liaise closely with the ALSE Airworthiness Standards Representative (ASR), who is able to provide authoritative standards advice on ALSE matters. In particular, the ALSE ASR will be able to assess the compatibility of ALSE (whether existing in-service items, or proposed new items) with the ADF's proposed CRE for the new aircraft. Section 2 Chapter 20 of this manual presents the ADF's preferred standards for ALSE.

CRASH PROTECTION ASSESSMENTS FOR IN-SERVICE AIRCRAFT

16. The draft ADF crash protection policy directs that ADF aircraft are to remain compliant with the crashworthiness design requirements against which the aircraft type was certified. However it also directs that, as far as is "reasonably practicable", in-service aircraft are to comply with contemporary crashworthiness design requirements. This section presents guidance on how this latter policy requirement might be implemented.

17. Fundamental to assessing whether the crash protection afforded by an in-service aircraft is appropriate, is a comprehensive understanding of:

a. the as-designed survivable crash envelope for the aircraft;

b. the crash protection features inherent in the aircraft;

c. previous crash performance of the aircraft type (if available); and

d. the aircraft CRE, so that crash protection measures are targeted at likely crash scenarios.

Equipped with this knowledge, an assessment of an in-service aircraft against contemporary crash protection standards may be conducted. In this case, 'contemporary' refers primarily to civilian crash protection standards (since these are most likely to be regularly updated), supplemented with military standards where the ADF's CRE ventures outside that of a normal civilian CRE.

18. As stated earlier in this chapter, a successful crash protection strategy is one that protects occupants from serious injury in potentially survivable crashes while limiting capability reductions, implementation costs and additional maintenance overheads to acceptable levels. Making an assessment of whether to reject a potential crash protection improvement on the basis of its capability, cost or maintenance impact, can be a difficult decision. The draft ADF crash protection policy provides guidance on how to assess whether compliance with contemporary standards is 'reasonably practicable'. As required by the draft policy, all decisions not to incorporate contemporary crash protection measures must be justified and documented. An Issue Paper is an appropriate medium for documenting the assessment, and for obtaining TAA and OAA concurrence.

Annex:

A. Crash Protection Standards

CRASH PROTECTION STANDARDS

1. This annex presents an assessment of the key elements of common civilian and military crash protection standards. In each case, the five crash protection principles defined in Section 2 Chapter 22 are used as a framework for the assessment.

CIVILIAN CRASH PROTECTION STANDARDS

Fixed Wing Aircraft

2. Aircraft Crash Resistance. Subpart C of FARs 23 through 29 cover structural and strength requirements for fixed and rotary wing aircraft. Although these requirements are not specifically labelled as "crash protection" requirements, they present the airworthiness design requirements for the platform's structural integrity and thus inherently address the structural crashworthiness requirements for aircraft to which these FARs apply. Relevant ADF aircraft that are certified to or will be certified to recent amendments of one of FARs 23 through 29 should explicitly address crash protection through the satisfaction of these requirements. For platforms not certified to these FARs but fit within its scope, the requirements in Subpart C should be used as a basis for satisfying the aircraft crash resistance criteria of this chapter.

3. Occupant Retention. A number of applicable advisory circulars have been released by the FAA as a means to satisfy the relevant FAR occupant retention clauses, as follows:

a. **AC 23.562** – Dynamic testing of Part 23 aircraft seat/restraint systems and occupant protection. Covers the method to satisfy the FARs applicable to the dynamic testing of aircraft seats and occupant protection (e.g. 23.562, 23.785, and 23.787).

b. **AC 25.562-1a/b -** Dynamic testing of Part 25 aircraft seat/restraint systems and occupant protection. Covers the method to satisfy the FARs applicable to the dynamic testing of aircraft seats and occupant protection (e.g. 25.562, 25.785, 25.787, and 25.789).

c. **AC 25-17** – Transport Airplane Cabin Interiors. This is a general AC covering the applicable cabin interior crashworthiness requirements of FAR 25. This AC does not include crashworthiness aspects such as fuel tank/system design, fuselage deformation and prevention of post-crash fires, but does incorporate guidance in seat/restraint system design. Appendix C of this AC provides a list of applicable FAA cabin interior crashworthiness advisory circulars.

4. Cargo and equipment retention. AC-25-17 includes specific coverage of design requirements for stowage compartments, compartment interiors, cargo and baggage compartments and miscellaneous equipment.

5. Post-crash emergency escape provisions. AC 25-17 includes crashworthiness considerations for doors and hatches, emergency evacuation (including lighting requirements and access to exits) and ditching equipment. It specifically highlights the sections in FAR 25 that are applicable in ensuring that this crash protection principle is addressed.

6. Post-crash injury prevention. This crash protection design principle encompasses a number of aspects in crashworthiness design considerations. Subpart E of FAR 23-29 cover powerplant airworthiness requirements including fuel system design requirements. The following ACs are also relevant to post crash injury prevention.

a. **AC 20-135.** This AC provides guidance in compliance to the powerplant fire protection requirements of FARs 23 through 29.

b. **AC 25-9.** This AC covers fire protection requirements (smoke detection, penetration and evacuation tests and emergency procedures).

c. **AC 25-16.** This AC covers electrical fault and fire prevention and protection.

d. **AC 25-17.** As described previously, this AC covers the design elements for cabin interior crashworthiness. It includes guidance in meeting requirements associated with fire extinguishing, safety equipment and oxygen equipment.

Rotary Wing Aircraft

7. AC 27-1 and 29-2 – Certification of normal and transport category rotorcraft. These ACs provide comprehensive guidance to compliance with certification requirements in FARs 27 and 29 respectively. This inherently includes consideration for all the crash protection principles covered in this chapter. For instance, AC 27-1 contains subsections providing guidance to seat/restraint system dynamic impact testing, fire protection, structural strength requirements, etc. Previous ACs relating to individual clauses of FARs 27 and 29 have been superseded by these ACs.

MILITARY CRASH PROTECTION STANDARDS

8. Aircraft Crash Resistance. Section 5.1 MIL-STD-1290A provides extensive guidance in addressing this design criteria. MIL-A-8865B also contains the strength and rigidity requirements for miscellaneous loads applicable to aircraft, including strength requirements in relation to crash loads.

9. Occupant Retention. Military specifications covering the aircraft seats are dated (eg. MIL-S-25073 was published in 1970) but are still referred to by manufacturers of some aircraft seats (eg. Simula seats). MIL-STD-1290A Section 5.2 covers occupant retention design requirements. Additionally, the US Army Crash Survival Design Guide and the US DoD Crew Systems Crash Protection handbook provide further guidance in satisfying these requirements.

10. Cargo and equipment retention. Section 5.3 of MIL-STD-1290A covers requirements for cargo and equipment retention. Additionally, the US Army Crash Survival Design Guide and the US DoD Crew Systems Crash Protection handbook provide further guidance in satisfying these requirements.

11. Post-crash emergency escape provisions. Section 5.4 of MIL-STD-1290A covers requirements for emergency escape provisions in the event of a crash. Additionally, the US Army Crash Survival Design Guide and the US DoD provide further guidance in satisfying these requirements.

12. Post-crash injury prevention. Section 5.5 of MIL-STD-1290 covers requirements for post crash fire protection. Additionally, the US Army Crash Survival Design Guide and the US DoD Crew Systems Crash Protection handbook provide further guidance in satisfying these requirements. Additional standards quoted in section 3.7.3.4 of the US DoD Crew Systems Crash Protection handbook are also applicable.

SECTION 2

CHAPTER 17

IN-SERVICE MANAGEMENT OF SOFTWARE FOR AIRBORNE AND RELATED SYSTEMS

INTRODUCTION

1. The in-service maintenance and development of safety-related software for airborne and related systems, if conducted without sufficient rigour, has the potential to impact the integrity of those functions implemented by the software, and therefore the safety of the aircraft. Furthermore, the recording, tracking and resolution of problems associated with safety-related systems is critical to ensuring these systems achieve the required level of safety. Only through appropriate in-service management will software achieve and maintain its intended level of safety.

2. This chapter identifies a number of 'key issues' which DGTA considers fundamental to the in-service management for ADF safety-related aerospace software. While their adoption is not mandatory, justification for their omission would normally be expected.

SCOPE AND APPLICABILITY

3. This chapter addresses the in-service management of safety-related software for airborne and related systems. It focuses on software support agency requirements, in-service problem and change management, design review and approval guidance for in-service development, and contingency build requirements. It is not the intent of this chapter to prescribe a process to which all Software Support Agencies must comply, although the chapter does provide an example process (refer Annex A) to provide some basis for comparison of new support agencies with previous practice. Software should generally transition to an in-service support arrangement with the extant standards that applied during the acquisition phase; for this reason, development assurance and safety standards are not addressed in this chapter. Rather, this chapter restricts discussion to organisational requirements and Commonwealth interfaces to software processes. For guidance on requirements for transition to in-service, software assurance, software safety, and software development and lifecycle standards, refer to Section 2 Chapter 7.

4. While this chapter specifically focuses on safety-related software, the principles are equally applicable to mission software. Section 2 Chapter 7 presents guidance on missionised hazards, which provides a mechanism for assessing the importance of mission software.

SOFTWARE SUPPORT AGENCY OR REPRESENTATIVE

Software Support Agency

Key Issue: In-service maintenance and development of software should be conducted by a Software Support Agency (SSA) that is an Authorised Engineering Organisation (AEO), and for which the scope and authority of software development is defined in an approved Engineering Management Plan (EMP).

5. The scope of authority of each SSA is likely to vary considerably across the ADF, depending on whether the in-service support is provided by the OEM, an OEM sub-contractor, the Commonwealth, or a non-associative third party contractor. Where the SSA belongs to the OEM or is an OEM sub-contractor, then there may be provision to waive the requirement for them to explicitly be an AEO. However the OEM's scope and authority of software development should still be defined within the relevant SPOs engineering system, and the SPO should still provide oversight of the OEM's software practices to the extent necessary to conduct design acceptance of software changes produced by the OEM.

6. An SSA's scope of responsibilities may typically include the following:

a. in-service management of problem reports and point of contact for problem resolution;

b. development of plans and requirements for software maintenance and development;

c. configuration management and control of software products;

d. development and implementation of software changes;

e. test and evaluation of software products; and

f. design review and approval of software changes.

7. To become an AEO, the SSA must demonstrate that it meets AAP 7001.053's Organisation, People, Process and Data (OPPD) requirements. The following paragraphs outline specific OPPD considerations for the SSA.

8. **Organisation**. The SSA should satisfy the normal AEO criteria for any organisation performing aircraft engineering for the Commonwealth including having a quality system (ISO 9001), SDE (responsible to the TAR for the engineering), Engineering Management System (documented in an EMP), Design Support Network (DSN), etc. For SSAs, the DSN should, where possible, include the software OEM, operating system OEM, hardware OEM, tool vendor technical support, and equipment suppliers for development and integration environments. SSAs may also find it advantageous to build relationships with specialist expert software analysis and verification organisations to assist with complex software designs and technologies.

9. **Personnel**. The SSA should employ a sufficient number of suitably qualified, trained and experienced software personnel to ensure that all activities are conducted by competent, authorised staff. A paper detailing competency requirements for software personnel can be found on the DGTA intranet website under DAIRENG/SCI1. The typical software roles within an SSA include:

a. Software Team Lead – responsible for general oversight and management of software development activities, and for developing the competencies of software development staff.

b. Software Architects (Designers) – responsible for assessing the impact of new requirements on the existing software architecture, and translating new high level requirements into changes to the software architecture.

c. Software Programmers – responsible for translating high and low level requirements (and the software architecture) into source code, including any necessary analysis in support of coding.

d. Software Testers – responsible for testing and analysis of software at unit and integration levels.

e. Software Quality Manager – responsible for Software QA activities

f. Software Configuration Manager – responsible for Software CM activities.

g. Technical Support Staff – responsible for configuring and maintaining the software development and test environments, including a software test bench and systems integration laboratory.

10. While it is possible for an individual person within an SSA to share a number of these roles, it should generally be discouraged. Careful management is required to ensure that independence requirements are not violated on reviews and test activities, and the distinct attributes of each role are preserved. Furthermore, for most systems of any reasonable size, a minimum critical mass of personnel is required to maintain sufficient knowledge of the software (requirements, design and verification).

11. **Process**. The SSA should clearly document the engineering development activities for software products as part of their procedures and quality system. It is expected that the procedures will follow the guidance outlined in Section 2 Chapter 7 of this manual and address the elements as illustrated in Figure 17–1. The process should address how the safety criticality for a software element or sub-element relates to the engineering rigour applied during development. Every effort should be made to ensure that the development process caters for the differing levels of criticality (e.g. Software Hazard Risk Index 1 through 5, or Design Assurance Levels A through E), and product types (e.g. Electronic Warfare Systems, Mission Computers) undertaken by the SSA. If the SSA only defines a single development process, it should be commensurate with the worst case criticality (i.e. function requiring the highest integrity) of the software products that the SSA is responsible for supporting. Section 2, Chapter 7 of this manual provides further details on the Software Assurance requirements for ADF airborne software.

12. **Data**. The SSA requires access to appropriate software design data including requirements specifications, design descriptions, source code, verification documentation, etc. SSAs that don't have sufficient access and understanding of original software design data are at risk of violating critical software design assumptions during subsequent in-service changes. This may result in software that lacks the required level of integrity, potentially leading to operating limitations or (if undetected) a latent reduction in the level of safety.

13. Figure 17-1 presents the key process elements of a SSA. Several of the elements are discussed in this chapter, while the remainder are addressed in Section 2 Chapter 7.

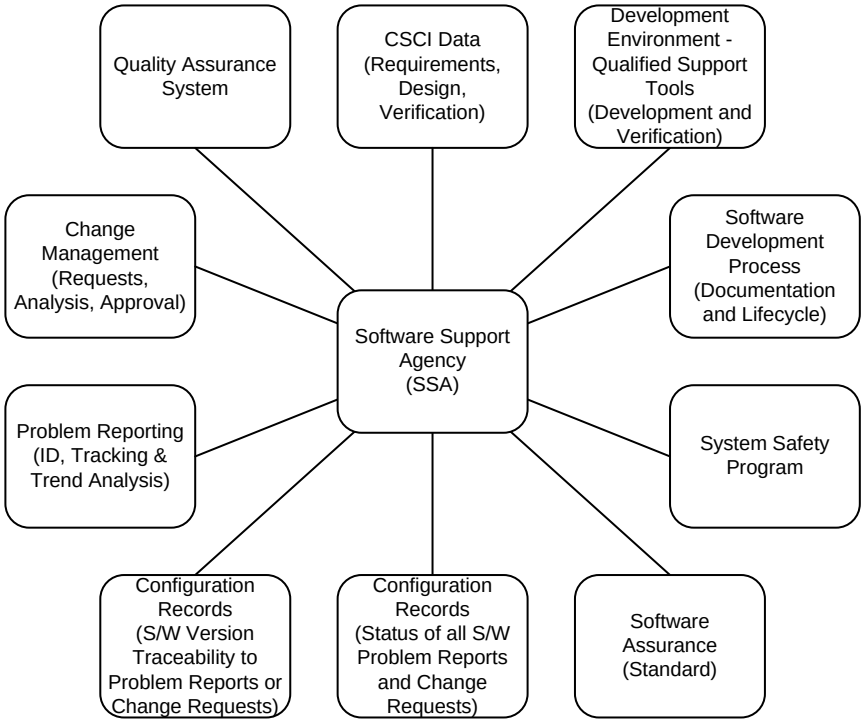


Figure 17–1 Key Process Elements of Software Support Agency

SOFTWARE PROBLEM AND CHANGE MANAGEMENT

Software Problem Reporting and Change Control

Key Issue: The SSA should ensure that all software problems are recorded, tracked, and reviewed by appropriate operational and technical personnel to ensure software problems with safety implications can be assessed and addressed within an appropriate timeframe.

Key Issue: The SSA should ensure that proposed capability enhancements to software are recorded, tracked, and reviewed by appropriate operational and technical personnel to ensure that only approved changes are incorporated into software builds.

14. While the application of best practice software development processes, a software assurance standard, and the formulation and integration of a software safety program with the system program should help to minimise the number of serious defects in safety-critical or safety-related software, most approaches do not guarantee the absence of errors. It is important that the SSA has a mechanism for detecting and assessing all types of software problems, including those experienced in-service, and during maintenance or development activities. Furthermore, the SSA requires an appropriate mechanism to permit operators to input minor change requests or enhancements to address capability deficiencies or improve the operational interface. SSAs should:

a. establish a system for problem reporting and for documenting proposed changes or enhancements;

b. maintain configuration control of all software problem reports or change requests;

c. ensure that enough information is captured to permit analysis of the problem or proposed change; and

d. ensure that every occurrence of a problem is documented, regardless of whether operators or maintenance staff believe that it is a recurrence of a previously documented problem.

15. For more subtle software defects, a significant amount of information (number of occurrences, initial conditions, contributing factors, etc) may be required to determine the specific problem. Problem reporting also assists

with determining the actual system performance and can provide the basis for assessing requirements for major changes such as system replacement or major upgrades.

16. The problem reporting system established by the SSA is not intended to be used to replace current aircraft documentation and should not be used to sign off an unserviceability. Symptoms must be recorded in the EE500/EE435, as with any fault, and normal defect action initiated where appropriate. The problem reporting system should therefore operate in parallel with the existing defect system.

Approval Authority for Software Changes and Release

Key Issue: The weapon system Configuration Control Board (CCB) should be the approval authority for commencement of all minor type design in-service software changes, the approval authority for aircraft ground and flight testing, and the approval authority for fleet release.

17. For most minor type design changes the CCB, supported competent software SPO personnel, provides sufficient oversight of the software change. However, some DARs have found it useful to elevate software modifications to a major type design change, where based on technical difficulty alone the change might normally be considered to be a minor type design change. Such an approach has been used when the SPO has limited experience with software acceptance, and can benefit from the greater level of oversight provided by various ADF stakeholders for major type design changes. DGTA advice should be sought before classifying design changes on this basis.

Problem Investigation and Review

Key Issue: A subordinate CCB (eg. Software CCB) or Software Working Group (SwWG) should be established by the CCB to review and prioritise all software problems and change requests.

18. A SwCCB or SwWG is required to filter individual problems and enhancements to ensure adequate engineering investigation and user consideration occurs before a method of resolution is determined. The SwCCB or SwWG should determine a relative priority for each software problem or change request. IEEE Std 1044-1993 ‘IEEE Standard Classification for Software Anomalies’ and MIL-STD-498 Appendix C Figure 5 provides guidance on classifying priorities for software problems. The SwCCB/SwWG should provide the CCB with a report outlining the status of all software problems annually, or more frequently as specified by the CCB.

19. In some cases, investigation might reveal that certain problem reports might relate to system wide problems (e.g. the software problem is a symptom of a wider system or hardware issue), and therefore the SwCCB or SwWG should ensure that the results of the investigation, and any identified trends are communicated to the SPO for further investigation.

20. A typical SwCCB or SwWG would include the following:

a. Operator representatives. Aircrew or Aircrew Liaison Officers.

b. Acquirer representatives. SPO Software DSDE and/or Software Manager.

c. Developer/Maintainer representative. Software Project Manager, and key personnel in the software development team.

21. A SwCCB or SwWG’s typical scope of responsibilities includes the following:

a. endorse software problem reports / change requests which are valid problems and cancel those that actually describe the system as it is specified or those which do not appear to provide tangible benefits,

b. assign a priority for resolution of the software problem reports / change requests,

c. ensure that all submitted software problem reports / change requests undergo appropriate analysis by the SSA,

d. ensure that all relevant agency/project interfaces have been considered,

e. ensure that appropriate action for each software problem report / change request is determined, and

f. endorse the relevant plans submitted by the SSA for each version change.

22. The SSA should propose the schedule and content of future software updates through the SwCCB or SwWG to the CCB, based on the direction received. The SSA may also propose that a number of problem reports or change requests be grouped together for implementation in a future software version/build. Allocation should be performed with consideration of the priority, effect of the change, interoperability requirements, hardware resource limitations, hardware compatibility and schedule for the version development. The CCB should ensure that the proposed plan is appropriate in terms of technical and procedural content, resources, schedule and other logistics or operational factors.

23. Where the DAR wishes to provide more rigorous oversight of the SSA's problem reporting and change management activities, then the DAR (or representative) should also take an active role in a Software CCB (SwCCB) or Software Working Group (SwWG). For more information regarding Commonwealth oversight of software modifications, see Annex C to Section 2, Chapter 7 of this manual

Software Lifecycle, Development and Assurance Standards

24. Section 2 Chapter 7 provides details on the application and tailoring of standards relevant to the software lifecycle, software development and software assurance. Annex A to this chapter illustrates an example change management approach for in-service software support activities, which is based on the Software Development Standard MIL-STD-498. It is not intended that all SSAs conduct in-service software support in accordance with the process detailed at Annex A, however it does provide a reference framework for SSAs to use in establishing their own processes.

DESIGN REVIEW AND APPROVAL OF IN-SERVICE SOFTWARE DEVELOPMENT

25. Regulation 3 of AAP 7001.053 describes the requirements for design review and approval. However, the development approach employed for software does not fully lend itself to the AAP7001.053 approach, where Design Reviews and Approval activities are conducted at the conclusion of the development project. This section provides some clarification to the role and purpose of Design Review and Approval for software. Readers may find it useful to refer to the diagram at Annex A when reading this guidance.

26. The development of an appropriate software design requires continued analysis and consideration of development products by the reviewers and approvers throughout the development process to ensure evolving issues are appropriately resolved. The first phases of design review for software typically commence during the requirements phase of the software lifecycle, and continue for each major phase of the software lifecycle. While this concept may be appear to violate AAP 7001.053's requirements for design review independence, and thus places challenges on the design reviewer or approver in terms of maintaining their independence from design development, it is necessary to ensure that each phase of software development has been performed with sufficient rigour and is assessed to provide a valid starting point for the next phase of the software lifecycle. Note that some SSA's commence design development or coding before the requirements are finalised and reviewed. This approach should be discouraged, as it often leads to the introduction of design defects that require patching late in the development lifecycle.

27. Initial design review should typically be conducted by an authorised DE from the initial specification of requirements through to completion of the software design and coding, prior to the commencement of formal developer unit or integration testing. Formal design review, in terms of recording an assessment in Emerald or on the relevant engineering form, should typically be completed by a DE, based on the completion of developer unit testing, and the finalisation of the software test plan and software test description for integration and on-aircraft testing phases.

28. Initial design approval should typically be completed by a DE or SDE based on the completion of the software integration testing, and prior to the commencement of on-aircraft testing phases. This approval milestone is required to support a CCB decision to approve on-aircraft ground or flight testing. Formal design approval, in terms of recording a final assessment in Emerald or on the relevant engineering form, should be completed by a DE or SDE, based on completion of all test activities, and the finalisation of all software documentation supporting the build. The Functional and Physical Configuration Audits will confirm that the software documentation is accurate and complete. The design approval by the SDE is based on the contents of the approved software design package. If the resulting products have deviated from the initial specification in a way that impinges on operating characteristics of the systems, the SDE may consider referral of issues to the CCB to determine if release is appropriate.

OTHER ISSUES FOR CONSIDERATION

Contingency Builds

29. Under certain operational circumstances, there may be a requirement to perform a contingency software build to provide a rapid capability enhancement or address a capability inhibitor. The objective of contingency builds is to

complete, within a reduced time-frame, a product that satisfies a minimum level of technical quality, without unacceptably compromising the safety or capability integrity objectives of the system. SSAs should define a contingency (or 'cut-down') process in preparation for such a requirement. The contingency process should be related back to the normal software development process. Exclusion of certain elements within the normal process should be justified, and a remediation phase should be established after the release of the contingency build to complete any outstanding tasks that would normally be required under the normal build process. Note that contingency processes are generally only applicable to mission systems (e.g. electronic warfare systems), and are not normally applied to safety of flight critical systems (e.g. automatic flight control systems). Some systems host safety-related functions, mission functions or a combination thereof (e.g. mission computer). For such systems, the SSA should carefully consider the failure condition severity and the software architecture, specifically the amount of partitioning between safety and/or mission functions, to determine whether a cut-down process is appropriate.

Annex:

A. Example Software Support Approach

EXAMPLE SOFTWARE SUPPORT APPROACH

1. This annex describes the typical artefacts (documents and products) used during in-service software support. The artefacts are based on MIL-STD-498 and are presented in the context of a typical approach to the in-service software development life cycle (see Figure 17A-1). It is not the intention of this annex to require that all SSAs conduct in-service software support in this manner, however it does provide a reference framework for SSAs to use in assessing their own approaches. SSAs are encouraged to make use of incremental and evolutionary development techniques where appropriate and to conform with recognised software lifecycle and development standards as described in Section 2 Chapter 7.

