

NOTICE OF PROPOSED RULE MAKING DGTA 03-11

SYSTEM SAFETY REGULATION

INTRODUCTION

Applicability

1. This proposal is applicable to all aerospace Authorised Engineering Organisations (AEOs) and Project Offices (POs) involved in the design, development, acquisition and management of Configuration Items (CIs) for aircraft and/or Aeronautical Product.

Purpose

2. The purpose of this Notice for Proposed Rule Making (NPRM) is to advise and seek feedback from stakeholders on the proposal to issue new System Safety ADF Technical Airworthiness Regulations (TAREGs) in AAP7001.053(AM1) *Technical Airworthiness Management Manual*.

Consultation

3. TAREG 1.1.2 requires that interested persons participate in TAREG drafting proceedings. The aim of this NPRM is to promulgate background and details of the proposed changes. Advice on how petitions on this proposal may be presented to the TAR is also provided.

PROPOSAL

Background

4. DI (G) OPS 02-2 (*Defence Aviation Safety Program*) states that the TAR is responsible to the Defence Aviation Authority, for the development of a regulatory framework for technical airworthiness management. The risk and flexibility of Defence's airworthiness management system is articulated in AAP7001.048 (*ADF Airworthiness Manual*), stating that the "... outcome of effective airworthiness management is that aircraft are operated in their intended roles and environments with acceptable risk to the lives of the aircrew, other ADF members and the public. The level of risk accepted for military operations, even during peacetime, will often exceed that allowed by civil authorities, and during conflict is a variable to be managed in light of the military situation". By definition, the application of System Safety¹ principles and practices provide a pragmatic, technically orientated framework to provide a robust systematic approach to risk management.

5. The TAREGs currently do not **specifically regulate**² a requirement for System Safety. However, a clear intent of the TAREGs is to optimise the *safety* of aircraft in all their intended roles. Further, AAP7001.054 Section 2 Chapter 1 (*System Safety*) provides extensive guidance on the TAR's preferred engineering management principles to be applied in determining and managing the level of technical risk.

¹ System Safety: The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle (ref: MIL-STD-882C).

² The Australian Defence Contracting (ASDEFCON) suite of tendering and contracting templates does, however, provide System Safety solicitation documents and contracts for acquisition by Defence.

6. The TAR now proposes to formally regulate system safety. There are numerous reasons for this decision, including the following:

- a. System safety is specifically regulated (or formally specified) by numerous National Airworthiness Authorities and regulatory agencies around the world, including the FAA, CASA, EASA, US Military Forces and UK MoD. There is a strong case that system safety represents best practice, and therefore warrants more than simply 'informal' adoption by the ADF;
- b. A well-constructed system safety program provides a strong contribution to safety, by ensuring that aircraft hazards are comprehensively identified and managed, and are subjected to periodic re-assessment. By regulating system safety, the associated compliance assurance program will strengthen the effectiveness of aircraft hazard management; and
- c. There has been a strong demand from some AEOs and POs for system safety regulation, to formalise their extant system safety efforts and assist them in further evolving their programs.

7. Summarised, inclusion of the proposed System Safety TAREGs will better align the ADF technical airworthiness regulatory framework with world's best practice, strengthening the effectiveness of existing measures through the provision for additional robustness in the approach to technical airworthiness risk management. Implementation of the proposed System Safety TAREGs is expected to be readily embraced, given that the majority of AEOs and POs have already implemented the existing TAR-sponsored System Safety guidance in AAP7001.054.

Objective

8. This NPRM proposes the addition of new TAREGs and the inclusion of System Safety Guidance (Section 3 Chapter 22) in AAP7001.053. The proposed amendments formally establish the requirement for System Safety Programs for all aerospace AEOs and POs involved in the design, development, acquisition and management of aircraft. Further, the System Safety TAREGs will align with the TAR's preferred System Safety design standards and practices as documented in AAP7001.054.