Documents – Planning and Software

2. The remainder of this annex outlines the purpose and context of the documents detailed in Figure 17-1, as well defining the concept of a software product and approved design package. The major influence in determining documentation requirements should be the existing document set for support of a software product, and the minimum amount of data required for the SSA to successfully maintain the software throughout its lifecycle. The strict application of the entire MIL-STD-498 document suite is rarely necessary in-service. Efficiencies can often be gained in-service by combining various DID requirements into a single document. The DIDs should simply provide guidance on what information is important to record and provide a common framework for discussing document types. The requirement for specific documentation requires continual review to ensure relevancy to the development and support of software products.

3. The initiating document for in-service support is the **Software Problem & Change Request (SPCR)**. This is the means the SSA uses to document software problems and change requests (sometimes referred to as Software Trouble Reports (STR) or System Trouble Reports). Other documentation can be broadly classified into the following categories: planning and software documentation.

4. **Planning.** The following planning documents are referenced in Figure 17A-1:

a. Preliminary Engineering Change Proposal (PECP). The PECP provides an overall summary of the change and conveys to the SPO an outline of the software and hardware requirements.

b. Systems Engineering Management Plan (SEMP). This optional document may be raised when the hardware component of the change is significant and the whole proposal needs formal planning of the hardware and software development and integration. The impact upon, and the effects of, other projects should be detailed in the SEMP to ensure adequate visibility of interactions between projects.

c. Software Version Plan (SVP). This document is described later in this annex.

d. Software Development Plan (SDP). The SDP (sometimes referred to as the Software Management Plan (SMP)), is the overarching plan that defines the software management processes to be followed by the SSA and the responsibilities, standards, procedures and organisational relationships for all activities associated with producing a software build. Refer to MIL-STD-498 for further information.

5. **Software Documention.** The following MIL-STD-498 software documentation is referenced in Figure 17A-1:

a. Software Requirements Specification (SRS)

b. Software Test Plan (STP)

c. Software Test Description (STD)

d. Software Test Report (STR)

e. Software Development File (SDF)

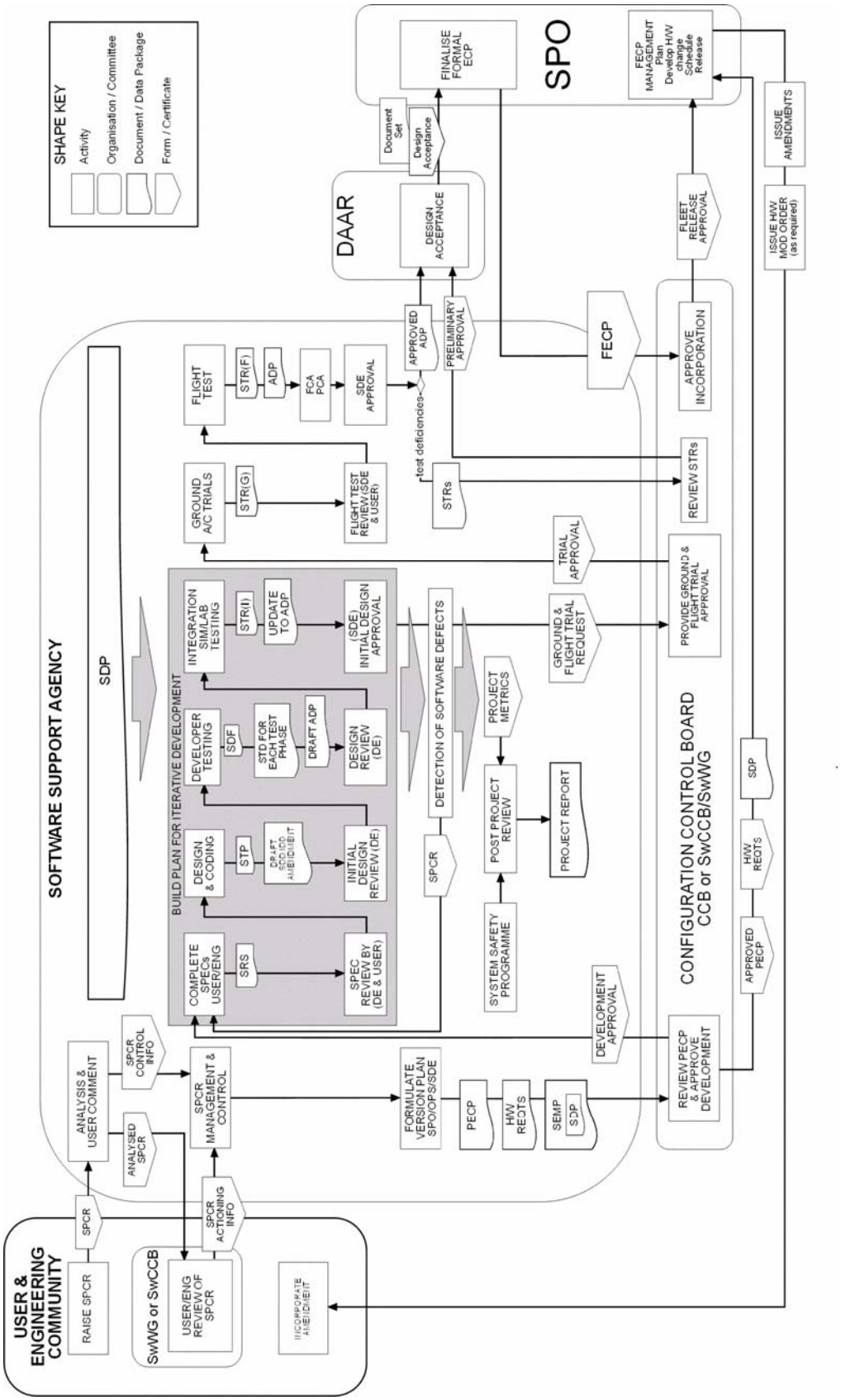


Figure 17A–1 Software Support Process

Software Version Plan (SVP)

6. The SVP acts as a subsidiary plan to the SMP and details the software version development program. The SVP is also sometimes referred to as a Software Build Plan or the Software Design Management Plan. The MIL-STD-498 DID for SDPs may be used as a guide, however, the SVP should only detail specifics of the project and reference procedural information in terms of deviations from an established, documented software development process. The standing instruction or development process documentation should address without further discussion the majority of MIL-STD-498 DID requirements and this should not be repeated in the SVP. Often software development is conducted in conjunction with a hardware change. In these cases the SVP detail should be integrated into an overall systems engineering plan that relates the components of the hardware and software development into a single coordinated plan. The following paragraphs discuss specific components of the SVP as detailed in Figure 17A-2.

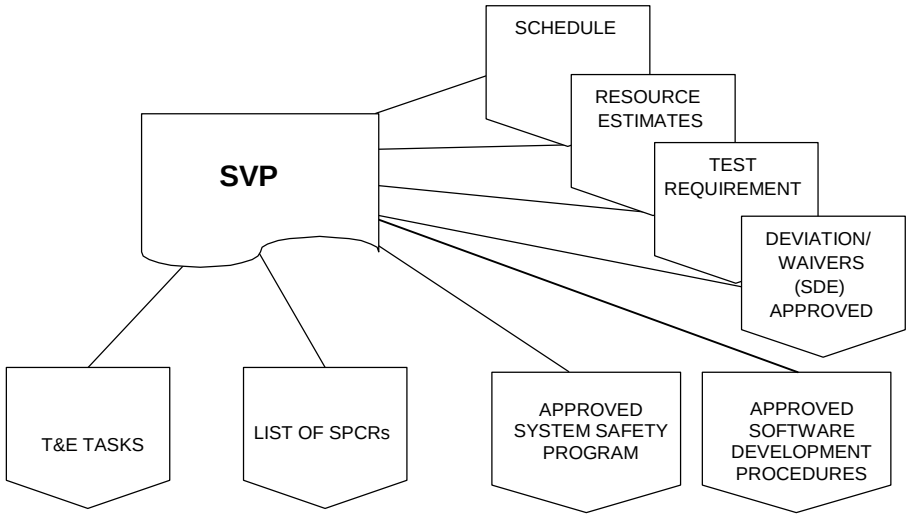


Figure 17A–2 Software Version Plans

a. ***List of SPCRs.*** The content of the software development task should be documented in clear requirement statements on the SPCRs. The approved SPCR should detail all known requirements for the outcome of the change. Thus, in the simplest case, the list of SPCRs in the SVP defines the scope of work required.

b. ***Software Development Procedures.*** The application of a set of standard software development procedures should be clearly defined and established in accordance with a recognised standard and should be based on the requirements of AAP 7001.053(AM1) and Section 2 Chapter 7 of this manual. These procedures are required for approval of the SSA as an AEO.

c. ***System Safety Program.*** The application of a SSP should be clearly defined and established in accordance with a recognised standard and should be based on the requirements of Section 2 Chapter 1 of this manual.

d. ***Resource Estimates.*** Quantitative estimates for the size of the software change should be demonstrated using a code size estimate for each change including staff hours and schedule duration for the project. Schedule milestones such as commencement of testing, user involvement and the timing of key reviews should be specified. Code size and staff hour estimates should be provided for each SPCR included in a software version.

e. ***Test Requirements.*** The duration and resources for testing should be detailed showing how and when specific changes will be tested. Quantitative estimates for ground and flight testing should be provided.

f. ***Deviations and Waivers.*** A software development process should be formally established at all SSAs and is normally documented in an SDP or similar document. The SVP will document the application of the process to a particular project and deviations that will be made from it. For example, sometimes a project may wish to tailor out a non-critical activity, or conversely increase the rigour of a particular critical activity. Approval of the SVP constitutes approval for any deviations from the standard process.

Software Product: Computer Software Configuration Item (CSCI)

7. A software product is more than simply the executable code that provides the required functionality. Figure 17A–3 provides a pictorial view of the complete software product and highlights important aspects of its configuration. Without this additional information which defines the product, supportability of the overall system can be undermined.

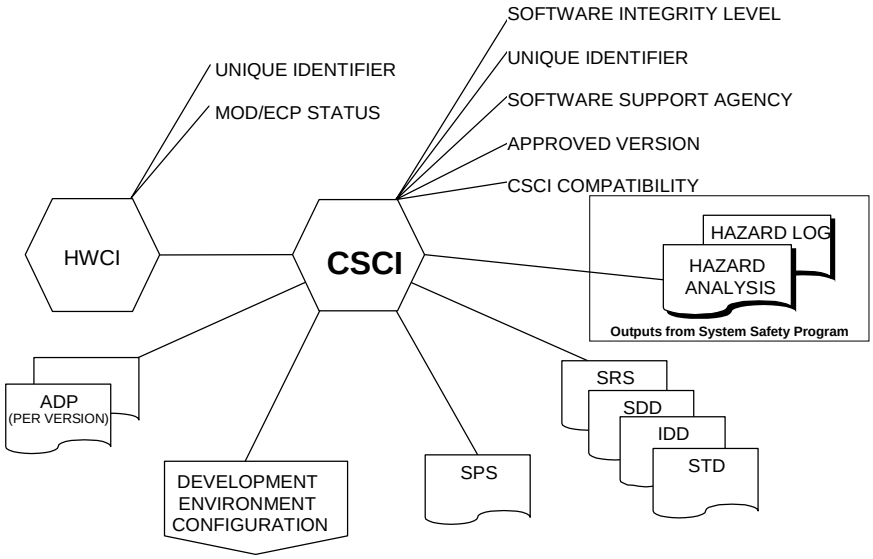


Figure 17A–3 A Software Product

a. ***Hazard Log and Hazard Analysis.*** To ensure ongoing safety of the aircraft and associated systems the SSA must identify the potential hazards and ensure that they are continually assessed and minimised during development. The process of safety management will include additional techniques as required by the development activities. A formalised hazard analysis and resolution process in accordance with recognised safety standards should be applied to all significant software developments. The outputs from the original SSP under which the software product was developed should form the basis of support documentation. The methods applied and work products produced during initial development should be maintained as part of the CSCI configuration and updated as required by new development.

b. ***Software Integrity Level.*** The safety criticality of a software component is based on assessment in accordance with the relevant safety and software assurance standard (eg. MIL-STD-882C, ARP4754/61, RTCA/DO-178B or Def Stan 00-55). The outcome determines the level of assurance required for a software component and thus the development requirements to be imposed in terms of the design and process standards. SSAs are to formally record the safety criticality associated with all supported software products. Safety criticality and integrity level definitions from recognised standards are discussed in Section 2 Chapter 7 of this manual.

c. ***Documentation.*** The set of documentation that constitutes the design of a software product is to be formally managed by the SSA and placed under configuration management. In MIL-STD-498 terms, this refers to the complete set of product related data deliverables, where available.

d. ***Development Environment.*** The SSA is responsible for establishing procedures to ensure the appropriateness of the development environment for its intended purpose. The development environment should be specified and placed under the same configuration control as delivered products of similar criticality.

e. ***Identification and Compatibility.*** The compatibility of each CSCI with its associated Hardware Configuration Item (HWCI) should be formally documented. The SSA should maintain configuration data that relates CSCI version numbers to HWCI identifiers that include MOD/ECP status.

Approved Design Package (ADP)

8. The ADP, as illustrated in Figure 17A–4, may take a variety of forms, and should in most cases be consistent with the development process applied by the initial developer. It would normally include:

a. the CSCI source code;

b. project documentation – planning, requirements, design, test, and reports (eg. SRS, SDD, IDD, SDP, STP, STDs, STRs and SVD);

c. records of all reviews and approvals; and

d. an amendment package that updates the existing documentation for the system and updates the design documents, user manuals and existing test procedures.

The level of design change documentation, testing and engineering review should be commensurate with the safety criticality of the system or change. For software products that undergo a number of changes in their service life, the existing document set should be amended to reflect the software product. This ensures that there is a single documentation baseline describing the software product. Alternatively some SSAs have found it convenient to issue supplements to existing documentation detailing only those aspects of the change. Note that the ADP submitted to the Commonwealth does not always include the complete set of information depicted in Figure 17A-4. This is acceptable, provided the Commonwealth has access to any information not included, but referenced, in the ADP.

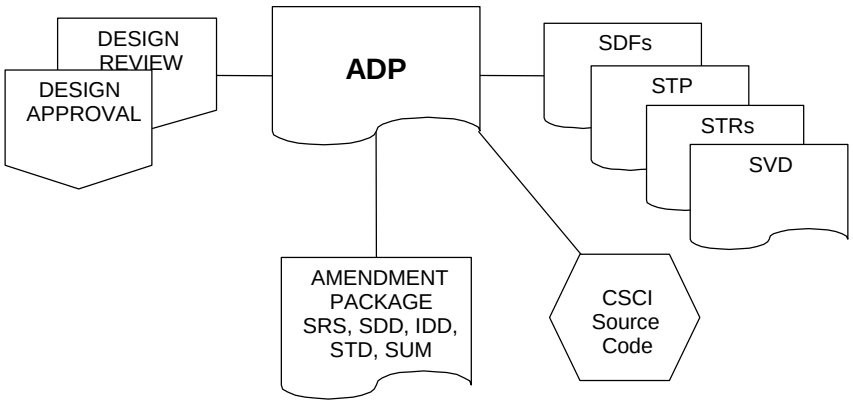


Figure 17A–4 Approved Design Package

Blank Page

SECTION 2

CHAPTER 18

CARRIAGE OF PORTABLE ELECTRONIC DEVICES

INTRODUCTION

1. Portable Electronic Devices (PEDs) have the potential to interfere with electronic equipment on ADF aircraft if not managed appropriately. As products in the consumer marketplace, PEDs are not manufactured or regulated with the intention of allowing operation in the sensitive electromagnetic environment of an aircraft, and therefore are not subject to the same stringent compliance requirements as avionics or other aircraft systems. Although the intentional EM radiation levels from PEDs are comparatively low, and unintentional emissions are even lower, they can still be high enough to interfere with aircraft avionics systems. The risks arising from these issues must be effectively mitigated before PEDs are approved for use in ADF aircraft.

2. Historically, the ADF has grouped PEDs into three categories, namely approved, restricted and prohibited items, with those items in the restricted category requiring CENGR approval prior to carriage. However, with the proliferation of PEDs, in particular laptop computers and personal entertainment equipment, this approach no longer meets the requirements of ADF aircraft passengers. This chapter provides guidance for managing PEDs on ADF aircraft.

PED MANAGEMENT

Commercial Aircraft

3. FAR 91.21 allows unrestricted use of portable voice recorders, hearing aids, electric shavers and heart pacemakers on commercial aircraft. Other PEDs may be used provided the aircraft operator has determined that they will not cause interference with navigation or communication systems. An RTCA study into the carriage of PEDs on transport aircraft (RTCA/DO-233) concluded that:

a. the use of PEDs should be prohibited during critical phases of flight (eg. take-off and landing), and

b. the use of any PED which has the capability to intentionally transmit electromagnetic energy should be prohibited unless testing has been conducted to ascertain its safe use.

4. While these recommendations are not reflected in FAR 91.21, similar precautions are commonly adopted by civil aircraft operators, that is, operation of PEDs is not permitted below 10,000 ft and intentional transmitters are prohibited.

PED ‘Safe Zones’

5. ADF aircraft are normally designed to be more immune to electromagnetic radiation than civilian aircraft. Despite this, ADF aircraft may in fact be more susceptible to interference from PEDs for the following reasons:

a. ***Physical Separation.*** Electromagnetic energy decreases rapidly with distance, and therefore physically separating PEDs from aircraft equipment is an effective means of minimising interference. In civilian aircraft, PEDs are almost always used in clearly defined areas (that is, while the passenger is seated), and therefore the physical separation between PEDs and aircraft equipment/wiring can be incorporated into the aircraft design. Military aircraft, on the other hand, do not always have clearly defined seating positions, they often have equipment racks and looming within the passenger compartment, and they allow passengers to move freely throughout the entire passenger compartment;

b. ***Differences in Role.*** Unlike civilian aircraft, the mission effectiveness of ADF aircraft is dependent on a wide array of electromagnetically sensitive equipment, for example, electro-explosive devices (EEDs), a profusion of antennas, sensitive role equipment (eg. Aeromedical equipment), and so on. Interference from PEDs can therefore be more than just a ‘nuisance’ factor, and their acceptability may depend on the configuration of the aircraft or even the particular mission phase; and

c. ***Modifications.*** Military aircraft are likely to undergo many more modifications than civilian aircraft during their lifecycle. Each modification has the potential to reduce the overall electromagnetic 'hardness' of the aircraft, for example, the lack of space within military aircraft often leads to non-optimal equipment locations and routing of wires, new capabilities may incorporate additional antennas which increase the likelihood of interference, and any one poorly designed or incorporated modification can introduce vulnerabilities both in itself and also to other systems.

6. Notwithstanding the above factors, larger ADF aircraft are likely to have PED 'safe zones', that is, areas where the risk from PEDs is equivalent to commercial aircraft, and therefore commercial airline precautions with PEDs may be adopted (ie. non-transmitting PEDs may be used freely during non-critical flight phases). Guidance for establishing these PED safe zones is provided in annex A. The remaining areas of the passenger compartment may be considered PED 'danger zones', and PEDs should not be used unless specifically authorised. These PED danger zones probably only account for a small portion of the available space in larger ADF aircraft.

7. Once the PED safe zone for an aircraft has been established, the critical phases of flight need to be defined. Take-off and landing are obvious candidates, however, there may be other phases (for example, times of high aircrew workload during missions) where even the slight possibility of system malfunction due to PED interference should be minimised. The final assessment of what constitutes a critical flight phase would probably be made by the aircraft captain, with guidance from local flying orders.

8. Table 18–1 provides a suggested list of endorsed PEDs. The 'approved' items are extracted directly from FAR 21.31, and have a proven safe history. The 'approved within PED safe zone' list attempts to encompass all common non-transmitting PEDs. While a blanket approval could be provided for all non-transmitting PEDs, this has the potential to remove engineering oversight from the list.

Table 18–1 Suggested PED Endorsement Table

Approved Items	Approved Within PED Safe Zone	Prohibited Items
Heart pacemakers	Video cameras/players	Any PED not included in the
Hearing aids	Cassette recorders/players	previous columns
Voice recorders	Compact disk players	
	Electronic games	Any PED capable of
	Radio receivers/scanners	intentional RF transmissions
	Portable TVs	
	Laptop computers/ peripherals	

Operational Imperatives

9. The commercial PED management procedures outlined above are probably adequate for the majority of ADF flights. However, operational imperatives may require the operation of a PED:

a. outside the designated PED safe zone (for example, a laptop computer immediately next to an equipment rack);

b. that intentionally transmits electromagnetic energy; or

c. during critical flight phases.

10. To ensure that the proposed arrangement will not compromise aircraft safety or mission capability, an individual assessment of the inherent risks by the relevant CENGR is required. The CENGR's assessment would be based on the likely emissions from the device, the vulnerability of nearby equipment and the potential consequences of interference. If a device's emission levels are unknown, it may require testing to a known standard. Conversely, if the areas where the device is to be used are undefined, then it may be necessary to test the PED to a stringent level that is known not to interfere with any aircraft systems (eg. MIL-STD-461E testing). The CENGR's endorsement would

specify the particular device, where it can be used, and the flight phases during which it can be operated. Annex B provides guidance on assessing non-standard PED operation.

Annexes:

A. PED Safe Zone Assessment

B. Non-Standard PED Assessment

Blank Page

PED SAFE ZONE ASSESSMENT

1. When assessing the interference potential between PEDs and aircraft systems, three modes of coupling need to be considered, namely PED-to-equipment, PED-to-wiring and PED-to-antennas. Once the safe distances for each of these modes have been established for a particular aircraft, a PED safe zone can be defined.

2. For illustration purposes in this annex, worst-case PED emissions of 1 V/m (within a few centimetres of the PED) will be assumed. The following is an attempt to quantify a worst-case PED: RTCA/DO-233 examined the emissions from a range of PEDs, and the worst case encountered was a laptop computer which displayed peak emissions of 85dBµV at one metre from the device. However, their PED sample size was limited to 37 devices, which is unlikely to be representative of worst-case PED performance. To establish a wider sample size, a leading Melbourne E^3 testing laboratory was contacted, and they stated they had never seen emissions exceeding 90dBµV (measured quasi-peak) for this type of equipment. An industry rule of thumb is to add 12dB to convert from a quasi-peak measurement to a peak measurement, taking the worst-case PED to 102dBµV. RTCA/DO-233 suggested that if multiple PEDs on the same aircraft were all radiating the same frequency, then a maximum overall signal increase of 8dB could be expected. Conservatively, therefore, worst-case PED emissions of 110dBµV (about 0.3V) at one metre from the PED may be possible, and therefore emissions in excess of 1V could be encountered within a few centimetres of the PED.

PED to Equipment Coupling

3. RTCA/DO-233 disregarded any possibility of PEDs coupling directly to critical aircraft equipment, probably because they cannot be collocated on civil aircraft. However, within military aircraft, electronic equipment is often located within or immediately adjacent to the passenger compartment. While this equipment is not likely to affect safety, it may be mission-critical and therefore PED-to-equipment coupling must be considered.

4. Safety-critical equipment on an aircraft will normally be rated to withstand between 100V/m and 200V/m. Even allowing for significant degradation of the equipment over its lifecycle, susceptibility to PED emissions for this equipment is still exceedingly unlikely. However, some categories of non-critical aircraft equipment only require testing to 1V/m. In this case, even without allowing for some equipment degradation over the years, there is potential for PED interference. As such, some separation between equipment and PEDs would be prudent.

5. To determine a ‘PED safe zone’ from equipment, a survey of the equipment in the aircraft passenger compartment would be required, followed by an assessment of the electromagnetic immunity of each piece of equipment. Some testing of the shielding effectiveness of the equipment racks or bulkheads could also be incorporated into the assessment. Adequate safety margins would then be added, and the resulting safe zone defined. If deemed necessary, some limited testing might be conducted to confirm the analysis.

PED-to-Wiring Coupling

6. RTCA/DO-233 concluded that harmful interference from PEDs was unlikely to couple onto cables. However, the methodology used to arrive at this conclusion was questionable, and may be a reflection of the limited scope of analysis undertaken in the study. For ADF aircraft, a similar approach to paragraph 4 should be adopted, where the conducted susceptibility rating of equipment, the shielding effectiveness of applicable wires and the worst-case PED emissions be used to arrive at an appropriate separation distance.

PED-to-Antenna Coupling

7. The extremely small signal levels used by aircraft antennas (including connectors and associated cabling) makes them a prime target for interference from PEDs. RTCA/DO-233 suggested that 81% of all recorded PED interference cases (137 in total) were associated with the aircraft navigation systems. Analysis in RTCA/DO-233 confirmed that there was potential for PEDs to interfere with navigation systems, although the probability was quite low. In fact, this was the only type of coupling considered as a real possibility in the study.

8. While it would be possible (with substantial difficulty) to predict how PEDs might couple to an aircraft's antenna systems, the results are unlikely to be particularly useful since they rely on a number of independent conditions that are difficult to predict. Realistically, the chance of a PED insidiously affecting a navigation system is extremely low, since there would normally be some outward sign of interference (eg. erratic pointer movement). RTCA/DO-233 suggested that since banning all PEDs was not a realistic option, an acceptable alternative was to ensure that PEDs were used only during non-critical phases of flight. This latter approach has been adopted successfully by the civilian airlines, and it also appears a reasonable approach for the ADF to adopt.

NON-STANDARD PED ASSESSMENT

1. The PED management procedures used by civilian aircraft operators are probably adequate for the majority of ADF flights. However, operational imperatives may require the operation of PEDs outside these bounds. If so, there is an increased risk of the PED electromagnetically interfering with aircraft equipment, and therefore endorsement by the relevant CENGR should be sought. This annex provides some basic guidance on how the CENGR might approve non-standard PED operations.

Operation of PEDs Outside the Safe Zone

2. Assessment of a PED for use in the PED 'danger zone' could be achieved along the following lines:

a. if the approximate emission levels for the PED are known (eg. it is a popular brand name, and marked as tested to a recognised commercial E^3 standard) and it will not be used in the vicinity of safety-critical equipment/wiring, little further analysis would probably be required. Source/victim testing might be used if there was thought to be potential for interference with mission-critical equipment or wiring;

b. if there is any uncertainty in the device's emission levels it may require testing to a known standard, either commercial or military; and

c. if the device is to be used immediately adjacent to safety-critical equipment or wiring then it would need to be tested to a stringent level that is known not to interfere with any aircraft systems (eg. MIL-STD-461E). Similarly, if there is any uncertainty as to where in the aircraft the device might be used, such testing may also be required.

Operation of Transmitting PEDs

3. If a transmitting PED is to be used in an aircraft, the safe distances from safety-critical and mission-critical equipment and wiring (based on the immunity ratings of the equipment) could be calculated. In addition, a frequency band assessment could be conducted to determine likely interference with the aircraft's radios and navigation systems. A suitable safety margin would then be added to all analysis figures, and an appropriate area of the aircraft assigned for the transmitter. Source/victim testing would probably then be conducted, first on the ground and then airborne, to assure the validity of the analysis.

Operation of PEDs During Critical Flight Phases

4. Provided the PED is to be used in a PED safe zone, is non-transmitting and has an extensive proven history in the same aircraft and location, little additional analysis or testing may be necessary. However, if any of these conditions are not met, risk mitigation strategies such as those outlined in paragraphs 2 and 3 are advisable.

Blank Page

SECTION 2

CHAPTER 19

HEALTH AND USAGE MONITORING SYSTEMS

INTRODUCTION

1. Health and Usage Monitoring System (HUMS) is an all-encompassing term for systems that perform a multitude of maintenance and airworthiness related tasks, and refers not just to equipment but also to the systems and procedures required to manage the information. The purpose of a HUMS is to improve flight safety, aircraft availability, maintainability, the ability to complete a mission, and to reduce life-cycle costs.

2. Health and Usage Monitoring covers two aspects of aircraft maintenance. Health monitoring can be performed through programs such as propulsion system condition monitoring or airframe environmental degradation assessments and can produce qualitative or quantitative review of the condition of the aircraft as a whole. Usage monitoring focuses on estimating accumulated damage effects on airframe primary structure, helicopter dynamic components or engine critical parts by measuring usage, and predicting damage from relationships between usage and life, as established during the design phase. It is when these two activities are combined and significantly automated that the term HUMS is typically applied. However, this chapter also (specifically para 11 and Annex A) addresses non-automated systems.

3. This chapter provides specification guidance and certification requirements for a HUMS where it directly relates to the monitoring of engine critical parts, airframe structure or helicopter dynamic components. The scope of this chapter is the acquisition of new aircraft with a HUMS fitted and for the retrofit of existing aircraft with a HUMS. The later sections of this chapter detail the management systems that must be put in place by Systems Program Offices (SPOs) to support a HUMS. Many avionics systems have Built In Test Equipment (BIT or BITE). This chapter is not concerned with this type of equipment.

4. The parts of a HUMS that are the most relevant for a particular platform depend on the configuration, role and environment of the platform. While a HUMS may contain a variety of on-board monitoring technology, the common sub-systems that constitute HUMS are:

a. turbine engine and transmission usage monitoring;

b. airframe and dynamic component usage monitoring, through parametric and/or strain based monitoring of loading for critical structural components;

c. engine, gearbox and airframe vibration monitoring;

d. engine performance (gas path, or power-check) monitoring; and

e. helicopter rotor track and balance.

5. It is unlikely that an automated HUMS would fulfil all the requirements for health or condition monitoring of an engine or airframe. Other established techniques that may assist in the health monitoring of aircraft are listed below, and should be treated in the relevant section of the ESIMP or ASIMP. Further details on these techniques are outlined in AAP 7001.059(AM1).

a. Non Destructive Inspection (NDI) of critical structural locations;

b. Structural condition reporting and data-basing

c. Wear Debris Analysis;

d. Spectrographic Oil Analysis;

e. Vibration analysis;

f. Performance monitoring;

g. Remote visual inspection (borescopic inspection) and

h. Oil Condition Analysis.

Cost-Benefit Analysis

6. There is the potential that significant savings can be achieved through use of a HUMS, but it has also been shown that many of these savings could be achieved through use of a more simplified system. Before developing a HUMS specification for a retrofit or new acquisition, it is essential that an analysis of the identified engine critical parts or airframe structure is performed and the benefit of monitoring these components or structure quantified. Ideally a full requirements analysis will be conducted and it should define those components or structure whose usage must be monitored for airworthiness reasons and identify those components or structure which, due to time and cost of replacement, would benefit from an effective health and usage monitoring program. Health monitoring is conducted to increase operational safety and availability, and reduce life cycle cost (LCC). Effective health monitoring helps to better plan maintenance to prevent further costly damage. When considering the cost of a HUMS the SQN, SPO, DSTO and DGTA ongoing and development costs must be included. DSTO and DAIRENG can provide practical assistance in conducting this analysis.

HUMS Fundamentals

7. DEF STAN 00-970 Issue 3 Part 1 Section 6 requirement 6.15.5 may be consulted for fundamental requirements for HUMS equipment. Requirements for fixed-wing airframe and all engine usage monitoring systems should be developed in consultation with Aircraft Structural Integrity Section ASI-DGTA and for rotary wing aircraft, with Rotary Wing Section RWS-DGTA. This chapter emphasises the requirements for usage monitoring as this is the main airworthiness focus. The requirements for health monitoring will have many similar requirements but will need to be tailored to suit the particular application. The requirements of a HUMS are dependent on the application, ie whether it is for engines, airframe or helicopters.

8. **Engines.** All gas turbine engines contain critical parts, the failure of which has the potential to cause the loss of an aircraft. These components are usually the high-speed rotating components that have sufficient energy that their failure will be uncontained. The compressor and turbine disks are typical examples. Modern gas turbine engine critical parts generally suffer from Low Cycle Fatigue (LCF), Thermal Fatigue and/or Creep. It is industry practice to set a throwaway life on these critical parts beyond which the risk of failure becomes unacceptably high. These lives are often given in cycles and hours. To monitor the accrual of these cycles and hours, recently acquired aircraft use an Engine Usage Monitoring System (EUMS). The EUMS is an integral part of the lifing of the critical parts, and therefore fundamental to the continuing airworthiness of the aircraft. The key requirement of an EUMS is that it accurately records all events that the engine manufacturer deems to be significant in determining critical component lifing. The EUMS equipment requirements should be included within the certification basis of the aircraft and thus require appropriate development oversight and certification. Health monitoring may also be integrated into the same software/hardware package, determining engine health based on performance data, data from vibration sensors, or chip detection using magnetic plugs or an electronic sensor.

9. **Airframe.** A HUMS should monitor all locations on an airframe that are determined by the Original Equipment Manufacturer (OEM) to be critical to the economic life of the aircraft or primary structure where failure due to fatigue is possible within the life of type of the aircraft. The life of this structure should be verified through structural demonstration or analysis. HUMS will monitor these locations through the monitoring of loads in the critical structure via strain and/or flight parameter recording. Health monitoring for aircraft structure is rarely automated, as sensors with the capability to significantly improve on visual inspection have generally not progressed past the trial stage to date.

10. **Helicopters.** The main rotor and tail rotor systems of a helicopter contain high speed, rotating dynamic components. These components are critical, as their failure may lead to loss of an aircraft. The purpose of the HUMS is to record the parameters of the usage spectrum utilised in determining component retirement times (CRT). The HUMS allows the accrual of dynamic component fatigue to be monitored and any deviation from the usage spectrum to be highlighted. Health monitoring for helicopter powertrains uses many of the same techniques as for aircraft engines, such as vibration and oil-debris analysis.

HUMS SPECIFICATION GUIDANCE

11. Requiring Health and Usage Monitoring. Systematic monitoring of health and usage of airframe and propulsion systems (with or without automation) is essential for continued airworthiness. Different specifications exist in different aircraft standards, but there is usually limited guidance. Therefore, the Project Office must include delivery of health and usage monitoring systems (in the broadest sense) for the airframe and engine in the specification. Example specification requirements are detailed in annex A. The rest of this chapter is primarily concerned with managing problems arising from automation of parts of the usage and condition monitoring cycle.

12. The health monitoring and usage monitoring functions may include some automation at various stages, but will eventually require a human interface to make a maintenance decision or carry out a maintenance action. The automated sections of a HUMS must be shown to meet the design requirements for the whole system. The following points are highly desirable features of a HUMS:

a. HUMS equipment should be fitted to each aircraft and engine: much of the benefit of HUMS comes from the fidelity of the system, and this fidelity is lost if data is extrapolated from one airframe to another.

b. HUMS equipment should store a significant proportion (preferably 100%) of the raw data generated, so that if a life limit processing algorithm changes, new accrued lives can be calculated from historical raw data. This obviously creates a significant burden of data storage, which should be balanced against the stability of the lifing algorithms.

c. HUMS equipment data formats should be published by the contractor to allow for easier upgrade of software, and easier interface with third-party software.

d. HUMS equipment should have Built-in Test functions (BIT) and clear fault indications to ensure that a faulty component is quickly removed from service.

HUMS CERTIFICATION

13. Usage Monitoring. If automated HUMS is to be considered the executive lifing tool for engine critical parts, and dynamic and structural components, it is essential that certification of the HUMS forms part of the certification basis for the aircraft type. Certification of the HUMS is broader than just ensuring that the computer hardware and software does not interfere with other airborne systems. The mathematical algorithms incorporated in the system must also be validated against the engine and component lifing algorithms used by the OEM. It is common that HUMS data will need some form of processing by a ground station before it can be entered into the ADF maintenance management system. The aim of the certification process of the HUMS should be to show that it is robust, sufficiently accurate for use as the critical part executive lifing tool.

14. Health Monitoring. If the benefit of the HUMS is required for the aircraft to meet its systems safety targets for certification, the functionality and reliability claimed **must** be validated. In particular the testing and analysis that lies behind the algorithm design must be examined. Some aircraft fitted by the manufacturer with HUMS equipment do not claim the safety benefit in the certification process, and the HUMS is acknowledged as an additional but unquantified safety measure. In this case, the ADF would still be imprudent to accept the HUMS design without an appropriate verification of the design and well-planned introduction to service.

15. Ground-side support. HUMS require complete integration in the aircraft maintenance management and engineering management systems to remain effective. A HUMS cannot achieve its goals unless it is integrated with the configuration and maintenance management systems. The HUMS and its ground station will require specific processes and training for users.

16. HUMSVP. Annex B contains information for Project Offices to assist in the development of a Data Item Description (DID) for the Contractor to deliver a HUMS validation plan (HUMSVP). The Commonwealth will use the HUMSVP to assess the acceptability of the validation activity for the system offered by the Contractor. The contractor may provide separate validation plans tailored for discrete systems. Where the system has already undergone prior validation, the HUMSVP can be used to describe the prior validation activity and demonstrate how the prior activity meets the intent of the DID.

17. **IV&V.** DSTO and ASI-DGTA have considerable experience with performing certification of HUMS and will usually assist with the assessment of a delivered HUMSVP and can provide specialist advice or perform independent verification and validation activities as required by the HUMSVP.

18. **Access to data.** The certification of a HUMS will require disclosure of sufficient data to make the necessary compliance findings. If the engine, aircraft or HUMS OEMs are not the prime contractor, the prime must ensure the data required for certification is available for Commonwealth review. It is essential that access to this information be negotiated before contract signature, as there may not be a practicable engineering alternative to use of the HUMS for life tracking and this may require management through a service release limitation.

HUMS MANAGEMENT

Threshold Setting and Adjustment

19. Current HUMS sub-systems generate indicator values from vibration recordings taken from different positions on the component or system being monitored. These indicators will show different pre-failure, wear or out-of-limit conditions for the component or system. An example for engines is gear tooth damage, shaft imbalance, or shaft misalignment. Each indicator value will alert the maintenance unit to investigate the problem.

20. All thresholds must be defined whether in the form of absolute signal values, number of standard deviations above the mean fleet value, or other means. Any change to these values should be agreed by the aircraft OEM and recorded along with the reason and justification for the change.

Minimum Equipment List

21. Generally, the HUMS is not a mission or safety-critical system and an unserviceability with it should not prevent short-term availability. As long as defined and approved provisions are in place to replace lost usage data, continuing airworthiness of the system will not be compromised.

22. The maximum allowable unserviceable period of any items of HUMS equipment will need to be approved by the SPO and defined in a minimum equipment list. The factors to be considered in establishing acceptable periods for HUMS equipment unserviceability should include:

a. The projected life remaining of critical parts;

b. The cost of applying conservative fill-in data;

c. Propagation rate of the failure mode being monitored;

d. Other means of monitoring the same failure mode;

e. Service history of similar failures on the aircraft type; and

f. Any mitigating actions, such as checking previous HUMS data to establish the indicator level and look for rising trends.

Training

23. Training must cover all personnel involved in the HUMS activity to ensure that the competencies necessary to ensure effective use of the systems can be achieved and maintained. Experience with health and usage monitoring to date has indicated that training is needed to make full use of the system. This can range from basic computer skills to detailed training in the vibration or lifing algorithms and their significance. The OEM or HUMS manufacturer should be contracted to provide training packages that meet all HUMS training requirements.

Annexes:

A. Example of Specification Clauses for Usage Monitoring and Health Monitoring

B. Example of Data Item Description – Health and Usage Monitoring System Validation Plan

EXAMPLE OF SPECIFICATION CLAUSES FOR USAGE MONITORING AND HEALTH MONITORING

Table 19-A-1

Title	Revision Status	Requirement	Compliance Method	NAA Involvement	Compliance Evidence Documents	Comments		Compliance Finding Agency	Compliance Outcome	Finding Reference
Airframe Usage Monitoring System		The contractor shall provide a validated structural usage monitoring system that enables tracking of critical aircraft structural component lives in accordance with AAP7001.054 Section 2 Chapter 11, Chapter 19 and AAP7001.053 TAMM Reg 3.5.4.	Analysis and Test	Prior acceptance documents may be presented.	HUMSVP ASIMP			DGTA, DSTO		
Propulsion System Usage Monitoring		The contractor shall provide a validated propulsion system life usage monitoring system that enables tracking of safety critical engine component lives in accordance with AAP7001.054, Section 4, Chapter 1 and Section 2 Chapter 19 and AAP7001.053 TAMM Reg 3.5.5.	Analysis and Test	Prior acceptance documents may be presented.	HUMSVP ESIMP			DGTA, DSTO		
Airframe Operation Loads Monitoring System		The contractor shall have a validated Operational Load Monitoring (OLM) system that meets the requirements of AAP7001.054 Section 2 Chapter 11, Chapter 19 and AAP7001.053 TAMM Reg 3.5.4.	Analysis and Test	Prior acceptance documents may be presented.	HUMSVP ASIMP			DGTA, DSTO		
Propulsion System Condition Monitoring System		The contractor shall provide a system for propulsion system condition monitoring that appropriately monitors system performance and serviceability in accordance with AAP7001.054, Section 4, Chapter 1 and Section 2 Chapter 19 and AAP7001.053 TAMM Reg 3.5.5.	Analysis and Test	Prior acceptance documents may be presented.	HUMSVP ESIMP			DGTA, DSTO		

Blank Page

EXAMPLE OF DATA ITEM DESCRIPTION HEALTH AND USAGE MONITORING SYSTEM VALIDATION PLAN

1. DID NUMBER: DID-ENG-XXX-HUMSVP

1.1 TITLE: HEALTH AND USAGE MONITORING SYSTEM VALIDATION PLAN

2. DESCRIPTION AND INTENDED USE

3.1 The Health and Usage Monitoring System Validation Plan (HUMSVP) describes the Contractor's plan for validating any ‘system(s)’ to determine the health, fatigue life usage monitoring or operational loads measurement (OLM) of the; propulsion system, dynamic components or airframe components.

3.2 The Commonwealth will use the HUMSVP to assess the acceptability of the validation activity undertaken for the system offered by the Contractor. The contractor may provide separate validation plans tailored for discrete systems. Where the system has already undergone prior validation, the HUMSVP can be used to describe the prior validation activity and demonstrate how the prior activity meets the intent of this DID.

3.3 Where the system OEMs is not the prime contractor, the prime must ensure contractual coverage to ensure the data required for certification and validation is available for Commonwealth review.

4. INTER-RELATIONSHIPS

4.1 Nil

5. APPLICABLE DOCUMENTS

5.1 AAP7001.054 – Airworthiness Design Requirements Manual, Section 2 Chapters 11 and 19 and Section 4 Chapter 1.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL Description clause entitled "General Requirements for Data Items".

6.2 Specific Content

6.2.1 The HUMSVP shall describe any propulsion system, dynamic component or airframe health, fatigue life usage or operational loads monitoring system offered by the Contractor.

6.2.2 The HUMSVP shall detail how the contractor plans to address the following:

a. **Electromagnetic Compatibility (EMC).** Ensure the electromagnetic compatibility (EMC) of the system with the parent aircraft.

b. **Environmental Effects.** Ensure that the system is not adversely affected by environmental effects such as; temperature, vibration, humidity, salt spray, dust and sand conditions.

c. **Software Design.** Ensure that all embedded software is developed to meet appropriate software assurance objectives as defined by an appropriate software assurance standard and the overall platform system safety goals. As for other HUMS elements, prior acceptance may be recognised. Normally, use of an appropriate assurance level of DO178B would satisfy the software validity requirement.

d. **Lifing Algorithm Validation.** Ensure the accuracy of any algorithms required to calculate damage accrual and summation of damage. For all algorithms, the contractor shall perform validation testing. This testing should include synthetic missions exercising the extremes of the

flight envelope and real missions to ensure satisfactory operation with transient operational data. The linkage of these algorithms to those used in the establishment of aircraft or engine component safe lives or inspection call outs are to be explicitly stated. Where the algorithms differ (from those used in the establishment of said lives or inspections) evidence is to be provided that satisfactory comparable results are produced when representative data is processed through both algorithms. Note: Fatigue is the most common usage-driven failure mode, and throughout this document the term 'cycle' is used to denote the basic unit of OEM-defined fatigue life. Logically, other failure modes such as creep have equivalent requirements that must also be addressed.

e. **Condition Monitoring Algorithm Validation.** Ensure the accuracy and efficacy of algorithms used to assess the condition (serviceability) of components and systems. The contractor shall provide evidence of validation testing and analysis for all systems. This testing should include synthetic missions exercising the extremes of the flight envelope and real missions to ensure satisfactory operation with transient operational data. The linkage of these algorithms to those used in the establishment of aircraft or engine component condition or inspection call outs are to be explicitly stated.

e. **Data Sampling Rates.** Ensure that data sampling rates are appropriate for each parameter, whilst maintaining a manageable level of data.

f. **Raw Data Integrity.** Ensure the integrity of raw data by addressing the following, as a minimum:

(1) **Ground Cycle Counts.** Ensure during ground runs that cycle counts are accurately recorded by the system. If ground cycle counts are not required, the HUMSVP shall include the engine and aircraft OEM's usage assumptions for ground running.

(2) **Flight Cycle Counts.** Ensure that cycle counts are accurately recorded by the system during flight. For the engines, this should include ensuring that in-flight shutdowns result in the correct number of cycles being counted on correct engines. For the airframe, this should include ensuring that touch-and-go landings are counted in an appropriate and consistent manner.

(3) **Cycle trigger.** Ensure that the system is consistent with the OEM definitions for engine and aircraft flight and fatigue cycles

(4) **Hours**. Ensure that the engine hours and flight hours reported by the system reflects actual ground running and flight times.

(5) **Engine and Flight Parameters.** Ensure the accuracy of engine and flight parameters such as; engine gas temperatures, pressures, revolutions per minute, airspeed, altitudes, Nz and other applicable aircraft performance data.

g. **Strain Gauges.** Where strain gauges are utilised, a description of all locations and installation procedures are to be provided.

h. **Calibration.** Ensure that all sensors and devices used in the system are appropriately calibrated and that a process for on-going assessment and re-calibration is verified and provided.

i. **Functionality Tests.** The HUMSVP shall describe validation of the system's function, as required and defined by the engine and aircraft OEM. Depending on the system specification this may include:

(1) cycle counts;

(2) engine hours;

(3) airframe flight hours;

(4) applicable exceedances (eg rpm, temperature and vibration, Nz);

(5) alerting the ground operator of any invalid data;

(6) calculating any performance margins that drive on-condition maintenance activities such as engine removals; and

(7) applicable condition monitoring data; eg rpm histories, vibration spectra, performance histories.

j. **Life Usage Indices (LUI).** Ensure the validity of any system reported LUIs.

k. **Lifing Database**. Ensure the integrity of all data.

l. **Lifing Database Design and Storage.** Verification of the design and data storage functions of the ground-based lifing database. As a minimum the following shall be assessed:

(1) The storage medium has adequate capacity to accommodate the database as it grows;

(2) Raw data sets are identified;

(3) There is a back-up process adequate to ensure complete redundancy, and it is fully implemented; and

(4) The retrieval of data sets has been tested and proven.

m. **HUMS Data Management Procedures.** Ensure that a controlled Data Management Procedure exists for the system and ensure that it addresses the following:

(1) Data flow management processes from the aircraft to the final lifing database for operational and deeper maintenance;

(2) Data flow management processes for any condition monitoring program that requires the use of data collected by the HUMS;

(3) Database security;

(4) Database access;

(5) Database backup procedures;

(6) Database archiving procedures;

(7) Management of missing/invalid data; and

(8) Management of exceedances in parameters such as temperature, pressure, rpm and Nz.

n. **Management of Significant Events (Invalid, Missing and Exceedance Data).** Ensure that the following is addressed:

(1) The system generates appropriate alert messages to maintenance staff when significant events occur such as invalid raw data and exceedances.

(2) The integrity of the process used to manage invalid data, ie whether the system accounts for invalid data automatically or it needs to be accounted for manually by maintenance staff.

(3) That the percentage of invalid data is within the engine or aircraft OEM’s acceptable limits. These limits are to be stated.

o. **Fill-in Factors.** Ensure that any ‘fill-in’ or conversion factors used to manage missing/invalid data are appropriate. Justification for the chosen ‘fill-in’ or conversion factors shall be provided and shall reflect ADF mission types and mission mix as documented in the approved Statement of Operating Intent (SOI).

p. **Configuration Changes.** Ensure usage cycles are correctly tracked when a configuration change occurs such as engine removal and installation, engine component replacements, new component configurations. Similarly, ensure that when configuration changes occur on the aircraft (for components that require usage cycles to be tracked by HUMS, such as control surfaces) that the HUMS correctly accounts for this.

q. **Software Upgrades.** Ensure that a process exists for modifying the system software and any of its default parameters. This process should include the requirement to state if historical data needs to be reprocessed with the modified software/default parameters, or if only new data needs to be processed using the new software/default parameters.

r. **CAMM/2 Interfaces.** It is desirable that the system database interfaces with CAMM/2. Verify functionality and ensure that lifing parameters tracked on CAMM/2 correspond to the parameters tracked on the system.