9. Some of the notable objectives of a System Safety program are to ensure that:

- a. safety goals consistent with world's best practice are established and documented;
- b. a safety management framework that clearly articulates the **risk level** to appropriate management authorities is established, implemented and maintained;
- c. safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner;
- d. hazards are identified, analysed, evaluated and eliminated or the associated risk reduced to a level acceptable to the applicable management authority throughout the life cycle of a system;
- e. hazards identified in-service are evaluated against established safety goals;
- f. hazard elimination/reduction is formally documented;
- g. pragmatic risk treatments are well thought out and considered;

- h. historical safety data, including lessons learned are continually assessed, considered and used;
- i. safety is not ensured by a reliance on Design Standards alone³.

Outcome

10. The outcome of this NPRM process will be the development and promulgation of System Safety regulations and guidance.

New or Amended Regulations

11. The proposed System Safety TAREGs are included at annex A. The proposed System Safety guidance is included at annex B.

HOW TO SUBMIT COMMENTS ON THIS NPRM

Format

12. Responses to this NPRM are to be recorded on the NPRM Response Sheet included at annex C, and as published on the DGTA-ADF Intranet and Internet websites.

13. Responses are to be submitted by email to DGTA-ADF.NPRM@defence.gov.au. Hardcopies of the NPRM Comment Sheet are not required.

Timing

14. Comments to NPRM DGTA 03-11 are to be received by close of business 30 Nov 11.

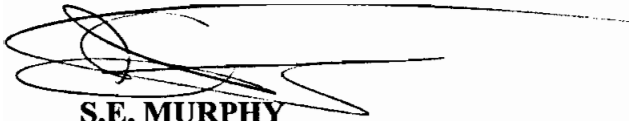
Additional Information

15. Additional information concerning this NPRM is available from SQNLDR Jason Dean OIC SCI3-DGTA on 03 9256 3711 or Jason.dean2@defence.gov.au.

³ Requiring and meeting Design Standards **alone** does not always ensure a *safe* system. The application of System Safety principles and practices provide a **functional** methodology that removes 'stove piping' that may result from applying a solely standards based design approach to *safety*.

DISPOSITION OF COMMENTS RECEIVED

16. A Summary of Responses will be prepared and published at <http://intranet.defence.gov.au/dgta/> and <http://www.defence.gov.au/dgta/NPRM.htm>. DGTA-ADF will not individually acknowledge or respond to comments or submissions.



S.E. MURPHY

WGCDR

Director Aviation Regulation

Directorate General Technical Airworthiness – ADF

Tel: (03) 9256 3651

17 October 2011

Annexes:

- A. NPRM DGTA 03-11 - Proposed System Safety TAREGs
- B. NPRM DGTA 03-11 - Proposed System Safety TAREG Guidance
- C. NPRM DGTA 03-11 - Comment Sheet

NPRM DGTA 03-11

PROPOSED SYSTEM SAFETY REGULATIONS

Proposed additions to TAMM glossary

(Note: The following entries will be added to the glossary at the rear of the TAMM)

Hazard:	A condition which is a pre-requisite to a mishap.
Hazard Log:	Provides a closed loop hazard tracking system or database of all identified hazards.
Safety Assessment Report (SAR):	A comprehensive evaluation of the risk being assumed. It identifies all safety features of the system, design and procedural hazards that may be present in the system and specific procedural controls and precautions that should be followed.
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.
System Safety Engineering:	An engineering discipline requiring specialised professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated risk.
System Safety Management:	A management discipline that defines System Safety Program (SSP) requirements and ensures planning, implementation and accomplishment of system safety tasks and activities consistent with the overall program requirements.
System Safety Program:	The combined tasks and activities of system safety management and system safety engineering.
System Safety Program Plan (SSPP):	A description of the planned tasks and activities to be used to implement the required system safety program. This description includes organisational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