Blank Page

SECTION 2

CHAPTER 20

AERONAUTICAL LIFE SUPPORT EQUIPMENT (ALSE)

INTRODUCTION

1. Aeronautical Life Support Equipment (ALSE) has typically not been considered as technical equipment, and subsequently has been over looked in the design phase of ADF aircraft acquisitions and upgrades. DEF STAN 00-970 does not adequately cover the ADF requirements for ALSE. Consequently, this chapter provides specific ALSE design requirements. ALSE design requirements will inevitably overlay onto aircraft, human factors and functional design requirements for a diverse range of engineering activities. This chapter will provide guidance on ADF preferred standards applicable to ALSE designs, thus enabling applicable agencies to define their requirements.

2. This chapter will not cover common airborne oxygen systems, specific fabric, webbing, thread and cordage requirements. Further guidance should be sought from Aerospace Equipment System Support Office - Aeronautical Life Support Equipment (AESSO-ALSE).

Definitions

3. ALSE can be defined as equipment that supports aircrew in the performance of their duties in aircraft. This distinguishes ALSE from personal protective equipment (PPE) used in the field by ground forces, although some of the equipment managed by AESSO-ALSE can perform this dual function.

4. The definition also provides a foundation to further expand the meaning of ALSE into its two primary types. The two types of ALSE that provide fundamental support to ADF aircrew are:

a. ***Mission Critical Equipment.*** Such equipment sustains a higher level of physical performance than otherwise possible. Examples include aircrew (ejection based) protective helmets, laser protection duties (typically helmet visors), Anti-G garments, oxygen masks, personal restraint harnesses, and Night Vision Goggles.

b. ***Emergency/Survival Equipment.*** Examples include aircrew (impact protective) helmets, immersion suits (quick don and constant wear), personal flotation devices & survival vests, single and multi-seat life rafts, ballistic protection devices, locater beacons (life raft, personal and emergency), Air Sea Rescue Kits (ASRK), storpedoes, survival aids and survival packs.

5. While both types of ALSE are managed and specified to assure aircrew safety, the definitions provide for understanding the safety criticality of various ALSE.

AIRWORTHINESS REQUIREMENTS

6. ALSE should be designed to meet the needs of aircrew for all aircraft mission phases including use after or during an aircraft incident or accident. In addition to meeting the ALSE unique design requirements, installed ALSE must also function properly within the aircraft operating environment. Consequently, two ‘standards’ may apply to ALSE, that being the weapon platform environmental standard and also the individual ALSE’s design standard. There are four primary sources of ALSE design certification criteria. Those areas include civil regulations including FARs, JARs or CASA regulations; the Air Standardisation Coordination Committee (ASCC) working party agreements; MIL-SPEC/Std’s (and DEF STAN970-00 where applicable), and the RAAF Spec Eng/DEF(AUST) series of specifications.

7. With the ADF currently acquiring aircraft that are civil certified (FAR/JAR), it must be emphasised to project offices and SPO's that although the ALSE (e.g. Life rafts) on board are civil certified, the equipment may not be appropriate for the intended ADF role, configuration and environment in which the aircraft will be used. Therefore, advice on the appropriate ALSE specifications/standard to be used for the equipment on-board these types of aircraft should be sought from AESSO-ALSE as early as possible within the acquisition cycle.

8. The MIL–SPEC/Std's (including TSO's) and RAAF Spec Eng 'S' series/DEF(AUST) series are the preferred specifications for ALSE. Although FAR/CASR and ASCC provide acceptable requirements, RAAF Spec Eng/DEF(AUST) requirements are mandatory for specific design aspects. The RAAF specifications/DEF(AUST) are tailored to ALSE employed in the Australian environment.

GUIDING PRINCIPLES

9. In the production of ALSE designs suitable for ADF service, the equipment should be suitably integrated with the person, the aircraft and the remainder of the aircrew ensemble. This ensemble methodology is used by AESSO-ALSE to design and integrate ALSE.

Aircrew Ensembles

10. Aircrew Ensembles are evaluated for their individual design specifications and standards as well as for their physical and functional performance in the specific weapon platform. When considering the certification of Aircrew Ensembles or the equipment that constitutes those designs, the design variables are expanded from the following primary considerations, those considerations include:

a. Equipment to Equipment interface and integration;

b. Equipment to Person interface and integration, and

c. Equipment to Aircraft interface and integration.

11. The use of the Ensemble model highlights the factors for consideration in both certifying new components into an existing aircraft ensemble, and the subsequent certification of the ensemble for use on a platform. Simple considerations, such as the effect of harness interference, ejection sequences or allowing the aircrew to perform their intended role without creating heat exhaustion may be overlooked without considering this framework.

ASSOCIATED STANDARDS

12. Broad guidance for ALSE design requirements is included in the following FARs:

a. FAR 23/25.1415 Ditching Equipment;

b. FAR 25.1439 Protective Breathing Equipment, and

c. FAR 23/25.1561 Safety Equipment.

13. ALSE should also meet the interoperability requirements of the following Air Standardisation Coordination Committee (ASCC) working parties:

a. ASCC WP 14 Gaseous Systems (AAP 8130.001-4);

b. ASCC WP 51 Survival Search and Rescue (AAP 8130.001-14);

c. ASCC WP 61 Aerospace Medicine, Life Support and Aircrew Systems (AAP 8130.001-17B1); and

d. ASCC WP 84 NBC Defensive Systems (AAP 8130.001-22).

14. ALSE should meet the design requirements commensurate with the operating environment of applicable aircraft as well as complying with ASCC and FAR requirements. In addition, each class of ALSE should comply with the following design standards where practicable.

a. ***Aircrew Protective Helmets***

(1) ANSI Z90.1-1992 for Protection Headwear for Motor Vehicle Users Specification

(2) MIL-H-87174, Helmet Flyers HGU-55/P

(3) MIL-H-43925D, Helmet Flyers Protective SPH-4

(4) MIL-H-85047A, Helmet Assembly HGU 34/P

(5) AS1270-1988, Acoustic Hearing Protective Equipment

(6) MIL-STD-27796D, Connector Bayonet, Three Pin, Oxygen Mask

(7) NOHSC:1007 (1993), National Standard for Occupational Noise

(8) DEFSTAN 00-970 Pt 1 Section 4 Issue 2 Supp 66, Requirements for Human Exposure to Noise and Vibration in Cockpits and cabins, General Procedures for Acoustic Measurements

(9) MIL-C-83409, Coatings, Visor, Polycarbonate, Flying Helmet

(10) MIL-V-43511C, Visors, Flyer's Helmet, Polycarbonate

(11) MIL-V-85374(AS), Visors, Shatter Resistant

(12) ASCC 61/102/8 Evaluation Procedures for Flying helmets

(13) ASCC 61/113/15A The Optical and Material Requirements for Aircrew Helmet Visors

(14) MIL-C-83409 (USAF) Coating, Visor, Poly Carbonate, Flying Helmet

(15) MOD (UK) DTD SPEC No 1218 Optical Requirements for Aircrew Helmet Visor and Uncorrected Sunglasses

b. ***Laser Protection***

(1) MIL-V-22272D(AS)QPL-22272-10, Visors, Neodymium Laser, Protective for Aircrewman's Helmet Visors

c. ***Ballistic Protection***

(1) National Institute of Justice – Level 3 and 3A

d. ***Anti-G Garments***

(1) MIL-A-83406B Anti-G Garment, Cut Away, CSU-13 B/P

e. ***Oxygen Masks***

(1) MIL-C-19246C, Connector Oxygen Mask Hose, type MC-3A

(2) MIL-C-38271B , Connector Oxygen Mask to Regulator CRU-60/F

(3) MIL-M-19417D, Mask Assembly, Oxygen and Smoke, Full Face

(4) ASCC 61/101/6A Minimum Physiological Requirements for Aircrew Demand Breathing Systems

(5) ASCC 61/101/5A Pysiological Requirements for Aircrew Oxygen Masks for use at High Breathing Pressures

f. ***Immersion Protection***

(1) ASCC 61/114/10 Methodology for Assessment of the Thermal Performance of Immersion Protective Clothing

(2) DEF (AUST) 9200 - Coveralls, Flyers, Anti-Exposure (Constant Wear)

g. ***Personal Flotation Devices***

(1) MIL-O-81375B, Oral Inflation Assembly, Safety Equipment

(2) MIL-C-25369C , Cylinders, Carbon-Dioxide for Inflation of Pneumatic Life Preserver

(3) RAAF Spec S3 Single Seat Liferafts to RAAF Ejection Seat Aircraft

(4) RAAF Spec S10 Life Preservers

(5) NAVAIR 13-6-6.1-2 Technical Manual, Aviation-Crew Systems, Inflatable Survival Equipment (Life Preservers)

(6) ASCC 61/114/1 Aircrew Inflatable Life Preservers, Flotation and Related Requirements

(7) ASCC 61/114/12 Methodology for the Measurement of Inherent Buoyancy of Aircrew and Passenger Clothing

(8) TSO C13f Life Preservers

(9) TSO C72c Individual Floatation Devices

h. ***Multi-Person Flotation Devices***

(1) RAAF Spec S9, Multi-seat Life Rafts

(2) RAAF Spec S5, Recharging and Reconditioning of Floatation Compressed Cylinders

i. ***Personal and Stowed Distress Devices.*** In addition to Section 2 Chapter 3 paragraphs 27 and 28, the following standards warrant consideration

(1) AS/NZS 4280:2, 406MHz Satellite Distress Beacons - Personnel Locator Beacons (PLBs)

(2) TSO-C91a – Emergency Locator Transmitter (ELT) Equipment

(3) TSO-C-126, 406 MHz Emergency Locator Transmitter (ELT)

(4) CASA 103.40 Equipment Standards - Buoyant Survival Radio Beacons Operating On 121.5 and 243 MHz

(5) TSO-C142, Lithium Batteries

j. ***ASRK/Storpedoes***

(1) MIL-HDBK-1763 Aircraft Stores Compatibility (for equipment interface only)

(2) Installed equipment to storpedos/ASRK shall meet their individual design standard as well as the target weapon platform design standard

k. ***Survival Aids***

(1) MIL-B-8571D, Bag, Storage Drinking Water ‘Validated’.

(2) MIL-S-11262F, Sunburn Preventative Preparation (cream paste and lotion)

(3) RAAF Spec S4 Emergency Drinking Water (250 ml flexible bag/bag-500 rigid container)

l. ***Parachutes/Restraint Systems***

(1) AS 1891.1:1995 Industrial Fall Arrest Systems and Devices Pt 1: Safety Belts and Harnesses

(2) AS 1891.4:2000 Industrial Fall Arrest Systems and Devices Pt 4: Selection, Use and Maintenance

(3) MIL-H-5364D, Harness, Shoulder Safety, General Specification for

(4) MIL-R-8592B, Rescue Equipment, Helicopter

(5) ARMY(Aust) 6285 For Parachute, Personnel, Army Despatcher

m. ***Personal Survival Packs***

(1) MIL-P-116 Preservation, Methods of.

n. ***NVG Technologies***

(1) Some NVG design requirements are already covered in Section 2 Chapter 4, *Aircraft Lighting*, although they are primarily limited to aircraft lighting requirements needed to assure NVG compatibility. While Helmet Mounted Displays (HMDs) are expected to be managed by AESSO-ALSE in the future, design requirements for HMDs will be reviewed at next amendment

(2) STANNAG-7042 ED.2, Image Intenssifying Night Vision Devices for Aircraft

Blank Page

SECTION 2

CHAPTER 21

AIRBORNE ENVIRONMENTAL CONTROL SYSTEMS

INTRODUCTION

1. The Environmental Control System (ECS) provides temperature, humidity, ventilation and pressure control to passenger/cargo areas, aircraft systems and equipment. The system must be able to provide this control under any possible role, configuration and environment that the platform will operate in. The air provided may be derived from internal sources (engine or auxiliary power unit), external sources (ram air or air-conditioning cart) or an ECS dedicated compressor. Expended heat is usually dispersed external to the platform and needs to be controlled to meet platform safety and mission requirements. ECS functions and sub-systems may include, but are not limited to: pressurisation, heating, cooling, ventilation, moisture control, pressure and anti-G suit control, defogging, defrosting, anti-icing, rain removal, windshield washing, and electronic and electrical thermal management.

2. This chapter provides functional ECS requirements and advice on new acquisitions or modifications to existing platforms. All factors relating to the physiological requirements of crew and passengers (eg. hypoxia) are not covered, and oxygen system technical design requirements are addressed separately in Section 2 Chapter 6 of this manual.

CLIMATIC CRITERIA

3. As ADF airborne platforms can operate in extreme climatic conditions, ECS design and test requirements for airborne platforms must be carefully defined. Common world practice for establishing climatic conditions is through the use of MIL-HDBK-310. While DEF(AUST) 5168 aims to establish Australian regional climatic criteria (and the rest of the world generically), the information is very dated. For ADF airborne applications, the guidance in MIL-HDBK-310 should therefore be used as the initial benchmark. The Project Office (PO) or SPO should establish the role, configuration and environment in which the platform will operate, and deduce whether additional tailoring from DEF(AUST) 5168 is required to properly define the criteria both within and outside of Australia.

4. ***MIL-HDBK-310 Global Climatic Data for Developing Military Products.*** This standard provides climatic data primarily for use in engineering analyses to develop and test military equipment and materiel. The data provided is intended to serve as the natural environmental starting points for the sequence of engineering analyses to derive environmental design criteria for materiel. This handbook provides the latest information for defining global criteria, and now incorporates more information applicable to NATO countries. The disadvantage of the handbook is it broadly groups Australian climatic criteria, and therefore may not provide sufficient granularity for some aircraft operating environments. In addition, it does not cover the Antarctic region.

5. ***DEF(AUST) 5168 The Climatic Environmental Conditions Affecting the Design of Military Materiel***. The purpose of DEF(AUST) 5168 is to provide for military requirements documents, the intensities of climatic conditions under which military materiel must remain safe and be capable of acceptable performance in storage or in use. The advantages of this standard are that the Australian climate is addressed in more detail than MIL-HDBK-310, and the climatic criteria for Antarctica are also included. However, the disadvantage is that the standard is quite old, and relies heavily on MIL-STD-210B, which was the predecessor to MIL-STD-210C and MIL-HDBK-310.

APPLICATION AND TAILORING GUIDANCE

US Military Documents

6. **JSSG-2009 (*Air Vehicle Subsystems*), Appendix D *(Air Vehicle Environmental Control Subsystems Requirements and Guidance*).** JSSG-2009 is a modern document that provides excellent design guidance, requirements, and ‘lessons learnt’ through military and commercial standards. Appendix D of this document provides extensive coverage of ECS sub-systems.

7. **MIL-E-18927E(AS) *Environmental Control Systems, Aircraft, General Requirements for*.** MIL-E-18927E establishes the requirements for design and performance of ECS. It includes coverage of systems such as pressurisation, heating, cooling, ventilation, moisture control, bleed air system, ram air supply, pressure and anti-G suit systems, defogging, defrosting, anti-icing, rain removal and external air cooling connections. Despite referencing

MIL-STD-210C (cancelled and superseded by MIL-HDBK-310), MIL-E-18927E is still a current standard and has a lot of similarities with the more comprehensive JSSG-2009.

8. MIL-STD-2218 ***Thermal Design Analysis and Test Procedures for Airborne Electronic Equipment.*** MIL-STD-2218 provides very detailed guidance and formulas to calculate the heat dissipation of electronic equipment and the required ECS air flow rates required per kilowatt of dissipation. MIL-STD-2218 also provides test procedures in addition to those normally specified for environmental qualification of airborne electronic equipment. MIL-E-18927E and JSSG 2009 both refer to MIL-STD-2218 (or its predecessor) for thermal design and test procedures for airborne electronic equipment.

9. MIL-T-5842B ***Transparent Areas, Anti-icing, Defrosting and Defogging Systems, General Specification.*** This document establishes requirements for ECS sub-systems that keep transparent areas on aircraft vision surfaces clear. MIL-T-5842B references a number of other documents related to view and clear vision requirements, and is itself referenced by MIL-E-18927E.

FAR/JAR/SAE Documents

10. The FAR/JAR requirements focus more on design outcomes for an aircraft that is already certified with ECS design requirements adequately scoped. For example, FAR 33.66 states that the engine must supply bleed air without adverse effect on the engine, excluding reduced thrust or power output at all conditions established as a limitation under FAR 33.7(c)(11). FAR 25 provides guidance on pressurisation systems, but very limited guidance on conditioning systems. For an airborne platform that is intended to operate in a different role, configuration and environment than originally certified, or in a military specific role, the FAR/JAR design requirements are inadequate, and require supplementation.

11. The FAR/JAR requirements relating to ventilation, heating and pressurised cabins are written to meet the requirements of passenger and cargo areas, but do not address avionic equipment ECS requirements directly. In addition, the FAR/JAR requirements list ‘design outcomes’, but do not provide direct design advice for the modification or construction of ECS systems.

12. SAE ARP/AIR documents capture many of the lessons learnt by the aerospace industry in the design of ECS, and are non-US Government standards used to meet FAR/JAR requirements. Human physiological requirements are comprehensively addressed by SAE ARP 1270, although the ADF COE (AVMED) should be contacted in the first instance. SAE ARP 1168/7 (Aerospace Pressurisation System Design) provides a reference source for applied thermodynamic procedures and equations for the aerospace industry and may be of assistance when dealing with FAR/JAR requirements.

13. For military derivatives of civilian aircraft, the following areas should be addressed for the design/modification of ECS systems*:*

a. ***Anti-G suits.*** Anti-G suit pressure systems, if required, shall meet the requirements of MIL-D-7890A.

b. ***Air supply and test connections***. Air supply and testing connections shall comply with ASIC AIR STD 25/15C. This standard details requirements for air-conditioning connections, cabin pressurising connections, canopy seal inflation connections and test pressure gauge connections.

NEW PLATFORM ACQUISITIONS

14. For all new platform acquisitions, adequate ECS margins should be stipulated for the generation of ECS air/liquids. As a minimum, the cooling provisions for electronic equipment should provide for an electronic heat dissipation load 25% greater than the equipment heat load of the first production aircraft. Sufficient structural clearance in the aircraft should be provided to allow the fitment of a 25% larger capacity ECS system, thus providing 50% greater load capacity than that required by the first production aircraft. U.S. experience (refer JSSG 2009) shows a 25% growth capacity from production is not necessarily enough to cover all future changes in avionics, especially on fighter, bomber and electronically intensive platforms. In addition, an appropriate leakage rate shall be applied to the system as defined in either JSSG 2009 or MIL-E-18927E. These requirements are drawn from MIL-E-18927E paragraph 3.2.7 and referenced in JSSG 2009 Appendix D.

15. Consideration should also be given to any alternate roles that the platform will perform that may effect ECS requirements. For example, secondary roles could include Aeromedical evacuation, paratrooper dispatch, troop

carrying and transport of dangerous cargo. In each case, the impact on the ECS will need to be comprehensively scoped.

MODIFICATION OF EXISTING PLATFORMS

16. Modifications to existing platforms may impact ECS requirements. Consideration should be given to the ECS 'generation' function, as well as the requirements of the dependent functions to ensure all integration issues are considered. In conjunction with the advice provided for new acquisitions, the following areas should also be considered:

a. an evaluation of existing ECS capabilities, design limitations, previous test qualifications and design standards should be carried out prior to modification. ECS capacity may either decrease or increase as a result of a modification and is dependent on the heat dissipation characteristics of the equipment removed, replaced or added. The lack of sufficient cooling air for additional heat dissipation may result in heat related faults or shortened MTBF for equipment. Conversely, as some modifications remove equipment (or replace it with more efficient equipment), the ECS flow rate and temperature may change, and could lead to 'freezing' of components. The 'freezing' in some cases may not induce faults, however upon defrosting, condensation may form on circuit cards causing moisture induced faults;

b. consideration should be given to any role, configuration or environmental changes, 'fitted for but not with' issues, possible links to other dependent systems, humidity requirements, and min/max temperature fluctuations. This will ensure that any previous ECS design assumptions are not invalidated;

c. as ECS systems are designed as a 'system' that provides cooling air to all applicable equipment in a platform, changing the flow rates in one section of the ECS system for new/removed equipment may have repercussions on flow rates in other parts of the system. This may lead to overheating of other equipment not involved in the modification;

d. consideration should be given to the different configurations of ECS that exist within any given fleet (eg. single/dual seat aircraft). Tailored design packages (eg. modifications/STIs etc) may be needed to compensate for such differences; and

e. ECS capacity pre- and post-modification should be closely monitored, as using all spare capacity early in the life-of-type does not allow for further expansion without significant changes to the ECS system. Where possible, the impact of the proposed modifications should be scoped before platform upgrades are considered. Therefore, as part of a pre-modification feasibility study of the system, the PO/SPO should ensure that sufficient growth is available to last through to the planned withdrawal date of the platform.

MANAGEMENT OF ECS SYSTEM CAPACITY

ECS Operating Modes Document (ECSOMD)

17. ECS air for airborne platforms is a resource, and as such should be managed similarly to other platform resources such as electrical loads and weight and balance. As part of the feasibility stage of a project where integration or modification to an ECS is required, the Commonwealth should either gather the equivalent information of an ECSOMD, or be the recipient of such a document. The ECSOMD simply summarises all the utilised and/or spare ECS resources pre- and post-modification/acquisition in all possible roles and configurations of the platform. An ECSOMD should include, but not be limited to all possible modes of operation of the parent platform including:

a. ground operations,

b. taxi, take-off and landing,

c. all flight attitudes within structural limitations,

d. zero gravity or negative gravity,

e. all altitudes within the flight envelope,

f. structural deflection,

g. integration with other systems as applicable (eg. oxygen system),

h. loss of engine propulsive power, and

i. emergency operation.

18. An assessment of the ECSOMD should enable the PO/SPO to determine whether closer management of the ECS system is required throughout the project. Further rigour may need to be applied to managing ECS issues during the acquisition or modification if the ECS:

a. has an uncertain or undefined spare and/or utilised capacity,

b. may impose limitations on aircraft operations, or

c. will be nearing capacity in the immediate future through concurrent or future defined modifications.

19. One method of applying this additional oversight is through the use an ECS Analysis and Integration Plan (ECSAIP). Where an ECSAIP is to be used to manage ECS capacity, this should be reflected in the contract requirements.

ECS Analysis and Integration Plan (ECSAIP)

20. An ECSAIP should be drafted by the contractor, and subsequently reviewed and approved by the Commonwealth for all aircraft modifications with the potential to significantly impact ECS capabilities. This document should not only demonstrate that the contractor has sufficiently scoped the possible ECS requirements, but should culminate in a mature document to be utilised throughout the project to manage all pertinent ECS issues. Annex A contains guidance for the development of an ECSAIP.

RELATED INFORMATION

21. For additional information relating to ECS integration issues, refer to Section 2 Chapter 3, General Avionics Equipment and Section 4 Chapter 1, Propulsion Systems.

Annex:

A. Environmental Control System Analysis and Integration Plan (ECSAIP) Requirements

ENVIRONMENTAL CONTROL SYSTEM ANALYSIS AND INTEGRATION PLAN (ECSAIP) REQUIREMENTS

DESCRIPTION AND INTENDED USE

Purpose

1. The Environmental Control System Analysis and Integration Plan (ECSAIP), or an equivalent document produced by the applicable Contractor, should describe the design philosophies and technical approach to be used by the Contractor to manage ECS capabilities. The Commonwealth will use this plan to evaluate the Contractor's ECS design, production, integration and verification approach to ensure the proposed design and installation will meet the contractual ECS requirements.

Application

2. An ECSAIP should be drafted by the contractor, and subsequently reviewed and approved by the Commonwealth for all aircraft modifications with the potential to significantly impact ECS requirements. An ECSAIP may also be required for minor modifications if the ECS system is critically nearing capacity, or expected to exceed capacity before the aircraft's planned withdrawl date. This submitted document should not only demonstrate that the Contractor has sufficiently scoped the possible ECS requirements, but should culminate in a mature document to be utilised throughout the project to manage all pertinent ECS issues.

CONTENT REQUIREMENTS

3. The following guidelines are designed to assist Contractors in addressing the key areas of an ECSAIP. The structure shown is not mandatory; however, the document should employ a structure that clearly and logically presents information required by the PO/SPO. For the purpose of clarity, the generic requirements of a deliverable document to the Commonwealth (eg. referenced documents, acronyms and abbreviations) are not shown, but should be clearly defined to the Contractor by the PO/SPO.

ECS Design

4. ***Design Concept.*** The ECSAIP should describe the overall ECS design concept, including all mechanical, electrical and software design considerations applicable and should naturally flow on from the completed ECSOMD. This design concept should also detail the design criteria of the proposed system using the tailored advice for the platform from the Commonwealth, and the advice offered in this manual. Additionally, this section should include an appraisal of the identified risks, future capability post-modification (ie. what spare capacity will the ECS system have for future modifications) and any potential vulnerabilities applicable to the platform.

5. ***Design Detail.*** The detailed design of the system should use the 'design concept' as a starting point and establish how the Contractor expects to meet the established criteria. Sufficient information should be included that the Commonwealth is able to appraise the proposed system and verify whether it is appropriate for the needs of the ADF. It should also detail any design assumptions, limitations, future scope expansion and how the contractor intends to meet the requirements of spare capacity and physical growth of the system if ever required.

6. Concurrently, the Contractor should ensure that as a minimum (where applicable), the following headings are addressed in the ECSAIP, especially if tailoring of civilian and/or military standards is required. The headings are as follows:

a. construction (eg. ducting pipes etc.);

b. post production/leakage;

c. backup systems;

d. pressurisation/pressurisation control valves/pressure drops;

e. occupied/unoccupied compartments, bays and equipment pressure schedules;

f. cooling/heating;

g. temperature control;

h. temperature-altitude-humidity requirements;

i. coolants (other than pressurised/condition air requirements if applicable);

j. ECS crew station interface;

k. emergency ventilation and smoke removal;

l. avionic equipment and compartment emergency cooling;

m. suit ventilation and pressurisation;

n. cargo and other compartment ventilation;

o. contamination;

p. dust/moisture/fog/frost/rain/ice protection and removal;

q. bleed air source shut-off;

r. overbleed protection;

s. bleed air distribution control;

t. isolation and crossover control;

u. reverse flow protection;

v. bleed air pressure/air temperature control/regulation;

w. bleed air leak detection/ air pressure relief;

x. uncontrolled bleed air/bleed air ducts;

y. thermal protection;

z. structural integrity;

aa. burst/proof pressure;

bb. rotating equipment structural integrity;

cc. NATO ground/air compatibility/duct couplings;

dd. hot surface temperatures;

ee. future growth/expansion;

ff. bearings/fans;

gg. air cycle machines;

hh. pneumatic actuated components;

ii. ram air/heat/liquid to heat/liquid to liquid exchangers;

jj. water boilers;

kk. liquid cooling/vapour cycle loops; and

ll. component performance data.

7. ***Design Validation.*** The Contractor should detail to the PO/SPO (through the use of analysis and/or system 'mock-up' test results) how the ECS design will be validated to meet the requirements of the Commonwealth prior to endorsement of the final design.

8. ***Related Design Factors.*** Factors not commonly associated with ECS design and integration should also be scoped. Impact of EMI/EMC is one example: ECS entrance points and ducting can act as a 'waveguide' for electromagnetic signals that may either disrupt the ECS system itself, or the equipment the ECS will deliver cooling air to. Other examples include software changes, role and configuration changes and moisture ingress from cooling air. Each should also be scoped to ensure that there is no or minimal impact.

9. ***Physiological Factors.*** Physiological factors are not considered in this chapter. Further information may be sourced directly from the ADF COE, AVMED.

Verification Requirements

10. Upon completion of the prototype platform, the Contractor should provide the Commonwealth with test results to show compliance against the previously endorsed design, and recommendations (if applicable) to rectify any shortfalls. Prior to the commencement of such tests, the Contractor should draft test procedures that are subsequently reviewed and approved to the satisfaction of the PO/SPO. Not only will this enhance any associated compliance finding activities, but it will also ensure that tests conducted on the platform realistically represent the intended role and configuration of the platform once accepted into service.

11. As such, the ECSAIP should provide the Commonwealth with all possible detail relating to the proposed verification activities. This will assist in formalising the expected verification activities between the Commonwealth and the Contractor at an early stage, peculiar to the project requirements.

Blank Page

SECTION 3

CHAPTER 1

ROTORCRAFT

INTRODUCTION

1. The airworthiness certification requirements and processes for rotorcraft are similar to those of fixed wing aircraft. However, there are unique aspects to the design and operation of rotorcraft, which require separate treatment during the airworthiness certification process.

2. Like fixed-wing aircraft, military rotorcraft are designed to a variety of design standards and specifications, the selection of which relies on the manufacturer and procurement authority at the time. This chapter provides a list of the more commonly used rotorcraft design standards and captures some of the 'lessons learnt' on the tailoring of appropriate design standards for ADF rotorcraft operations. It provides *rotorcraft* specific guidance on the airworthiness certification process, *additional* to that contained in sections 1 and 2 of this manual, and should not be read in isolation.

DESIGN SPECIFICATIONS AND STANDARDS

3. Rotorcraft are designed and certified to various standards, including both military and civil, which provide for an acceptable level of safety. Annex A provides a list of specifications and standards relevant to rotorcraft. Whilst this list provides the more commonly used and internationally accepted specifications and standards, it is not exhaustive, and other relevant specifications may be employed.

4. The manufacturer usually specifies the standards to which a rotorcraft or modification is designed, built and certified. The manufacturer may group these into a unique specification, which references military/civil specifications and standards. The ADF should ensure that the standards applied by the manufacturer are adequate for the intended Configuration, Role and Environment (CRE) of the rotorcraft, and tailor the standards to suit any unique requirements.

APPLICATION AND TAILORING GUIDANCE

5. Dynamic Components Fatigue Lives. For rotorcraft, an assessment of fatigue for dynamic components requires increased consideration due to the complexity of the analysis, and the non-redundant load paths in the Main Rotor and drive train assemblies. For safe-lived components, fatigue lives should be based on a thorough testing program and formalised fatigue calculation methodology. There is no standard fatigue calculation methodology with each OEM having developed their own methodologies over time based on established assumptions and experience.

6. Rotorcraft OEMs generally develop fatigue lives for dynamic components based on a Design Usage Spectrum (DUS) which is established early in the development program, with the expected operations in mind. Although it may differ from expected ADF operations at time of acquisition, diverting from the established OEM DUS may lead to further complications for the ADF and is generally not recommended. Once the aircraft is in ADF service, then a dedicated usage monitoring program is able to identify whether ADF operations are conservative with respect to the original DUS assumptions. Subsequently, this provides confidence that the corresponding fatigue lives are conservative for ADF operations.

7. Ship-borne Considerations. The operation of helicopters at sea requires unique engineering considerations. For new aircraft acquisitions where the aircraft is expected to operate at sea, or where existing land-based aircraft undergo role changes where they will be expected to operate at sea, the following factors as a minimum should be considered:

a. ***Undercarriage.*** In general terms, maritime helicopters require significantly higher design landing sink speeds than those of land-based helicopters. Therefore, the undercarriage requires an assessment of suitability for the intended embarked operations. The design landing sink speed and the compatibility with ship deck motion on the expected operating platform is difficult to quantify, and often requires extensive flight trials to validate. These limitations are often critical for the subsequent development of the Ship Helicopter Operating Limits (SHOL). For example: the S-70B-2 Seahawk design landing sink speed was designed to 12 ft/s to allow embarked naval operations, whereas the S-70A-9 Black Hawk was designed to 10 ft/s for land based operations.

b. ***Tie-down points for securing and stowage***. For embarked operations, the ground handling loads are often quite different and considerably higher in magnitude than land-based ground handling loads due to the dynamic nature of ship deck motion. An assessment of the suitability of the tie-down configuration, and the static strength of each tie-down point is recommended for the intended embarked operations. This is especially important for aircraft not originally intended for embarked operations.

c. ***Mechanical securing systems***. It is often necessary to employ unique securing systems for embarked operations due to large ship motions. Systems such as the Recover And Safely Traverse (RAST) impart large securing loads on the airframe supporting structure, that should be considered as part of the helicopter design. In addition to this, these systems often impart additional landing loads during the landing case (due to haul down tension) that requires an assessment of the undercarriage and associated backup structure.

d. ***Corrosion Prevention and Control Program (CPCP)***. Due to the severity of the corrosive environment during embarked operations, it is often prudent to place increased rigour into the development of the CPCP. This is increasingly important for aircraft not originally intended for embarked operations.

e. ***Fatigue***. For embarked operations, the loads imparted on the airframe due to ship motion whilst the aircraft is secured to the deck, are usually significantly less than those experienced in flight. Whilst fatigue in this condition is not usually a consideration for either the structure or dynamic components, the landing gear and tie down points should be considered and undergo some form of analysis. Fatigue conditions should also be assessed if the aircraft is to be transported by ship.

8. Counter Measure Dispensing System (CMDS) Loads. The static loads reacted by the airframe during CMDS firing are often quite significant. As modern CMDS fires counter measures at millisecond intervals, the system peak firing load often exceeds that of an individual firing load due to the super-position of loads over a small time period. It is important that these loads are identified early within the project, and identified as the design limit load for the subsequent structural design. Under-estimation of these loads could result in costly redevelopment work later within the project, or limitations on the CMDS capability.

9. Restraint of Mobile Crew. Crew members whose duties require them to stand near an open door in flight are referred to as ‘mobile crew’ eg. loadmaster or aircrewman. Mobile crew can be restrained from falling from an aircraft by a harness or belt connected by a ‘restraint strap’ to an ‘attachment point’ on the aircraft.

10. The ADF’s preferred standard for the ‘mobile crewman’ is DEF STAN 00-970. Chapter 104 paragraph 8.2 requires a body harness providing vertical head up overhead suspension and adequate restraint for both pelvis and thorax. Chapter 714 paragraph 3.8 requires the attachment point to have an ultimate factor of not less than 1.0, on a force of 10,000N (2500lbs) acting in any direction within a cone of 60^{o} included angle having its apex at the attachment point and its axis parallel to the vertical datum of the aircraft.

11. ***Restraint Strap.*** Restraint straps which comply with ATSO-C1001 ‘Dispatcher Restraint Strap’ (which refers to AS/NZS 1891.1:1995 are suitable for the restraint of mobile crew.

12. ***Attachment Point.*** FARs 27/29.865 (read in conjunction with AC27-1B and AC29-2C) is a design standard which applies to the carriage of external loads, *including human cargo.* The standard requires attachment points *for external human cargo* to withstand a limit static load equal to 3.5g multiplied by the maximum external load for which authorisation is requested. A static limit load less than 3.5g (but greater than 2.5g) may be applied for a restricted flight envelope. The load must be applied in the vertical direction and must also be substantiated in any direction making an angle of 30^{o} with the vertical. A lesser angle may be applied if operating limits are established, or the lesser angle cannot be exceeded in service. Safety (1.5) and fitting (1.33) factors from FAR 27/29.303 and FARs 27/29.625 would also apply.

13. The design loads in FARs 27/29.865 for the carriage of external human cargo are suitable for attachment points designed *to prevent a wearer from falling out of a rotorcraft.* These design loads provide an equivalent level of safety for mobile crewmen to that accepted by the FAA for persons carried external to rotorcraft, and similar design standard for the Seahawk. This is provided that the restraint strap restricts the wearer to the door threshold of the aircraft (and no further), and that there is a minimum of slack in the restraint strap at all times.

14. IMC Requirements. Design requirements for IMC operations are not specified in any military rotorcraft design standard. Civil aircraft are not typically certified for IMC operations, rather they are certified for Instrument

Flight Rules (IFR). If an aircraft is certified for IFR, then flight in IMC is permitted. A relevant design standard for helicopter IFR operations is FAR 27/29 Appendix B, read in conjunction with FAA AC27/29 Appendix B.

15. Where aircraft do not comply with this design standard, the following factors (not comprehensive) might be considered in an operational risk assessment for flight in IMC:

a. Suitability of the flight critical instruments, taking into account their accuracy, reliability and redundancy;

b. Aircraft handling characteristics and pilot workload;

c. Adequacy of the flight manual in specifying limitations, performance and procedures; and

d. Appropriate operational procedures and training to mitigate potential hazards.

16. **Crashworthiness**. In general, military and civilian airworthiness design standards adopt a systems approach towards rotorcraft crashworthiness design, with 6 basic design principles being adopted. These are:

a. Energy absorption, to limit the energy transferred to passengers and crew, during the rotorcraft crash. This is achieved in various ways, predominantly through the use of energy absorbent undercarriage, airframe, and seating.

b. Restraint of mass items, to prevent parts of the rotorcraft becoming projectiles within the cabin during a crash (eg engines/transmission/blades coming through the roof, internally mounted items dislodging etc.)

c. Preservation of cabin volume, so that passengers and crew are not crushed during a crash.

d. Maintaining ability for passengers/crew to escape, by ensuring doors/hatches can be opened even after significant cabin deformation.

e. Prevention of fire, and reduction of toxic emissions; and

f. Safe restraint of crew, by:

(1) Ensuring the seat remains attached to the aircraft during the crash,

(2) using a suitable harness which keeps the body upright, and

(3) designing to reduce the hazards associated with the flailing of the head and limbs.

17. Application of each of these principles increases crew survivability. The TAR accepts legacy certification standards of in-service ADF aircraft, without requiring modifications to meet current crashworthiness design requirements. The OAA may also use operational risk management principles for operations where compliance with appropriate crashworthiness standards cannot be achieved with current aircraft configurations.

Annex:

A. Standards and Specifications

Blank Page

STANDARDS AND SPECIFICATIONS

Standard or Specification	Title
AC 20-95	Fatigue Evaluation of Rotorcraft Structure
ADS-11	Rotary Wing Survivability Program
ADS-24	Crashworthy Design Principles
ADS-36	Rotary Wing Aircraft Crash Resistance
DEF STAN 00-970	Design and Airworthiness Requirements for Service Aircraft: Volume 2 - Rotorcraft
FAR Part 27	Airworthiness Standards: Normal Category Rotorcraft
FAR Part 29	Airworthiness Standards: Transport Category Rotorcraft
MIL-D-2322A (AS)	Demonstration Requirements for Helicopters
MIL-R-85510	General Specification for Crashworthy Seats and Helicopter Cabin
MIL-S-8698 (ASG)	Helicopter Structural Design Requirements
MIL-S-58095	General Specification for Crash Resistant Non Ejection Aircrew Seat System
MIL-STD-250D	Aircrew Station Controls and Displays for Rotary Wing Aircraft
MIL-STD-1290A (AV)	Light Fixed and Rotary Wing Aircraft Crash Resistance
MIL-STD-1807	Crash Survivability of Aircraft Personnel
MIL-T-81259B (AS)	Requirements for Airframe Design - Tie Downs
SAE-AS-8049	Performance Standard for Seats in Civil Rotorcraft and Transport Airplanes

Blank Page

SECTION 4

CHAPTER 1

PROPULSION SYSTEMS

INTRODUCTION

1. This chapter provides guidance on the application of design standards for use in ADF design, certification and in service management activities. ADF design requirements for aircraft propulsion systems are provided where specific, additional requirements exist. Prevalent civil and military design standards are listed and explained.

2. This chapter also continues to provide useful information for Project Office (PO) staff involved in the acquisition of, or modification to, ADF propulsion systems. This information may also apply to Logistics Management Unit (LMU) staff involved in design changes to ADF propulsion systems, and Defence contractors. As a result, a background section is included to provide a context for propulsion system airworthiness design requirements. Finally, the Engine Structural Integrity Program (ESIP) philosophy is discussed and generic Detailed Services Description (DSD) and Data Item Description (DID) templates for services and documents required by contractors involved in Engine Structural Integrity (ESI) management are provided.

BACKGROUND

Propulsion System Design Standards

3. For reasons specified in Section 1, it is a practical requirement for the ADF to accept a range of design standards for aircraft type certification and continuing airworthiness. Since the ADF does not normally specify its own design standards, comparative standards are identified to evaluate engine design standards that form the certification basis for an engine under consideration. A comparative standard is an accessible and comprehensive airworthiness design standard with which another standard can be compared. It is not necessarily inherently safer or more complete than other standards, but provides an acceptable baseline standard for ADF applications. For aircraft structure and some systems, more than one comparative standard is specified (refer applicable chapter of Section 2, this publication). In the case of propulsion systems, only one system level comparative standard is identified. This reflects the maturity of engine design standards, which in general provide a good equivalent level of safety.

4. The ADF propulsion system comparative standard is DEF STAN 00-971. This standard may be obtained from the UK Defence Standardisation Organisation's website: www.dstan.mod.uk.

Design Requirements

5. The TAR's design requirements provide additional aspects for a design that are either not identified in the design standard (or comparative standard), or are not adequately defined in the design standard. A TAR design requirement exists to provide a discrete design deliverable considered highly desirable to the ADF. For example, "The engine shall operate, without restriction over the entire operating envelope, with JP8+100 fuel". The TAR's design requirements are to be considered in addition to the requirements contained within the engine design standard(s).

6. The TAR's design requirements for propulsion systems are listed in annex A.

7. Due to the large uniformity between propulsion system design standards, the TAR would not normally specify a propulsion standard in its entirety. Where a proposed standard were deficient in a particular area, evaluation against the comparative standard would identify this, and additional specific requirements would be applied on a case by case basis.

APPLICATION AND TAILORING GUIDANCE

Deficiencies in Design Standards

8. Section 1 Chapter 1 of this publication identifies why a particular design standard may not be adequate for ADF application[1]. Review of the propulsion system design standard against the comparative standard and any of the TAR's design requirements should identify where the design standard is deficient. The PO or SPO is strongly encouraged to consult with ESI1-DGTA during this process for efficiency and to ensure all irregularities are identified. Where the engine design standard is assessed as being deficient, requirements contained in the comparative standard and any additional TAR design requirements should be added to the offered standard. The certification basis then becomes an amalgamation of the primary design standard and the additional requirements.

9. For propulsion systems, the most common deficiency of a standard is that it may not be applicable to the ADF Configuration, Role and Environment (CRE). This situation may (for example) arise when engines designed to a civil standard are acquired by the ADF and the intended or actual usage differs from the civil role. Careful attention must be payed to the ADF CRE to ensure that engines designed for civil applications are capable of meeting military requirements, based on the aircraft Statement of Operating Intent (SOI). Specific military requirements should be addressed when developing the aircraft Certification Basis Description (CBD). Annex B contains guidance on common issues that may be identified as deficient when a civil certified propulsion system is intended for use in the ADF. The list is indicative only and does *not* form a list of additional design requirements.

Interfacing with the Airframe

10. For new aircraft acquisitions or major engine modifications/upgrades, it is important to recognise that certification requirements affecting the propulsion system exist in the parent aircraft standard (ie FAR Part 25, for civil transport category aircraft) in addition to the requirements of the corresponding engine design standard (ie FAR 33). Specific requirements may exist for both engines and propellers. The issue arises through necessity: the aircraft cannot be fully certified until married with a particular engine. For example, the effect of installation on engine performance is unknown during engine certification, but may impact overall thrust and efficiency. The engine may be installed on a number of different aircraft (for example, the Pratt and Whitney PT6 engine is fitted to numerous military and civil aircraft such as the Pilatus Turbo-Porter, Pilatus PC-9, DHC-6, Cessna Caravan, Beech King Air and several helicopters). This makes estimating some aircraft level certification requirements (such as installation effects) very difficult.

11. An excellent example to illustrate this issue is FAR Part 25.939, which states "Turbine engine operating characteristics must be investigated in flight to determine that no adverse characteristics … are present … during normal and emergency operation …". This requirement exists for obvious reasons and could not be a requirement of FAR Part 33. FAR Advisory Circular (AC) 25.939-1 provides a means of compliance for this requirement and highlights issues such as installation effects, engine location, aircraft configuration (flap settings, weight, etc) and aircraft service demands (bleed air and power extraction).

12. This issue is most relevant for engine upgrades. Potential impacts to the aircraft design standard must be identified where they may occur, including conflict with any of the TAR's aircraft level design requirements. Early PO consultation with ESI1-DGTA is recommended.

Using Advice from foreign National Airworthiness Authorities

13. In TAMM Regulation 2.2.7., the ADF recognises several National Airworthiness Authorities (NAA's), including civil authorities such as the US FAA, and various foreign military forces. ADF experience has shown that these organisations sometimes apply policies that do not comply with OEM recommendations. For propulsion systems, this issue normally arises with regard to critical part lifing policy and/or Usage Monitoring (UM) methodology. The success of both aspects is *crucial* for effective in-service engine airworthiness management. For propulsion systems, the technology involved in design is very highly specialised and knowledge associated with such technology is treated as extremely valuable Intellectual Property (IP) by OEM's. As a result, the OEM is usually the

[1] As per Section 1 Chapter 1, these are: differences in Configuration, Role and operating Environment (CRE), a deficiency in the level of safety provided by a standard, intentional ambiguity in a standard and/or the ADF's approach to Through Life Support (TLS).

most appropriate organisation to set life limits and UM methodologies[2]. The TAR preferred approach IAW TAMM Regulation 3.5.5. is to accept OEM critical part life limits and UM methods *whenever possible*.

14. The ADF should not follow the policies of foreign NAA's without appropriate evaluation. Such evaluation requires adequate disclosure of design information from the NAA to allow such a review to occur. Given the sensitivity of information, PO's must ensure the contractor is aware of this issue as early as possible in the acquisition process since obtaining such information may be a lengthy process. ESI1-DGTA must be involved in any evaluation of non-OEM life limits and UM methodology.

Design Requirements for Critical Parts: Life Limits and UM requirements

15. Engine standards are usually not prescriptive regarding the design of critical parts, and the life limits and UM methods employed for these parts. OEM's may apply different lifing methodologies and use their own materials databases. OEM's continually improve their corporate methodologies in order to progress the technology and maintain competitive advantage. A particular methodology will not normally be specified in a design standard, nor will an OEM present their methodology to the ADF in any other form. As a result, ESI1-DGTA must be involved with assessing the suitability of specified design standards (acceptability criteria and verification methods) for new engines. This would normally occur as part of the normal SOR and PDAS review IAW TAMM Regulation 2.2.3.

16. For in service engines, life limits and the UM methodology must remain relevant and thus continue to provide an acceptable level of safety, through the life of the aircraft. This is usually done with through life support from the OEM. In cases where this is not possible, significant effort will be required to evaluate the continuing acceptability of life limits and UM. ESI1-DGTA is to be involved in any such evaluation IAW TAMM Regulation 3.5.5.

The Purchase of Used Engines

17. When used engines are being considered for acquisition, recognition must be made that their previous operation and engine life management processes may not meet ADF requirements. Accordingly, particular care must be exercised in assessing their degree of conformity to ADF standards. The relevant PO must ensure that the following is completed before used gas turbine engines are operated under an Australian Military Type Certificate (AMTC):

a. Previous usage, maintenance, repair and modification records of each individual engine are obtained, examined and an assessment made of the acceptability of previous usage, maintenance, repair and modifications,

b. A physical configuration audit is performed on a sample of engines to confirm the accuracy of documentation and general suitability of the engines for service. Ideally, this would involve some level of teardown,

c. Where there is a concern or uncertainty with the reliability of previous lifing data, the remaining life on critical parts is factored appropriately, and

d. The ESIMP is used to document any corrective actions required to raise the standard of the engines to a level acceptable to the TAR.

18. It would be expected that ESI1-DGTA should be involved in this process.

Health and Usage Monitoring Systems

19. Modern aircraft such as the BAe Hawk are fitted with a Health and Usage Monitoring System (HUMS), which may be defined generally as a system combining the functions of UM and CM systems, and in some automated form. Older aircraft such as F/A-18 Hornet may still be fitted with automated UM systems. Automated systems introduce additional sophistication and complexity into the design. Furthermore, current engine (and aircraft) design standards, including the comparative standard, do not usually have rigorous requirements for automated UM or CM systems. As a result, certification of such systems can be difficult. For this reason, the TAR's design requirements at annex A include a requirement for any automated UM or CM system to be validated as part of the overall HUMS Validation Plan (HUMSVP).

[2] The OEM will usually be the most appropriate organisation since it should have superior/quality people, processes, data and training (in the Organisation, People, Processes, Data and Training model – "OPPDT"). This may not be true in every case and in exceptional circumstances, scope may exist for the ADF to deviate from OEM policy. ESI1-DGTA must be involved with any such deviation, IAW TAMM Regulation 3.5.5.