Proposed changes to TAREG 2.2.3

(Note: The extant TAREG text is in black. The new System Safety TAREGs are in red)

2.2.3. Issue of a Design Acceptance Certificate for New Aircraft or Major Changes

- a. Except as otherwise authorised by the TAR, the DAR must only issue a Design Acceptance certificate for an aircraft type being acquired for ADF operations or one which has undergone a major design change, if he has ensured that:
 - (1) the Design Acceptance strategy has been documented in accordance with Annex A;
 - (2) TAR endorsement has been obtained for ADF Statements of Requirements (SORs) before inclusion as part of a formal instrument for the acquisition and related engineering services referenced in the Design Acceptance strategy, as provided in TAREG 2.2.4;
 - (3) any amendments to the TAR endorsed ADF SOR:
 - (i) have been approved by the DAR where there was no reduction in the level of safety established by the airworthiness standards of the ADF SOR, or
 - (ii) have been endorsed by the TAR or a relevant ASR where there was a reduction in the level of safety established by the airworthiness standards of the ADF SOR.
 - (4) the design agency or agencies providing aircraft engineering services to the Commonwealth for the acquisition have achieved and maintained AEO status relevant to the services provided for the duration of the engineering activity;
 - (5) the design agency or agencies have submitted:
 - (i) a list of all identified OHS risks, together with an associated risk management plan;
 - (ii) a Type Record in accordance with TAREG 2.2.9;
 - (iii) a Design Approval certificate in accordance with TAREG 3.4.3;
 - (iv) test reports, calculations and other Type Design data necessary to show compliance with the ADF SOR;
 - (v) Instructions for Continuing Airworthiness as required by the applicable airworthiness standards;
 - (vi) flight manual documents as required by the Operational Airworthiness Regulator (OAR) and applicable airworthiness standards;

- (vii) an Aircraft Structural Integrity Management Plan (ASIMP) and Engine Structural Integrity Management Plan (ESIMP) as required by the applicable airworthiness standards;
 - (viii) a Software Management Plan covering in-service management of software as required by TAREG 3.5.3;
 - (ix) a System Safety Program Plan;
 - (x) a Safety Assessment Report; and
 - (xi) a Hazard Log.
- (6) an examination of the Type Design has been conducted and all compliance findings completed in accordance with TAREG 2.2.11 and that:
- (i) the Type Design and the product are found to meet the prescribed airworthiness standards of the ADF SOR or provide an equivalent level of safety;
 - (ii) any airworthiness issues identified through the course of Design Acceptance activities have been processed in accordance with TAREG 2.2.11; and
 - (iii) no feature or characteristic of the aircraft makes it unsafe for its intended operations.

Proposed changes to TAREG 2.4.1

(Note: The extant TAREG text is in black. The new System Safety TAREGs are in red)

2.4.1. Service Release Submission and Recommendation

- a. The DAR seeking a TAR recommendation for Service Release must submit evidence that:
 - (1) a Supplemental Type Certificate (STC) or AMTC has been or will be issued;
 - (2) a DAR has been delegated responsibility for the Design Acceptance of the aircraft following Service Release;
 - (3) an AEO is in place to provide CI management of the aircraft in accordance with TAREG 3 following Service Release, including the establishment of a suitable Design Support Network;
 - (4) appropriate Aircraft and Engine Structural Integrity Management systems are in place for the aircraft in accordance with TAREGs 3.5.4 and 3.5.5;
 - (5) a Maintenance Support Network (MSN) including Approved Maintenance Organisations (AMOs) has been established;
 - (6) all identified OHS risks have been documented, together with an associated risk management plan;

- (7) all OHS risks have been assessed, where appropriate making reference to OHS information from a competent authority and appropriate treatments have been implemented;
 - (8) a Software Integrity Management System covering in-service management of software is established as required by TAREG 3.5.3; and
 - (9) the in-service management of System Safety is established.
- b. The DAR is entitled to a Service Release recommendation from the TAR if the TAR is satisfied that the evidence submitted in accordance with Paragraph a. supports such a recommendation.