20. ESI1-DGTA should be consulted where the requirement to conduct a HUMSVP is not clear. Additional information on HUMS is contained in Section 2 Chapter 19 of this publication.

A Note on Design Handbooks and Guides

21. A design standard is by definition a *general* specification. A standard is mandatory in the sense that a particular certifying organisation mandates particular design standards for use within its area of influence (ie a UK standard is not mandatory in the US – though it is certainly recognised). Particularly in the US, an increasing number of standards are being converted to handbooks or guides (for example, MIL-STD-1783 is now MIL-HDBK-1783). For propulsion systems, where a handbook, guide, or element thereof, is specified in the certification basis, it shall be considered as a design standard for the purposes of certification.

COMMON PROPULSION SYSTEM DESIGN STANDARDS, HANDBOOKS AND GUIDES

22. Table 1–1 lists prevalent design standards, handbooks and guides for propulsion systems and includes the applicable National Airworthiness Authority (NAA) that sponsors the standard. A detailed explanation of these standards follows.

Table 1–1 Propulsion System Design Standards, Handbooks and Guides

Certification Code	Application	Sponsor
DEF STAN 00-971	UK Military Gas Turbine Engines	UK MoD
JAR-E JAR-P	European Civil Aircraft Engines European Civil Aircraft Propellers	JAA
CS-E CS-P	European Civil Aircraft Engines European Civil Aircraft Propellers	EASA
BCAR Section C	UK Civil Aircraft Engines and propellers	UK CAA
FAR Part 33 FAR Part 35	US Civil Aircraft Engines US Civil Aircraft Propellers	US FAA
MIL-E-5007E MIL-E-8593E	US Military Turbojet and Turbofan Engines US Military Turboshaft and Turboprop Engines	US DoD
JSSG-2007 JSSG-2009	US Military Turbine Engines US Military Propellers	US DoD
CASR Part 33 CASR Part 35	Australian Civil Aircraft Engines Australian Civil Aircraft Propellers	CASA
MIL-HDBK-1783B	USAF Engine Structural Integrity Program	US DoD

23. ***DEF STAN 00-971.*** DEFence STANdard 00-971 is a general specification for aircraft gas turbine engines. The standard details the general requirements for the performance, operating characteristics, design, reliability and maintainability of gas turbine aero engines and associated jet pipes for use in UK military aeroplanes and rotorcraft. It also includes the demonstrations, tests, reports and provision of other data required to be completed satisfactorily and accepted prior to prototype flight clearance and subsequent type approval of these engines by the UK Ministry of Defence (MoD) on behalf of the user Service(s). Where requirements are dependent on the particular operational role or design of the aircraft, guidelines are given on the detailed requirements to be included in the individual engine specification. DEF STAN 00-971 is the ADF comparative standard and can be downloaded from the UK Defence Standardisation Organisation's website: www.dstan.mod.uk. ESI1-DGTA holds a copy of DEF STAN 00-971.

24. ***JAR-E and JAR-P.*** Joint Aviation Requirements E (Engines) and P (Propellers) are general specifications detailing the minimum airworthiness requirements for civil European engines and propellers respectively. Section 1 of JAR-E and P contains the design requirements and Section 2 contains information on an Acceptable Means of Compliance (AMC), defined as Advisory Circular Joint (ACJ) material. JAR-E and P are published by the European Joint Aviation Authority (JAA), responsible for developing and implementing common safety regulatory standards and procedures for the civil aviation regulatory authorities of a number of member European States.

25. On 28th September 2003, the European Aviation Safety Agency (EASA) became responsible for the airworthiness and environmental certification of products, parts and appliances for the majority of the civil aircraft registered in the Member States of the European Union (EU). At the time of writing, the JAA continues to exist, but

only with a limited capacity: its authority being slowly transferred to EASA over a five-year period. JAR-E and P are not freely available on the internet but may be purchased through the JAA website: www.jaa.nl. ESI1-DGTA holds a copy of JAR-E, Sections 1 and 2.

26. ***CS-E and CS-P.*** Certification Specification E (Engines) and P (Propellers) are general specifications detailing the minimum airworthiness requirements for civil European engines and propellers respectively. CS's are published by EASA, the body superseding the JAA as discussed above. In a method similar to the JAR's, Book 1 of CS-E and P contains the design requirements and Book 2 contains AMC material. Book 1 of these standards may be found on EASA's website: www.easa.eu.int. ESI1-DGTA holds a copy of CS-E, Books 1 and 2.

27. ***BCAR Section C.*** British Civil Aviation Requirements Section C is a general specification detailing the minimum airworthiness requirements for UK civil engines and propellers. BCAR Section C is published by the British Civil Aviation Authority (CAA). Where EASA rules are not yet in place, the national requirements of Member States still apply. Due to the staged nature of the transition to EASA, CAA requirements continue to be applicable to all aircraft with UK certificates of airworthiness until these requirements are superseded by EASA requirements. BCAR's are not freely available on the internet. ESI1-DGTA holds a copy of BCAR Section C.

28. ***FAR Part 33 and Part 35.*** Federal Airworthiness Regulation Parts 33 and 35 are general specifications detailing the minimum airworthiness requirements for civil US engines and propellers respectively. AMC material is contained separately in Advisory Circulars (AC's). FAR Parts 33 and 35 are published by the US Federal Aviation Administration (FAA). FAR Parts 33 and 35 may be downloaded from the FAA's website: www.faa.gov. ESI1-DGTA holds a copy of FAR Parts 33 and 35.

29. ***MIL-E-5007E.*** MIL-E-5007E is a general military specification for turbojet and turbofan engines, applicable to the US Department of Defence (DoD). It establishes the performance, operating characteristics, design features, detailed interface configuration definitions and installation envelopes for turbojets and turbofans. It also establishes the demonstrations, tests, reports, inspection procedures and other data required for satisfactorily completion and acceptance prior to type approval of these engines. This standard supersedes MIL-E-5007D, and has itself been superseded by JSSG 2007 (discussed below). A copy of MIL-E-5007D may be downloaded from assist.daps.dla.mil. ESI1-DGTA holds a copy of MIL-E-5007D and E.

30. ***MIL-E-8593E.*** MIL-E-8593E is a general military specification for turboshaft and turboprop engines, applicable to the US DoD. It establishes identical requirements to those of MIL-E-5007E, but for turboshafts and turboprops. A copy of MIL-E-8593A may be downloaded from assist.daps.dla.mil. ESI1-DGTA holds a copy of MIL-E-8593C and E.

31. ***JSSG 2007A and JSSG 2009.*** Joint Services Specification Guides have been introduced by the US government to provide generic guidance for development of program unique specifications. JSSG's cannot be used in isolation since they require a large amount of performance and functional information to be specified by the PO. JSSG 2007A, for aircraft turbine engines, contains 3 parts. Part 1 is a template for developing the program unique performance specification. Part 2 is the appendix A handbook which provides the rationale, guidance, and lessons learned relative to each statement in Part 1. Part 3 is the appendix B handbook that provides rationale, guidance, and lessons learned to establish an engine model specification for the production phase of the engine program. JSSG 2007A refers to other engine specifications such as MIL-E-5007E and MIL-E-8593A.

32. JSSG 2009, for air vehicle subsystems, contains 2 parts. Part 1 is a template for developing the program unique performance specification. Part 2 is a handbook providing the rationale, guidance, and lessons learned relative to each statement in Part 1. JSSG 2009 refers to other subsystem specifications for program unique requirements.

33. Copies of JSSG 2007A and 2009 may be downloaded from assist.daps.dla.mil. ESI1-DGTA holds a copy of JSSG 2007A and 2009.

34. ***CASR Part 33 and Part 35.*** Civil Aviation Safety Regulation Parts 33 and 35 are general specifications detailing the minimum airworthiness requirements for Australian civil engines and propellers respectively. CASR Part 33 states that the airworthiness standards for an aircraft engine are the airworthiness standards in Part 33 of the FAR's (including AC material). CASR Part 35 makes a similar statement regarding FAR Part 35. CASR Parts 33 and 35 are published by the Australian Civil Aviation Safety Authority (CASA). A copy of CASR Parts 33 and 35 may be downloaded from the CASA's website www.casa.gov.au.

35. ***MIL-HDBK-1783B.*** MIL-HDBK-1783B defines the USAF developed damage tolerance ENgine Structural Integrity Program (ENSIP). ENSIP is an organised and disciplined approach to the structural design, analysis,

development, production and life management of gas turbines. To date only USAF engines have been designed and managed to ENSIP. The ENSIP Handbook is intended for use in conjunction with JSSG 2007. A copy of MIL-HDBK-1783B may be downloaded from assist.daps.dla.mil. DGTA holds a copy of the latest revision to MIL-HDBK-1783B (Change 2), and previous revisions.

ESIP PROJECT REQUIREMENTS GUIDANCE

36. To promote the continuing airworthiness of ADF aircraft engines, the ADF TAR has established the concept of an ESI management system for the in-service management of ESI for each ADF gas turbine engine. An ESI management system is required for every ADF gas turbine engine IAW TAMM Regulation 3.5.5. The associated guidance at TAMM Section 3 Chapter 17 details the requirements of the recommended (TAR preferred) form of ESI management system: the ESIP. IAW TAMM Regulation 3.5.5., all ESI management systems must be documented by an ESIMP.

ESIP Requirements for Weapon System Through Life Support Contracts

37. For in service AEO's, many requirements of an ESIP can be met with the assistance of ESI1-DGTA staff. For example, it is common for the ESI1-DGTA ESIP manager to draft the engine ESIMP on behalf of the AEO. When Through Life Support (TLS) contractors are (or are to be) engaged for the complete management and support of propulsion systems, certain elements of ESI management responsibility will be transferred from ESI1-DGTA to the contractor.

38. In such cases, ESI1-DGTA recommends that PO's seek the TAR preferred ESI management system - the ESIP - as a contract deliverable, as detailed in TAMM Section 3 Chapter 17. Several documents have been designed in order to assist the PO achieve a satisfactory outcome regarding a propulsion system ESIP (and by implication, assist the contractor to understand and meet ADF regulatory requirements). These documents are listed below.

39. ***Engineering Support Services DSD.*** Annex C is provided to assist PO's develop an Engineering Support services contract DSD. The scope of the DSD shall encompass all ESIP management tasks identified as the responsibility of the contractor. Combined with the regulations covering any remaining ESIP tasks to be retained by the Commonwealth, this DSD will ensure that the subject engine is able to operate safely in accordance with the SOI, through life. The DSD also specifies DID's which fall subordinate to it, as detailed below. The PO may wish to combine the requirements of the ESI and ASI DSD's (refer Section 2 Chapter 11) into one aircraft level DSD, for contractors with responsibility for both ASIP and ESIP management. Tailoring of the DSD may be required for specific projects, to ensure appropriate requirements are identified (for example, the requirements identified regarding CAMM2 may not be applicable).

40. ***ESIR DID.*** Annex D is provided to assist PO's develop an Engine Structural Integrity Report (ESIR) tender DID. The ESIR is required during the tendering phase of a project to provide the Commonwealth with confidence in the ability of the tenderer to address ESI management issues and is a precursor to the ESIMP Contract deliverable. ESI1-DGTA should authorise any ESIR prior to its inclusion in the TLS contract.

41. ***ESIMP DID.*** For new acquisition aircraft the ESIMP should be developed and agreed to by the Contractor and the Commonwealth during acquisition. Since the negotiating leverage of the ADF reduces after contract signature, the contract must specify clearly the requirements of the ESIMP, including Condition Monitoring (CM) requirements[3]. ESI1-DGTA must authorise all ESIMP's prior to their inclusion as a deliverable in the TLS contract. PO's should note that IAW TAMM Regulation 3.5.5., all new ESIMP's and *all subsequent amendments* are to be approved by ESI1-DGTA. Annex E is provided to assist PO's develop an ESIMP contract DID. ESI1-DGTA must be involved in all reviews of contractor draft ESIMP's since the annex E template is generic and cannot cater for the exact requirements of any specific engine ESIMP.

42. ***ESIDP DID.*** To accept the engine type into service, sufficient data is required from the engine OEM to establish compliance with the engine certification basis. In some previous ADF aircraft acquisitions, the lack of a direct relationship between the Commonwealth and the engine OEM meant that access to such data was difficult. The PO must also ensure that sufficiently robust contractual arrangements exist to allow the Commonwealth access to data necessary to support certification and continuing airworthiness. Annex F is provided to assist PO's develop an Engine Structural Integrity Data Package (ESIDP) contract DID. The ESIDP is required for the Commonwealth to gain access to the ESI data necessary to support initial certification and continued airworthiness activities.

[3] The ESIMP includes all information relating to CM which previously appeared in a separate CM Program Plan (CMPP). For further details, refer TAMM Section 3 Chapter 17.

43. ***HUMSVP DID.*** All automated UM or CM systems are to be validated as part of the overall HUMSVP, IAW annex A. A generic HUMSVP contract DID is provided in Section 2 Chapter 19 of this publication to assist PO's meet this requirement. ESI1-DGTA should be involved with all HUMSVP's developed by PO's.

Cases where documentation may not be required

44. ***State owned aircraft operated and maintained in a Civil Role***. The ADF owns a small number of state registered aircraft, which are operated and maintained under civil regulations. For these aircraft (such as the BBJ fitted with the CFM56 engine), there is no requirement for an ADF ESIP and associated ESIMP, providing that the civil equivalent ensures an equivalent level of safety. ESI1-DGTA should be involved in this determination. This situation is acceptable where a state aircraft is essentially identical to its civil certified equivalent (ie ADF BBJ to civil BBJ), and it is being operated in a role very similar to its civilian equivalent.

45. For engines with prior civil certification and operated in a civil role, there is still a requirement for the PO to acquire a statement that the System of Maintenance (SoM) developed for the engine is appropriate for the intended role of the aircraft. If the parent aircraft SOI is modified by the ADF, then the contractor must review the amended SOI and ensure that changes do not affect the limitations and schedules in the SoM or any agreements with the engine OEM.

46. ***Missiles and other specialist gas turbine engines.*** ESIMP's are not required for missiles fitted with air breathing gas turbine engines (ie Harpoon). Given their role as "single use" items, coupled with the fact that their engines are small and the asset is relatively inexpensive, a missile ESIMP will not normally be required. Maintenance via technical publications should normally be expected to maintain ESI. Finally, MB-326 Macchi aircraft used for technician training at RAAF Base Wagga do not require an ESIMP given there role requiring a very low level of engine usage, similar to that of an APU.

47. ***Auxiliary Power Units.*** Although APU's may have critical parts, APU Structural Integrity Management Plans are not required. This is acceptable since APU's are mostly operated for short periods of time on the ground and are less susceptible to variations in aircraft mission profiles and mission mixes in comparison to propulsion systems. Notwithstanding, APU component lives must be identified in the applicable TMP and APU hardware is to be managed with a maintenance program satisfying the requirements of the TAMM. Should the PO or ESI1-DGTA be concerned with the management of a new or in-service APU, APU structural integrity may become an issue for the corresponding engine ESIP (and thus be documented via the engine's ESIMP).

48. ***Piston engines.*** ESIMP's are also not required for piston engines (such as those used in the DHC Caribou aircraft). This is acceptable since there are normally no critical parts to these engines and fewer ESI issues to be dealt with. As a result, ESI may be managed via technical publications without the need for further documentation. Again, where specific issues exist or are identified (for example, a requirement for a large amount of CM), then an ESIMP may be required. ESI1-DGTA should be consulted in such cases.

49. In all cases, it is important to recognise that an ESI management system still exists. However, the system is simply the set of Instructions for Continuing Airworthiness (ICA) and given its standard form, the system does not require an ESIMP.

Component Improvement Programs

50. Engine operators are normally invited to participate in a Component Improvement Program (CIP), or an alternatively named equivalent (eg International Engine Management Program). Such a program is normally managed by the engine OEM or a prime customer (eg USAF or USN). CIP's provide a means of coordinating engineering efforts to continue the improvement of engine reliability, durability and maintainability, as well as addressing service revealed problems that might lead to repair schemes, modifications or lifing changes. Another advantage of participation is that it provides a unique opportunity for customers to influence the manufacturer, such as through life extension of critical parts or improvements in CM. As a result, ADF participation in CIP's is strongly encouraged by ESI1-DGTA. Historically, involvement in such programs is very cost effective. The PO should consult ESI1-DGTA if a new acquisition engine is not to be supported by a CIP.

Usage Reviews

51. Differences between the engine OEM's design assumptions and the ADF actual usage are unavoidable. The engine OEM should be provided with a copy of the aircraft SOI and then perform a review of aircraft operations (mission types, mission mixes and ambient temperature variations) during the first two years following service

introduction, as this is when the actual usage is being explored and defined. Care should be taken in cases where the first two years usage is not representative of the SOI, or predicted future usage, of the engine. For many aircraft types (particularly specialist military aircraft), role and operating environment can have a significant effect on actual engine fatigue life usage. The engine OEM should be made aware of any variations to the SOI to ensure that the propulsion system certification basis and the life limits for critical parts remain valid for the aircraft life of type (LOT).

52. If the usage monitoring system is not of sufficiently high fidelity, it may also be necessary for mission reviews to be undertaken periodically throughout the LOT. ESI1-DGTA recommends a usage review once every 5 years as a general rule.

53. PO's should ensure these aspects are considered in any acquisition contract, as significant costs may be involved.

Lessons Learnt

54. The ADF has experienced some interesting and difficult propulsion system issues in certification and through life support. Annex G contains details of these valuable lessons learnt. Further information for each case can be obtained through ESI1-DGTA.

RELATED INFORMATION

55. The following references provide additional information related to this chapter:

a. AAP 7001.053 TAMM Regulation 2 ,

b. AAP 7001.053 TAMM Regulation 3,

c. AAP 7001.053 TAMM Section 3, Chapter 7 (Design Acceptance),

d. AAP 7001.053 TAMM Section 3, Chapter 12 (Project Design Acceptance – DGTA's Expectations),

e. AAP 7001.053 TAMM Section 3, Chapter 17 (Engine Structural Integrity Management),

f. AAP 7001.054 ADRM Section 1, Chapter 1 (The Application of Design requirements), and

g. AAP 7001.054 ADRM Section 2, Chapter 19 (Health and Usage Monitoring Systems).

Annexes:

A. Propulsion System Design Requirements

B. Common issues Regarding Civil Certified Propulsion Systems Intended for use in the ADF

C. Example of a Contract Detailed Services Description – Engineering Support Services – ESI Aspects

D. Example of a Tender Data Item Description – Engine Structural Integrity Report

E. Example of a Contract Data Item Description – Engine Structural Integrity Management Plan

F. Example of a Contract Data Item Description – Engine Structural Integrity Document Package

G. Lessons Learnt

PROPULSION SYSTEM DESIGN REQUIREMENTS

For Certification of all ADF Gas Turbine Engines

1. The aircraft shall, without restriction and over the entire operating envelope defined in the specification:

a. automatically restart, in a controlled manner, any engine that has experienced a flame-out condition; or

b. automatically detect and alert the flight crew to the presence of a flame-out condition in any engine.

2. The engine shall operate with JP8+100 fuel, without restriction and over the entire operating envelope defined in the specification.

3. Where an automated Health and/or Usage Monitoring (UM) system is employed in the engine design, a HUMS Validation Plan (HUMS VP) shall be required. Validation shall occur as part of overall HUMS validation IAW AAP 7001.054 Section 3 Chapter 19.

For Certification of Engines which are to Employ Non-OEM Life Limits and/or UM Methodology

4. The ADF shall acquire adequate design disclosure to allow review of the acceptability of critical part life limits and UM methodology.

For Certification of Used Engines

5. Previous usage, maintenance, repair and modification records for each engine shall be obtained to allow an assessment of the acceptability of previous usage, maintenance, repair and modifications for ADF service.

Blank Page

COMMON ISSUES REGARDING CIVIL CERTIFIED PROPULSION SYSTEMS INTENDED FOR USE IN THE ADF

Gas Turbine Engines

1. The aircraft engine shall be capable of continuous operation, free from stall, surge or handling restrictions, particularly in relation to throttle operations, in any part of the operating envelope defined in the Specification.

2. The aircraft engine shall be capable of complying with all of the requirements of the Specification when using the fuel types specified by the Project Authority.

3. The aircraft shall, without restriction and over the entire operating envelope defined in the specification:

a. automatically restart, in a controlled manner, any engine that has experienced a flame-out condition; or

b. automatically detect and alert the flight crew to the presence of a flame-out condition in any engine.

4. Depending on the configuration, role and environment in which the aircraft and engine is to be operated, consideration should be given to inclusion of the additional requirements derived from DEF STAN 00-971, Part 2 and the draft DEF STAN 00-970 Section 4. A summary list of requirements is provided below:

a. Sand Ingestion;

b. Vectored Thrust;

c. Reheat Lighting and Burning;

d. Infra-Red Radiation/Suppression;

e. Nuclear Weapons Effects;

f. Armament Gas Ingestion;

g. Steam Ingestion;

h. Reduction of Vulnerability to Battle Damage;

i. Exhaust Smoke Emission;

j. Electro-Magnetic Compatibility;

k. Corrosion;

l. Prototype Flight Clearance; and

m. Accelerated Mission Endurance Test.

Propellers

5. The design and construction of the propeller blades shall be such that impact damage that could reasonably be expected to occur when operating from the airfields described by the Project Authority in the Statement of Operating Intent shall not result in an unsafe condition between overhauls.

Blank Page

EXAMPLE OF A CONTRACT DETAILED SERVICES DESCRIPTION - ENGINEERING SUPPORT SERVICES – ESI ASPECTS

1 DSD NAME: DSD-ENG-XXX-ESS

2 TITLE: ENGINEERING SUPPORT SERVICES – ESI ASPECTS

3 DESCRIPTION AND INTENDED USE

3.1 This DSD provides generic guidance for Engineering Support Services that may be required to be provided by a contractor AEO as part of routine Engine Sturctural Integrity Program (ESIP) management, to ensure that the subject propulsion system is able to operate safely in accordance with the SOI, through life.

3.2 This DSD may require tailoring for specific propulsion systems.

4 PREPARATION GUIDELINES

4.1 Applicable Documents

4.1.1 The following documents form part of this DSD to the extent herein:

DI(G) LOG 8-15	Regulation of Technical Integrity of ADF Materiel
DI(G) OPS 2-2	ADF Airworthiness Management
AAP 7001.048	ADF Airworthiness Manual
AAP 7001.053	Technical Airworthiness Management Manual (TAMM)
AAP 7001.054	Airworthiness Design Requirements Manual (ADRM)
AAP 7001.060-4	CAMM2 Manual Authorised Engineering Organisation

4.1.2 The following Data Items are subordinate to this DSD and shall be delivered by the contractor:

Engine Structural Integrity Report (ESIR),	DID-ESIR
Engine Structural Integrity Management Plan (ESIMP),	DID-ESIMP
Engine Structural Integrity Document package (ESIDP),	DID-ESIDP
Health and Usage Monitoring System Validation Plan (HUMSVP),	DID-HUMSVP

(note: a HUMSVP is only required where specified by Section 4 Chapter 1 annex A)

4.2 Scope of DSD

4.2.1 This Detailed Service Description (DSD) describes the Engineering Support Services that the Contractor shall provide to support continuing airworthiness of the subject propulsion system fleet. This DSD describes the following:

a. Engineering Support Services that the Contractor shall conduct;

b. Embedded Commonwealth personnel that the Contractor shall employ within their Engineering Support Element (ESE); and

c. Constraints under which the ESE will conduct and manage the Engineering Support Services.

5 ENGINEERING SERVICES

5.1 Contractor Engineering Responsibilities

5.1.1 The Contractor shall manage and conduct all Engineering Support Services for the subject propulsion system, with the exception of Engineering Support Services that will be an ADO responsibility (refer clause 5.2).

5.1.2 DGTA provides overall program management of the reporting requirements. The Contractor is responsible for the project management of routine reporting and is to ensure tasking is in place in a timely manner for actioning of all requirements.

5.2 ADO Engineering Responsibilities

5.2.1 The Engineering Support Services to be conducted by the applicable ADO AEO are to be defined and listed in this part of the DSD.

5.3 Engine Structural Integrity Management

5.3.1 The Contractor shall be responsible for the establishment and implementation of an Engine Structural Integrity (ESI) management system for the subject propulsion system.

5.3.2 In implementing the subject propulsion system ESIP, the Contractor shall, as a minimum, conduct the following routine activities:

a. Document the ESIP through an ESI Management Plan (ESIMP), IAW AAP 7001.053 Regulation 3.5.5, as per the method detailed in the subject propulsion system ESIMP DID;

b. Review and amend the ESIMP on a biennial basis. The initial ESIMP and all subsequent ESIMP revisions shall be approved by DGTA prior to release;

c. Conduct annual planning to identify and prioritise ESIP tasks, responsible agencies and resources required;

d. Produce a written ESI submission to the annual parent aircraft Airworthiness Board (AwB), the content of which is to be approved by ESI1-DGTA prior to the AwB;

e. If required, deliver the ESI AwB presentation at the annual parent aircraft AwB;

f. Collect, record, store, and assess/trend usage data as obtained from the HUMS, EE500 sheets, EE360 sheets and CAMM2 (whichever is appropriate). Assessments shall be provided to ESI1-DGTA on an annual basis. Access to all UM data shall be made available to ESI1-DGTA on request;

g. Perform propulsion system condition monitoring activities on an ongoing basis as defined within the ESIMP for the propulsion system. Access to all CM data shall be made available to ESI1-DGTA on request;

h. Review (and initiate necessary improvements if required) to the propulsion system condition monitoring program on a no greater than biennial basis, with the aim of improving safety, reliability, availability and maintainability;

i. Provide to DGTA, on an agreed basis, a document summarising the propulsion system performance measures required to be trended in accordance with the ESIMP, including justification and proposed actions for any negative performance trends;

j. Establish and maintain a robust, in-country organisation for the management and conduct of the subject propulsion system ESIP, with adequate association to the propulsion system OEM to ensure adequate Instuctions for Continuing Airworthiness are received and actioned (for example, life limit revisions).

5.3.3 In implementing the subject propulsion system ESIP, the Contractor shall also:

a. Carry out validation of the Health and Usage Monitoring System (HUMS) for the subject propulsion system, IAW the HUMSVP DID;

b. Provide in-country access to adequate ESIP information (design, verification, and in-service usage/condition monitoring) for the life of the propulsion system;

c. Provide access to all design and certification data for the life of the propulsion system;

d. Upon request, provide access to data, processes, assumptions, executable software and other executable tools used in all ESIP management activities, sufficient to enable independent verification and validation;

e. Upon request, release any defective, cracked or non-conforming product to the Commonwealth for independent forensic investigation and analysis;

f. Allow for the embedding of one Commonwealth employee (DSTO or RAAF) in the in-country ASIP management organisation for periods of up to 24 months;

g. Upon request, accommodate DSTO and/or other contracted third party IV&V agencies acceptable to the Contractor, throughout the life of the propulsion system;

h. Document how the ESE shall comply with the ESI management policy/regulatory requirements within the documents listed at clause 4.1.1; and

i. Justify, in writing to DGTA, any need to deviate from any regulation or guidance, within the documents listed at clause 4.1.1, which are relevant to ESI management.

5.3.4 The Contractor shall carry out all other requirements of AAP 7001.053 Regulation 3.5.5, except where requirements are defined as an ADO engineering responsibility IAW paragraph 5.2 above. The Contractor shall note that guidance for Regulation 3.5.5 is contained in AAP 7001.053 Section 3 Chapter 17, and futher information is contained in AAP 7001.054 Section 4 Chapter 1.

5.4 Employment of Embedded Commonwealth Personnel

5.4.1 Where the Commonwealth provided Embedded Personnel to be employed within the ESE, these personnel are to be employed in accordance with the associated personnel DSD for this Contract and the approved Duty Statement (agreed between the Contractor and the Commonwealth).

5.5 Constraints

5.5.1 Deployment of Contractor Personnel

5.5.1.1 Contractor Personnel shall be deployed on exercises and to an AO by exception only. It is not envisaged that any Contracted personnel within the ESE shall deploy to an AO.

5.5.2 CAMM2

5.5.2.1 The Commonwealth will provide the Contractor with on-line access to CAMM2, if CAMM2 is mandated as the primary lifing tool by the Commonwealth. The following requirements will then also apply:

5.5.2.2 CAMM2 shall be used as the primary tool for Usage Monitoring for life limited parts.

5.5.2.3 Life limits and information associated with life limits (such as individual component damage factors) shall be in derived from those prescribed in the parent aircraft Technical Maintenance Plan.

5.5.2.4 The Contractor shall maintain the Engineering data within CAMM2 in accordance with AAP 7001.060-4 (AM1) CAMM2 Manual Authorised Engineering Organisation.

5.5.2.5 All CAMM2 System Management Centre (SMC) generated CAMM2 Action Notices (CANs) shall be complied with.

5.5.2.6 The Contractor shall warrant the data provided in CAMM2 in accordance with the associated Conditions of Contract.

5.5.2.7 The Contractor shall make available personnel, documentation, tools, data and access to the facilities required for DGTA to conduct internal and external CAMM2 audits.

5.5.2.8 Any tool supplied to augment CAMM2 shall be supplied and maintained by the Contractor. The Contractor shall provide the Commonwealth with the tools and training required to access this data.

5.6 Commonwealth Access to Data

5.6.1.1 On request, the Contractor shall provide the Commonwealth with access to all ESE data considered to be part of the baseline data items. The Contractor shall provide the Commonwealth with the tools required to access this data.

5.6.1.2 The Contractor shall make available to the Commonwealth, access to the facilities, the personnel, documentation, tools and data required to conduct AEO compliance assurance audits.

5.7 ESE Master Schedule

5.7.1 The Contractor shall maintain (and provide to the Commonwealth on request) a schedule of planned ESE activities, projecting future work effort for a period of not less than five years, or until the end of the Contract, when that is less than five years.

5.7.2 The Contractor shall provide to the Commonwealth a detailed schedule of planned ESE activities for a period of not less than one year, or until the end of the Contract, when that is less than one year.

5.8 Performance Measurement

5.8.1 The Contractor's performance of Engineering Support Services shall be measured against an agreed list of documented health measures, which shall be reviewed by DGTA at an agreed frequency. Performance measurement will focus on efforts made by the Contractor to improve the airworthiness of the propulsion system, whilst optimising the availability and cost to Commonwealth of the propulsion system.

5.8.2 Such measures may include a review of the following indicators (tailor as appropriate):

a. The success of upgrades and modifications carried out to improve safety, reliability, availability, maintainability and/or cost of ownership;

b. In Flight Shut Down (IFSD) rate;

c. IFSD drivers (ie reason for IFSD);

d. Mission Abort (MA) rate;

e. MA drivers (ie reason for MA);

f. Scheduled and unscheduled shop visit rates;

g. Unscheduled shop visit drivers (ie reason for shop visit);

h. Appropriate measures of engine availability (eg "engines above fit"); and

i. Average Time On Wing (TOW).

EXAMPLE OF A TENDER DATA ITEM DESCRIPTION – ENGINE STRUCTURAL INTEGRITY REPORT

1. DID NAME: TDID-ENG-ESIR

2. TITLE: ENGINE STRUCTURAL INTEGRITY REPORT

3. DESCRIPTION AND INTENDED USE

3.1 The Engine Structural Integrity Report (ESIR) describes the structural integrity issues associated with the proposed engine for the aircraft, including Condition Monitoring (CM) activities. The ESIR is a precursor to the Engine Structural Integrity Management Plan (ESIMP), which the Commonwealth will seek as part of the acquisition contract to meet the requirements of AAP 7001.053(AM1) Regulation 3.5.5.

3.2 The Commonwealth will use the ESIR to assess the engine certification basis, critical part lifing assumptions and analyses, the engine Usage Monitoring (UM) system and the effectiveness of the CM system.

Note to Tenderer: The Commonwealth considers a critical part to be one, which, upon failure cannot be contained by the engine casing or nacelle, or is the cause of another condition hazardous to aircraft safety.

Note to Tenderer: If the engine Original Equipment Manufacturer (OEM) has a corporate document (such as an engine Life Management Plan), which addresses some of the following ESIR requirements, the corporate document may be referred to by the ESIR but must also be provided to the Commonwealth.

4. INTER-RELATIONSHIPS

4.1 Nil

5. APPLICABLE DOCUMENTS

5.1 The following documents are referenced herein:

a. AAP 7001.054 – Airworthiness Design Requirements Manual, Sections 2 and 4.

b. AAP 7001.053(AM1) – Technical Airworthiness Management Manual, Reg 3.5.5 (including Section 3 guidance).

c. AAP 7001.059 – ADF aviation Maintenance Management Manual, Section 8, Chapter 13.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the TDRL Description.

6.2 Specific Content

6.2.1 The ESIR shall include the following information:

6.2.1.1 Certification Information

6.2.1.1.1 A general description of the propulsion system, including an engine cutaway diagram. This section should reference a detailed design specification and summarise the engine performance characteristics including thrust, maximum turbine entry temperature and specific fuel consumption.

6.2.1.1.2 A description of the proposed certification basis for the propulsion system. The certification basis shall be applicable to the unique configuration, role and operating environment that the Australian Defence Force (ADF) intends to use the Weapon System, as described in the *PROJECT ID* Statement of Operating Intent (SOI).

6.2.1.1.3 A description, in as much detail as possible, of the methodology employed by the OEM to life critical parts (eg safe life to crack initiation, damage tolerance, retirement for cause). Information shall include the mission profile chosen to life parts (ADF specific or other), design assumptions made when determining engine operating conditions and life limits (design mission types and mission mix, ambient temperature conditions, etc) and details of part testing carried out to validate life limits.

6.2.1.1.4 Where the ADF missions defined in the *PROJECT ID* SOI vary from the design assumptions, this shall be clearly identified and the implications on critical part life limits shall be documented.

6.2.1.1.5 A description of how the propulsion system will be certified against the chosen basis. Include details of any deviations from a prior certification basis for the engine as a result of the ADF unique configuration, role and operating environment.

6.2.1.1.6 As a minimum this section of the ESIR shall also include:

a. A description of any previous design certification by other airworthiness authorities. Any existing Type Certificate (TC) and Type Certificate Data Sheet (TCDS) should be attached to the ESIR.

b. For each prior certification, stipulate the design standard and its amendment status.

c. For each prior certification, provide details of any deviations or waivers that were granted against the referenced design standard.

d. A proposed plan for the certification of the propulsion system against the *PROJECT ID* SOI (this certification plan may be included in the Type Certification Plan).

6.2.1.2 Critical Part Life Management and UM

6.2.1.2.1 Identification of the authoritative source of critical part life limits (ie OEM Service Bulletin) for the engine.

6.2.1.2.2 A description of the UM methodology employed on the engine (ie conversion factor, cycle equation, real time cycle recording system). Where the ADF methodology is to differ from the OEM methodology, all differences are to be explained (ie where the OEM specifies a cycle equation but the ADF choses to utilise a conversion factor).

6.2.1.2.3 An explanation of any requirement to track ground running hours and/or cycles. If there is no requirement for tracking of ground running hours and/or cycles, this section shall define what assumptions this is based on (ie less than 10% of all engine hours/cycles are expected to be accrued on the ground and are accounted for in the published life limits).

6.2.1.2.4 A list of the engine critical parts determined by the engine OEM.

Note to Tenderer: The DID-ENG-XXX-ESIDP (Engine Structural Integrity Documentation Package) will request more detailed critical part lifing information such as; critical part lifing design assumptions, results of analytical crack growth modelling, results of any coupon testing and results of any critical part rig testing.

6.2.1.2.5 An explanation of the type, extent, performance, and details of data recording, storage and down-loading, of any Health and Usage Monitoring System (HUMS) to be fitted to the aircraft which is to be used for engine life management and maintenance management.

6.2.1.2.6 A description of the proposed method of validating the HUMS for the Aircraft propulsion system. This should include pre-service introduction bench testing of HUMS equipment and post-service introduction Verification and Validation (V&V) activities to verify the HUMS and associated procedures.

Note to Tenderer: A DID-V V-XXX-HUMS VP (HUMS Validation Plan) will be requested, refer ADRM Section 2 Chapter 19.

6.2.1.2.7 If the propulsion system to be used by the Weapon System is to include any used critical parts, this section shall define what life usage data is to be applied to the used components prior to ADF service introduction.

6.2.1.2.8 A description of the actions to be taken after the engine has entered Service to ensure the continued safe operation of critical parts. Includes identification of who will be responsible for carrying out these actions and should include specific responsibilities for the Weapon System Operator, the Through Life Support (TLS) Contractor, and the engine OEM where applicable. This section shall also include:

6.2.1.2.8.1 A definition of any engine OEM requirements for service sample inspections, and/or rig testing of service samples, to confirm initial design assumptions.

6.2.1.2.8.2 A definition of the requirements for usage data to confirm or update design mission type and mission mix assumptions. Responsibilities shall be specified for the TLS Contractor to regularly provide in-service usage data in a specified format suitable for the engine OEM to review critical part life limits.

6.2.1.2.8.3 Critical part life reviews at specific intervals to consider all aspects that impact on component life limits in order to confirm or revise critical part lives and define any actions for continued safe operation.

Note to Tenderer: More details on Critical Part Life Management activities will be required of DID-ENG-XXX-ESIMP (Engine Structural Integrity Management Plan).

6.2.1.3 CM Program

6.2.1.3.1 A description of the routine servicing requirements and CM techniques used for in service management of the engine. Refer AAP 7001.059 ADF AMMM Section 8, Chapter 13 for guidance.

6.2.1.4 Engine OEM Support Arrangements

6.2.1.4.1 A description of the Technical Assistance Agreement (TAA) or equivalent, that will exist between the TLS Contractor and the engine OEM for access to propulsion system and any HUMS technical data. The TAA shall also enable Commonwealth access to documentation pertaining to the certification process and the results of critical part lifing analyses to support any certification basis compliance finding activity the Commonwealth may get involved with.

6.2.1.4.2 This section shall describe the engine OEM's proposed in-service Component Improvement Program (CIP) or equivalent, including the frequency of meetings and the procedure for the TLS Contractor to communicate CIP issues. A statement on the amount of ADF involvement is required.

Blank Page

EXAMPLE OF A CONTRACT DATA ITEM DESCRIPTION – ENGINE STRUCTURAL INTEGRITY MANAGEMENT PLAN

1. DID NAME: DID-ENG-XXX-ESIMP

2. TITLE: ENGINE STRUCTURAL INTEGRITY MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 For a contractor AEO to meet the requirements of AAP 7001.053(AM1) Regulation 3.5.5., an Engine Structural Integrity Management Plan (ESIMP) is required. The ESIMP details the source of life limits for engine critical parts and the usage monitoring method required to track life consumption. It also defines ongoing actions required in-service, including CM, to ensure the continued airworthiness of the propulsion system.

4. INTER-RELATIONSHIPS

4.1 AAP 7001.054 – Airworthiness Design Requirements Manual Section 4 Chapter 1 ESI Document Package DID.

5. APPLICABLE DOCUMENTS

5.1 The following documents are referenced herein:

a. AAP 7001.054 – Airworthiness Design Requirements Manual.

b. AAP 7001.053(AM1) – Technical Airworthiness Management Manual.

c. AAP 7001.059 ADF Aviation Maintenance Management Manual

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL Description clause entitled “General Requirements for Data Items”. The specific content described by Section 6.2 below shall be included as a minimum requirement. *Paragraphs 6.2.1.1 through 6.2.1.5 (inclusive) shall be transposed to the Data Item verbatim. The remaining parts of this DID provide guidance for the information required*.

6.2 Specific Content

6.2.1 Introduction *(ESIMP Section 1)*

6.2.1.1 **General.** To promote the continued airworthiness of propulsion systems on ADF aircraft, DGTA has established the concept of an Engine Structural Integrity (ESI) management system. The ADF technical airworthiness regulations pertaining to ESI management systems are defined by **Regulation 3.5.5.**, contained in AAP 7001.053 Technical Airworthiness management Manual (TAMM). Guidance on this regulation is contained in Section 3 Chapter 17 of the TAMM.

6.2.1.2 IAW the guidance to TAMM Regulation 3.5.5., the TAR preferred ESI management system is the ESI Program (ESIP). An ESIP is an organised, holistic approach to the **acquisition** and **in service life**

management of a gas turbine engine[1]. An ESIP requires effective **fatigue life management** and **condition assessment** of the propulsion system. Fatigue life management is achieved by correctly implementing approved component life limits and a Usage Monitoring (UM) system to track appropriate accrued fatigue life. Condition or 'health' assessment is achieved through implementation of an effective Condition Monitoring (CM) Program. Specific guidance on CM Programs is contained in Section 8 Chapter 13 of AAP 7001.059 ADF Aviation Maintenance Management Manual (AMMM). Both disciplines require some knowledge of the engine's design.

6.2.1.3 TAMM Regulation 3.5.5 requires the ESIP (or equivalent ESI management system) to be documented through an ESI Management Plan (ESIMP). An ESIMP Data Item Description (DID) is contained in Section 4 Chapter 1 of the AAP 7001.054 Airworthiness Design Requirements Manual (ADRM).

6.2.1.4 **Purpose of an ESIMP.** The information contained in an ESIMP will enable:

a. The retention of corporate knowledge on ESIP management within the ADF;

b. The ADF TAR to maintain oversight and understanding of the ESIP employed;

c. The ADF TAR to make informed decisions, particularly when approving ADF life limits and managing life reductions, should they occur in service; and

d. Implementation of a maintenance program that regularly assesses the condition of oil wetted components, components exposed to the gas path, and other components where applicable, to optimise system Reliability, Availability and Maintainability (RAM). For rotary wing aircraft, the CM program will also address CM of the transmission system.

6.2.1.5 **Content of an ESIMP.** The ESIMP will document the ESIP and include, as a minimum:

a. An overview of the engine certification basis, including a basic engine description, details of the certification basis and reference to the type data. Where available, the Type Certificate Data Sheet (TCDS) is to be included as an enclosure;

b. Identification of all critical parts that are life limited;

c. Identification of the authoritative source for life limits and any mandatory inspections;

d. A description of the UM system required to track the life usage of critical parts and to manage maintenance servicing;

e. Where applicable, identification of the authoritative source for conversion factors required to track fatigue accrual on rotating parts;

f. Identification of engine life management activities, such as periodic reviews of ADF usage, component fatigue tests and Technical Life Reviews (TLR) for critical parts;

g. A detailed description of significant events affecting the propulsion system through life, such as fleet wide life limit reductions, the results of TLR's, modifications, upgrades, etc;

h. All actions (both one-off and recurring) that are required to ensure that life limits and UM systems remain valid over the service life of the engine type; and

i. A detailed description of the CM program employed on the engine, including a description of the system being monitored, details of the CM techniques employed and the frequency of monitoring, and a propulsion system materials map.

---

1 This definition of an ESIP differs fundamentally from that of an ADF ASIP (and the definition of an ESIP in MIL-HDBK-1783B). The ADF ESIP focuses almost entirely on in service management, whereas the ADF ASIP (and MIL-HDBK-1783B ESIP) also cover design and construction aspects. The primary reason for the difference is simply that the ADF will not usually be able to obtain adequate information on engine design and construction to benefit from its use in the ESIP. For example, ADF ESIP's normally rely heavily on the adequacy of OEM derived life limits, and no ADF validation of these limits is possible since the relevant design data is usually proprietary. In comparison, an ADF ASIP may benefit from indigenous aircraft fatigue testing, which can validate an OEM derived life limit (or identify an ADF specific limit), using known or obtainable design data.

6.2.1.6 **Scope of the ESIMP.** This section should describe which engines the ESIMP is applicable to, the aircraft types the engines are fitted to and the ADF units that operate these aircraft.

6.2.1.7 **ESIMP Stakeholders.** This section should list the ESIMP stakeholders. As a minimum, it shall include the following AEO/Contractor and Commonwealth representatives:

a. the relevant Design Acceptance Representative (DAR);

b. the Engine Structural Integrity (ESI) Manager within the AEO/Contractor organisation;

c. the engine OEM (if the AEO is someone other than the engine OEM);

d. DAIRENG-DGTA;

e. The ADF Operating Units; and

f. The engine's maintenance facilities, (all Operational and Deeper Maintenance - OM and DM).

6.2.1.8 **ESIMP Responsibilities.** This section should detail the responsibilities of all parties involved in the management and implementation of the ESIMP.

6.2.1.9 **Maintenance Venues.** This section should detail the OM and DM venues, including location and scope of work (type of servicing).

6.2.1.10 **Planned Withdrawal Date (PWD).** State the PWD for the aircraft (as distinct from the aircraft Life Of Type).

6.2.1.11 **Amendment of the ESIMP.** This section of the ESIMP should detail the procedures to be followed and approvals required for changes to the ESIMP. The DAR should endorse ESIMP amendments before approval by DAIRENG-DGTA. The ESIMP is to undergo a full review by the ESI Manager at the AEO and DAIRENG-DGTA at least once every two years.

6.2.1.12 **Information Security and Privacy.** This section should describe any security or privacy considerations associated with the use of the information in the ESIMP.

6.2.2 **Certification Information *(ESIMP Section 2)***

6.2.2.1 **General Engine Description.** The ESIMP shall include a general description of the breakdown of the engine (including an engine cutaway) and summarise the engine performance characteristics including thrust, maximum turbine entry temperature and specific fuel consumption. This section shall also make reference to the engine design specification, obtained separately by the Commonwealth via the ESIDP (refer ESIDP DID). The Part Number (PN) for the engine variant used by the ADF will be listed.

6.2.2.2 **Engine Certification.** The ESIMP shall state the engine certification basis including any limitations placed on the engine or aircraft, the engine TC and TCDS shall be provided as attachments. The certification basis includes the design standard and any unique ADF requirements as described in ADRM Section 4 Chapter 1.

6.2.2.3 This section shall include any deviations from the prior certification of the engine as a result of the unique ADF Configuration, Roles and Environment as described in the parent aircraft SOI.

6.2.2.4 This section shall also include:

a. A synopsis of any previous design certification by other airworthiness authorities;

b. For each prior certification, the design standard and its amendment status; and

c. For each prior certification, details of any limitations placed on the engine or aircraft that were more severe than the limitations of the referenced design standard.

6.2.2.5 **OEM Critical Part Lifing Philosophy.** This section shall include:

a. A definition of the design philosophy used to identify life limited critical parts; eg safe life to crack initiation, damage tolerance, retirement for cause, 2/3 dysfunction. Detail other aspects of the OEM policy such as the amount of part testing carried out to validate life limits, and the

statistical confidence applied to life limits. Discuss any irregularities to the general philosophy relating to parts in the engine (for example, if different critical crack sizes are assumed).

b. The engine usage assumptions made by the engine OEM when determining engine operating conditions and life limits, such as reference mission types, mission mix, ambient temperature mix, and any other relevant parameters.

c. The ADF mission types that are published in the respective aircraft SOI. Where the ADF missions are known to vary from OEM reference missions, this should be clearly detailed and the implication on life limits shall be documented in the ESIMP. Where possible/applicable, a statement from the OEM detailing that the ADF mission has been accounted for in deriving life limits is required. Where the effect of any variations is ignored by the OEM in providing ADF life limits, justification is to be provided.

6.2.3 Critical Part Life Management and Usage Monitoring *(ESIMP Section 3)*

6.2.3.1 OEM Authoritative Source of Critical Part Lives and UM Methodology. Detail the document(s) which stipulate(s) OEM recommended part life limits and UM methodology. Provide details of how fatigue life is accrued via the OEM methodology. Where applicable, a description of the lifing algorithm used to calculate cyclic life accrual is to be provided, including definitions for all parameters (eg full and partial cycles). Where several UM options exist for the operator, describe the options briefly and explain in detail the chosen option for the ADF, including reasons for why the method was chosen.

6.2.3.2 To avoid repetition and the requirement for unnecessary ESIMP amendment, reference to the OEM document(s) for life limit information is desirable, but only where it contains all the information required in para 6.2.3.3 below. Otherwise, lifing data sheets for each critical part are required, as appendices to this section. Where critical parts are available as more than one part number, data for each part number shall be included.

6.2.3.3 Each lifing data sheet shall contain the following information about the component:

a. Name;

b. Part Number;

c. Material;

d. Schematic clearly identifying all life limiting locations;

d. The current OEM life limit for each life limit location;

e. The current ADF life limit for each life limit location (if different to the OEM limit);

f. The basis of the selected life limit, eg -3 life to Low Cycle Fatigue (LCF) crack initiation;

g. The predicted consequence of failure for the critical part, ie contained or uncontained;

h. Any other relevant lifing factors for the critical part, eg damage factors; and

i. A summary of the critical parts lifing history. For each change to the critical parts declared life limit (both OEM and ADF changes). This section should record:

1) The date that the change became effective;

2) The new declared life limit;

3) The reason for the change; eg updated mission analysis, updated stress analysis, ADF variation; and

4) Reference details for any applicable lifing reports, Service Letters or Service Bulletins.

6.2.3.4 Data sheets must be included in this section for parts where the ADF has adopted a different life limit or UM methodology to that of the OEM. A suggested example format for a critical part lifing data sheet is in AAP 7001.054 Section 4, Chapter 1, Annex E, Appendix 1.

6.2.3.5 ADF Authoritative Source of Critical Part Lives and UM Methodology. State that the ADF authoritative source for critical part lives is the applicable AAP Technical Maintenance Plan. Provide justification for any difference between OEM life limits (provided to the ADF IAW Service Bulletins,

engineering letters, drawings, etc) and ADF life limits. A NAA (or recognised foreign military force) is not the OEM. Where the ADF adopts life limits provided by a NAA, justification for any difference between these limits and those prescribed by the OEM (IAW Service Bulletins, engineering letters, drawings, etc) is required.

6.2.3.6 This section shall also describe in detail the ADF methodology for UM, if different from the OEM method (provided to the ADF IAW Service Bulletins, engineering letters, etc), including a justification for all variations. For example, where an OEM recommended mathematical algorithm is transformed into a generic cycle/hour Conversion Factor, the algorithm is to be described in the preceding section and the CF methodology is to be described here. Where the ADF adopts a UM method of a NAA, justification for any difference between this UM method and that prescribed by the OEM is required.

6.2.3.7 **UM System Architecture.** Provide a description of the system architecture, including airborne hardware, ground hardware, interfaces between airborne and ground hardware and software storage capabilities (as applicable). Include a description of the engine parameters that are recorded for UM purposes such as specific temperatures, pressures and spool speeds. Also provide:

a. **Data Flow Management.** A description of the data flow management processes and the responsibilities of organisations involved with data flow management from the aircraft to the lifing database. For complicated parts life tracking systems, it may be more appropriate to refer to a controlled document rather than describe the data flow management processes in the ESIMP.

b. **Lifing Database.** A description of the database system used to record and track life usage and to ensure critical part removal before reaching life limits.

c. **Lost or Corrupted Usage Data.** This section should list the actions to be taken in the event that lifing data is lost or corrupted. For engines managed by tracking cycles, this should include the use of suitable ‘fill-in’ factors or conversion factors to convert known hourly accrual into cyclic accrual.

d. **Verification and Validation (V&V).** If applicable, provide details of any V&V testing carried out by the ADF for a Health and Usage Monitoring System (HUMS).

6.2.3.8 **Ground Running Requirements.** Detail whether damage accumulation during installed and uninstalled ground running is required to be accounted for. If there is no requirement for tracking of ground running hours and/or cycles, this section shall define what assumptions this is based on (ie less than 10% of all engine hours/cycles are expected to be accrued on the ground and are accounted for in the published life limits).

6.2.3.9 **In service requirements.** This section of the ESIMP shall detail the actions to be taken after the engine has entered service that will ensure the continued safe operation of critical parts through life. It shall:

a. Detail any OEM requirements for in-service sample inspections or rig testing of Service Samples, to confirm initial assumptions regarding the service environment.

b. Detail any Technical Life Review (TLR) required at specific life intervals to confirm or revise the life limit for a particular critical part, and outline any actions necessary for continued safe operation.

c. Specify that an ADF mission analysis (usage review) is to be carried out at least once every 5 years, or as recommended by the OEM, to confirm or update service usage assumptions which could impact fatigue life accrual.

6.2.3.10 Finally, this section shall detail any other significant factors in life management and UM aspects, such as fleet wide lifing reductions, recovery programs, etc.

6.2.4 Condition Monitoring Program *(ESIMP Section 4)*

6.2.4.1 The CM program shall describe all propulsion system CM programs directed for use by the OEM, and those offered by the AEO/Contractor in addition to OEM requirements. For each program, this section shall detail as a minimum the following information:

6.2.4.2 **Description.** This paragraph shall detail:

a. the system being monitored by the program;

b. the failure modes of the system that the CM program is designed to detect;

c. an overview of the program and the CM techniques required; and

d. the samples/data collected including the limits and appropriate links to the maintenance manuals should these limits be exceeded.

6.2.4.3 **Operation.** This paragraph shall detail:

a. who will process and analyse the samples/data;

b. who will review the program results and decide if the system is serviceable; and

c. on what basis the serviceability decision will be made.

6.2.4.4 **Training.** This paragraph shall detail:

a. the training required for sample/data collectors;

b. the training required for sample/data processing and analysis; and

c. how often training will be required and who will provide it.

6.2.4.5 **Performance Feedback.** This paragraph shall detail:

a. how the missed detection rate will be measured,

b. how the false alarm rate will be measured, and

c. how the successful detection rate will be measured.

6.2.4.6 **Propulsion System Material Map.** Where possible, a Propulsion System Materials Map (PSMM) shall be included that provides sufficient information on each propulsion system component to enable the Commonwealth to identify the origin of collected wear debris from the oil system. This information should include:

a. material compositions and specific details of heat treatments and any other surface modification treatments; and

b. non-metallic materials, in addition to metallic materials if the AEO/Contractor believes that non-metallic debris could be useful in determining system condition.

6.2.4.7 The AEO/Contractor shall use the PSMM to document details of any change to the composition of components, throughout the life of the tendered aircraft.

6.2.4.8 The AEO/Contractor shall also provide a material map for any other oil wetted aircraft system (eg, Auxiliary Power Unit) that requires condition monitoring.

6.2.5 **Technical Investigations *(ESIMP Section 5)***

6.2.5.1 The purpose of this section is to record engine life management information that might be of use in the future. For example:

a. Synopses of any engine related Service Release Limitations raised by the ADF Airworthiness Representative when issuing an Australian Military Type Certificate,

b. Any life reductions to components resulting from manufacturing defects,

c. Any life reductions to components as a result of re-analysis of material properties,

d. Any DSTO investigations/tasks of significance, or

e. Any large changes to the CM program to improve poor RAM of the propulsion system.

6.2.5.2 This section shall also be used to record the outcomes of significant technical queries to the engine OEM.

6.2.6 Performance/Trend Monitoring (ESIMP Section 6)

6.2.6.1 This section shall detail all measures in place to trend the performance of the propulsion system. The following measures shall be trended, or justification provided where there is nil requirement:

a. In Flight Shut Down (IFSD) rate;

b. IFSD drivers (ie reason for IFSD);

c. Mission Abort (MA) rate;

d. MA drivers (ie reason for MA);

e. Scheduled and unscheduled shop visit rates;

f. Unscheduled shop visit drivers (ie reason for shop visit);

g. Some appropriate measure of engine availability (eg “engines above fit”); and

h. Average Time On Wing (TOW).

6.2.6.2 All measures shall be trended on a periodic basis. The level/rate of acceptability for each measure shall be defined in order to ensure management action is taken where required.

6.2.7 OEM Support Arrangement *(ESIMP Section 7)*

6.2.7.1 This section should describe the engine OEM Component Improvement Program (CIP) or equivalent, including the frequency of meetings and the procedure for communicating on CIP issues between user Nations. The section shall also document any Technical Assistance Agreement (TAA) existing between the AEO/Contractor and the engine OEM. Other specific technical support arrangements shall also be recorded.

6.2.8 Actions Required *(ESIMP Section 8)*

6.2.8.1 This section shall describe the actions that must be undertaken to ensure ongoing effective ESI management. This may include ongoing or one-off tasks required of the engine structural integrity manager or other parties. Tasks shall include those which relate to:

a. Sponsorship and maintenance the ESIMP;

b. DAIRENG-DGTA approval for ESIMP amendments through ESI1-DGTA;

c. Life management of engine critical parts being correctly performed in accordance with engine OEM requirements and definitions;

d. Ensuring updates to relevant lifing bulletins/OEM advice are received and subjected to the TIR process in accordance with the TAMM in an appropriate timeframe;

e. Notification to ESI1-DGTA of any changes to critical part life limits, inspections, UM or CM requirements;

f. Ensuring relevant critical part life limits are transferred to the aircraft TMP in an appropriate timeframe;

g. Ensuring CM programs are adequate and up to date;

h. Notification to the ADF TAR (through ESI1-DGTA) of any un-contained failures; and

i. Action of any outstanding issues from previous ESIMP reviews.

Appendix:

1. Example of a Engine Critical Part Lifing Data Sheet

Blank Page

EXAMPLE OF A CONTRACT DATA ITEM DESCRIPTION – ENGINE STRUCTURAL INTEGRITY DOCUMENT PACKAGE

1. **DID NAME: DID-ENG-XXX-ESIDP**

2. **TITLE: ENGINE STRUCTURAL INTEGRITY DOCUMENT PACKAGE**

3. **DESCRIPTION AND INTENDED USE**

3.1 The Engine Structural Integrity Documentation Package (ESIDP) will be used by the Commonwealth to support the Type Certification Program conducted in accordance with the Approved Type Certification Plan.

4. **INTER-RELATIONSHIP**

4.1 Nil

5. **APPLICABLE DOCUMENTS**

5.1 Nil

6. **PREPARATION INSTRUCTIONS**

6.1 **Generic Format and Content**

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL Description clause entitled “General Requirements for Data Items”.

6.2 **Specific Content**

6.2.1 The ESIDP shall contain the FAA (or equivalent National Airworthiness Authority) Certification data provided in the same format that was presented to the FAA Certification Officer during the original certification process.

6.2.2 If not included as part of the documentation at paragraph 6.2.1, the contractor shall also provide the Commonwealth with the engine design specification document(s) and all applicable Type Certificates and Type Certificate Data Sheets.

Blank Page

LESSONS LEARNT

Consideration of ADF Configuration Role and Environment for previously certified aircraft

1. For example, the ADF may acquire a helicopter previously certified by the USN but then modify the aircraft configuration such that additional cooling air is required from the turboshaft engines. The engine OEM needs to be informed of this to ensure that the performance ratings of the engine are still applicable and to ensure that the engine does not have to operate at higher rpm and temperature to accommodate the additional bleed air to the aircraft ECS. Increasing engine rpm and operating temperatures will increase stresses on critical rotating components and may warrant a lifing review and re-analysis.

Lockheed C-130J Hercules Propulsion Certification Issues

2. ***Propulsion System Induced Vibration.*** Propulsion systems are one of the main sources of vibration within an aircraft system. Multi engine propeller driven aircraft in particular may suffer from vibrations induced by the propellers, due to the passing of the propeller tips across wings/airframe. The frequency of this vibration is effected by a number of factors including the number of blades per propeller. In the case of the C-130J-30 the introduction of a six-blade propeller has changed the vibration environment of the aircraft, compared with that of earlier models of the C-130. This in turn has lead to a reassessment of the suitability of some equipment for carriage in the C-130J-30.

3. This issue highlights the need for PO's to inform all stakeholders of the potential impacts that new or modified engines may have on other aircraft systems or cargo. PO's should seek information from the engine/airframe OEM's concerning potential impacts.

4. ***HUMS Validation.*** FAR 33 civil certification of the AE2100D3 engine fitted to the C-130J-30 was based on the inclusion of an automated and functioning HUMS capable of tracking the cyclic accrual of the engine critical parts. Unfortunately, the possibility that HUMS interface issues between the new engine and airframe could exist was not highlighted during the acquisition process. Insufficient attention was placed on the specification, development and validation of the HUMS. When the aircraft was delivered to the ADF the HUMS did not appear to function correctly and no validation evidence was provided. This put the responsibility back onto the ADF to ensure that a robust manual cycle counting procedure was in place to maintain the airworthiness of the engines and the certification basis.

5. This issue highlights the need for PO's to understand the certification basis of the engine. It also highlights that ESI-DGTA must provide clear guidance to PO staff on specialist aspects of engine certification, including integration aspects. It will not usually be possible for the ADF to influence the design of a HUMS. This means validating the HUMS before introduction to service is extremely important and a HUMS Plan has been formulated for future use.

6. ***On-condition Components.*** The AE2100D3 engine OEM anticipated that the HUMS would be able to evaluate the engine condition and alert the user when engine overhaul was required. Unfortunately, the HUMS CM functionality did not work and the manual procedure provided by the OEM did not capture the creep failure mode of the turbine blades. This led to an RAF in-flight turbine blade failure and subsequent short-term disruption of C-130J operations. In conjunction with the OEM, the ADF developed a borescope inspection program to enable the condition of the turbine to be assessed.

7. This issue highlights that during the acquisition process, it is essential for the PO to have an understanding of the engine OEM requirements and to ensure those requirements form part of the certification basis for the airframe (and the requirements are correctly implemented by the airframe OEM).

8. ***Usage Assumptions.*** The RAF tubine blade failure discussed above, combined with previous ADF/DSTO analysis, highlighted the importance of communication between the airframe OEM, the engine OEM and the customers. In the design specification for the engine, the airframe OEM had assumed a mission with 79% of the total Engine Operating Time (EOT) at the Part Power (PP) setting and 2% of the total EOT at the Maximum Continuous Power (MCP) setting (ie for take off only). The ADF, like other customers, actually flew missions where only around 8% of EOT was at PP and 90% of EOT was at MCP. The significant difference in EOT at MCP caused a massive increase in the rate of degradation of turbine components exposed to the gas path. If left unresolved, the engines would have had a time between overhaul of less than half of that expected. When the problem was identified, the ADF altered its operations to reduce the time spent at MCP until engine durability could be improved.

9. A comparison of the Statement of Operating (SOI) to the engine design specification earlier in the acquisition phase may have highlighted the discrepancy and the damage incurred to the AE2100D3 fleet may have been avoided. Also, an early review of operator usage data would have alerted the engine OEM to the fact that the engines were being operated more severely than assumed during design.

Boeing CH-47D Chinook Propulsion Certification Issues

10. The engines identified for ***Project AIR9000 Phase 5A (T55 engine upgrade).*** were Foreign Military Sales (FMS) T55-GA-714A engines, sold by the US Army. The US Army is a recognised foreign Military Force IAW TAMM Regulation 2.2.7. Sale of these engines to the ADF included the provision of all technical documentation such as technical maintenance publications and documents specifying the life limits and UM methodology for critical parts. In terms of ESI and critical parts management, the US Army owned GA-714A is manufactured by the OEM and is identical to the OEM's L-714A engine. Given the TAR preferred approach for gas turbines is to accept OEM life limits and UM methodologies, additional design disclosure of US Army policy was required for ADF certficiation to be carried out. To assist the PO in determining whether "prior acceptance" under Regulation 2.2.7. was possible, DGTA-ESI1 sought advice/justification from the US Army on the acceptability of the US Army policy for the ADF.

11. The responses from the US Army, spanning several months, were generally insufficient to establish confidence that the US Army policy had been adequately justified to the extent necessary for the adoption of "prior certification". Specifically, concerns include the adoption of hot section life limits up to 55% higher than those recommended by the OEM, turbine blade life limits being ignored, and the adoption of a Digital Electronic Control Unit (DECU) for UM, which accrues fatigue cycles differently to the OEM recommended method. Finally, the DECU does not record cycles for all life limited parts identified by the OEM. Neither the US Army life limits, nor the use of the DECU for UM, was endorsed by the OEM, and the US Army had not provided adequate justification that their policy was acceptable.

12. This issue highlights that for engines purchased through NAA's or recognised military forces, early identification and comparison between the life limits and UM methodologies of the NAA and OEM is essential to efficient engine certification. It is important to consider whether an agreement with the OEM to provide such information is a necessary requirement.

13. Where possible, PO's should commit to purchasing FMS engines with adequate agreements in place to allow the OEM to supply technical information such as life limits. Such agreements exist for many ADF engines such as the GE F404 (Hornet).

BAe Hawk 127 In Service Usage Reviews

14. The BAe Hawk 127 was introduced into RAAF service in 2000. As discussed in the usage reviews paragraph of Section 4 Chapter 1, it is usual to conduct a review after (approximately) two years of in service use. However, in the case of Hawk, the flying conducted from 2000 to 2002 was predominantly capability development missions, not Lead In Fighter (LIF) training. Initially, the aircraft was flown like the MB-326 Macchi aircraft it replaced, and the missions adapted over time to take advantage of the improved capabilities of the new aircraft. Initially therefore, the Hawk's Rolls Royce Adour Mk 871 engines were utilised in a relatively benign way. As a result, a decision could be made to defer the initial usage review to a more appropriate time, to enable more applicable data to be collected.

This issue highlights that before any usage review is carried out, a comparison of engine intended to actual usage should be carried out. PO's should consider this aspect in any contractual requirement for TLS. ESI1-DGTA should be consulted in cases where the need for a usage review is not clear.

LIST OF ABBREVIATIONS

Abbreviation	Definition
AAP	Australian Air Publication
AAR	Air-to-Air Refuelling
AD	Airworthiness Directive
ADF	Australian Defence Force
AEEC	Airlines Electronic Engineering Committee
AELD	Aircraft Electrical Load Data
AEO	Authorised Engineering Organisation
AIP	Airworthiness Inspection Plan
AMAFTU	Aircraft Maintenance and Flight Trials Unit
AMCPTS	Aeromedical Clinical Performance Tests
AME	Aeromedical Evacuation
AMRL	Aeronautical and Marine Research Laboratory
AMTC	Australian Military Type Certificates
AMTDU	Air Movements Training and Development Unit
AOC	Australian Ordnance Council
APR	Antenna Placement Report
APU	Auxiliary Power Unit
ARDU	Aircraft Research and Development Unit
ARINC	Aeronautical Radio, Inc.
ARP	Aerospace Recommended Practice
ARS	Autonomous Recovery System
AS/NZS	Australia/New Zealand Standards
ASCC	Air Standardisation Coordinating Committee
ASEMM	Aircraft Software Engineering Management Manual
ASIMP	Aircraft Structural Integrity Management Plan
ASIP	Aircraft Structural Integrity Program
ATC	Air Traffic Control
ATF	Automatic Terrain Following
BIT	Built-in Test
BITE	Built-in Test Equipment
BSSC	Board for Software Standardisation Council (ESA)
CAF	Chief of Air Force
CASA	Civil Aviation Safety Authority
CASE	Computer-aided Software Engineering
CBD	Certification Basis Description
CBIT	Continuous BIT
CCP	Corrosion Control Plan
CDR	Critical Design Review
CENGR	Chief Engineer
CI	Configuration Item
CIP	Component Improvement Program
CLR	Component Life Review
CMM	Capability Maturity Model
COE	Centre of Expertise
COM	Computer Operation Manual

Abbreviation	Definition
COTS	Commercial Off-The-Shelf
CPM	Computer Programmers Manual
CSCI	Computer Software Configuration Item
CSF	Contracted Support Facility
CVR	Cockpit Voice Recorder
DAA	Design Approval Authority
DAC	Design Approved Contractor
DAIRENG	Directorate of Aircraft Engineering
DAO	Defence Acquisition Office
DAR	Design Acceptance Representative
DBDD	Database Design Description
DEF STAN	Defence Standard (UK MoD)
DGTA	Directorate General Technical Airworthiness
DI(AF) LOG	Defence Instruction (Air Force) Logistics
DID	Data Item Description
DM	Deeper Maintenance
DoD	Department of Defence (US)
DSTO	Defence Science and Technology Organisation
DTA	Damage Tolerance Assessment
E^3	Electromagnetic Environmental Effects
E^3ATP	E^3 Acceptance Test Plans
E^3CAB	E^3 Control Advisory Board
E^3CP	E^3 Control Program
E^3CPP	E^3 Control Program Plan
E^3TR	E^3 Test Report
ECP	Engineering Change Proposal
ECS	Environmental Control Systems
EED	Electro-Explosive Device
EIA	Electronic Industries Association
ELT	Emergency Locater Transmitter
EMC	Electromagnetic Compatibility
EME	Electromagnetic Environment
EMV	Electromagnetic Vulnerability
ENSIP	Engine Structural Integrity Program
ESA	European Space Agency
ESIMP	Engine Structural Integrity Maintenance Plan
EUMS	Engine Usage Monitoring System
FAA	Federal Aviation Administration (US)
FAR	Federal Aviation Regulation (FAA)
FBW	Fly-by-Wire
FCA	Functional Configuration Audits
FCS	Flight Control System
FDR	Flight Data Recorder
FEG	Force Element Group
FHA	Functional Hazard Analysis
FHQ	Flight Handling Qualities
FPO	Failure Probability Objectives

Abbreviation	Definition
FSM	Firmware Support Manual
FTS	Flight Termination System
GCS	Ground Control Station
GOA	Generic Open Architecture
GPS	Global Positioning System
GPWS	Ground Proximity Warning System
HE	Human Engineering
HHA	Health Hazard Analysis
HOL	Higher Order Language
HWCI	Hardware Configuration Item
HUMS	Health and Usage Monitoring
IBIT	Initiated BIT
ICD	Interface Control Document
IDD	Interface Design Description
IEEE	Institute of Electrical and Electronic Engineers
IFF	Identification Friend or Foe
IFR	Instrument Flight Rules
IRS	Interface Requirements Specification
ISO	International Organisation for Standardisation
IV&V	Independent Validation and Verification
JAA	Joint Airworthiness Authority
JAC	Joint Airworthiness Committee (UK MoD)
JALO	Joint Army Logistics Organisation
JAR	Joint Airworthiness Regulations
LCC	Life Cycle Costs
LMSQN	Logistic Management Squadrons
LRU	Line Replacement Unit
LSLMFLT	Life Support Logistic Management Squadron
MFCS	Manual Flight Control System
MFD/HUD	Multi-Function Displays/Head Up Displays
MIL-STD-xxx	Military Standard (US)
MoD	Ministry of Defence, United Kingdom
NAA	National Airworthiness Authority
NDI	Non Developmental Items
NEMP	Nuclear Electromagnetic Pulse
NVIS	Night Vision Imaging System
OAAR	Operational Airworthiness Authority Representative
OAR	Operational Airworthiness Regulator
OBOGS	On-board Oxygen Generating System
OCD	Operational Concept Document
ODWS	Oxygen Delivery Warning System
OEM	Original Equipment Manufacturer
OFP	Operational Flight Program
OM	Operator Maintenance
OS&HA	Occupational Safety and Health Analysis
PBIT	Power on BIT
PCA	Physical Configuration Audits

Abbreviation	Definition
PDR	Preliminary Design Review
PED	Portable Electronic Device
PFR	Primary Flight Reference
PHA	Preliminary Hazard Analysis
PO	Project Office
PPB	Positive Pressure Breathing
PRV	Pressure Reducing Valves
PSSA	Preliminary System Safety Assessment
RFT	Request For Tender
RPT	Resident Project Team
RSF	Commonwealth Support Facility
RTCA	Requirements and Technical Concepts for Aviation
S/N	Serial Number
SAE	Society of Automotive Engineers
SCI	Systems Certification and Integrity
SDA	Service Design Agency
SDD	Software Design Description
SDF	Software Development File
SDP	Software Development Plan
SE	Specified Effort
SEICMM	Software Engineering Institute Capability Maturity Model
SHA	Safety Hazard Analysis
SIL	Software Integrity Level
SIOM	Software Input/Output Manual
SIP	Software Installation Plan
SLA	Service Life Assessment
SLOC	Source Lines of Code
SOI	Statement of Operating Intent
SOW	Statement of Work
SPO CENGR	Systems Program Offices Chief Engineer
SPS	Software Product Specification
SRS	Software Requirements Specification
SSA	System Safety Assessment
SSDD	System/Sub-system Design Description
SSHA	System Safety Hazard Analysis
SSP	Software Support Plan
SSPP	System Safety Program Plan
SS	Specified Support
SSS	System/Sub-system Specification
SSWG	System Safety Working Group
STANAG	Standardised Agreement NATO
STD	Software Test Descriptions
STSC	Software Technology Support Centre (USAF)
STP	Software Test Plan
STR	Software Test Report
STrP	Software Transition Plan
SUM	Software Users Manual

Abbreviation	Definition
SVD	Software Version Description
T&E	Test and Evaluation
TACAN	Tactical Air Navigation
TAR	Technical Airworthiness Regulator
TCAS	Traffic Collision Avoidance System
TCDS	Type Certificate Data Sheet
TEWG	Tender Evaluation Working Group
TN	Note to Tenderers
TRR	Test Readiness Review
UAV	Unmanned Aerial Vehicle
ULD	Underwater Locating Devices
USAF	United States Air Force
US DoD	United States Department of Defence
USN	United States Navy
V&V	Validation and Verification
VFR	Visual Flight Rules
VHF	Very High Frequency
VS	Vendor Support
VSTOL	Very Short Take-off and Landing
WSLMSQN	Weapon System Logistics Management Squadron

Blank Page