Proposed changes to TAREG 2.5.6

(Note: The extant TAREG text is in black. The new System Safety TAREGs are in red)

2.5.6. Design Acceptance for Minor Changes to Type Design

- a. Except as provided under TAREG 2.5.9, the DAR must provide a Design Acceptance certificate to record the Design Acceptance of minor changes to an aircraft or aircraft equipment Type Design prior to the grant of Incorporation Approval in accordance with TAREG 3.5.12.
- b. The DAR must only provide a Design Acceptance certificate for a minor change to Type Design for a design change originating from an AEO if:
 - (1) the DAR is satisfied that the AEO certification is relevant to the services provided for the duration of the design activity;
 - (2) the AEO has verified to the satisfaction of the DAR that the design change complies with:
 - (a) the relevant ADF SOR prescribed in accordance with TAREG 2.5.7, and
 - (b) airworthiness standards prescribed in accordance with TAREG 2.5.8.
 - (3) the AEO has:
 - (a) provided a Design Approval certificate for the design change as required by TAREG 3.4.3;
 - (b) provided copies of such design data as the DAR may require in determining the acceptability of a design;
 - (c) conducted System Safety in accordance with TAREG 3.7.1;
 - (d) documented all identified OHS risks, together with an associated risk management plan; and
 - (e) assessed all OHS risks, where appropriate making reference to OHS information from a competent authority and implemented appropriate treatments.

- c. The DAR must only provide a Design Acceptance certificate for a minor change to Type Design for a design change originating from a non-AEO if:
 - (1) the DAR is satisfied that the design is applicable to the ADF's configuration, intended roles and environment for the aircraft or aircraft-related equipment, and either:
 - (a) the design has been previously approved by the NAA of a recognised country or by a recognised military force as defined in TAREG 2.2.7, or
 - (b) the DAR is satisfied that:
 - i. the design complies with airworthiness standards prescribed in accordance with TAREG 2.5.8;
 - ii. the source of the design change data is reliable and of acceptable quality;
 - iii. the original customer for the design services and intended application for the design change is known; and
 - iv. the design was approved by the aircraft or aircraft-related equipment Original Equipment Manufacturer (OEM) or other established supplier of engineering services of acceptable quality.
- d. If a design change, assessed in accordance with Paragraph b. and c., requires additional design effort to adapt the design for ADF purposes, or substantial additional verification activity to demonstrate the airworthiness or applicability of the design change for ADF purposes, then the required design activity must be conducted by a suitable AEO and a Design Approval certificate provided in accordance with TAREG 3.4.3 prior to Design Acceptance certification.

Proposed changes to TAREG 3.4.1

(Note: The extant TAREG text is in black. The new System Safety TAREGs are in red)

3.4.1. Design Control System

- a. For the purposes of this regulation, design must mean the design of a product (component or item), a design change or design service performed for another AEO.
- b. Each applicant for the issue of an EAC must establish a design control system to:
 - (1) control and verify designs to ensure that specified requirements are met, and
 - (2) ensure that all design decisions are documented and recorded.
- c. The design control system must include procedures to ensure that:
 - (1) data is controlled as provided in TAREG 3.4.2;

- (2) appropriate development plans are prepared for each design project and those plans:
 - (i) include a requirement to conduct an OHS risk analysis;
 - (ii) describe or reference all design activities, including Judgement of Significance, design development, Design Review and Design Approval;
 - (iii) assign responsibility for their implementation to competent, authorised individuals equipped with adequate resources;
 - (iv) are approved by the person who is to approve the design, prior to commencement of the design project; and
 - (v) are updated as necessary as the design evolves.
- (3) organisational and technical interfaces between different groups are defined and the necessary information is documented, transmitted and regularly reviewed;
- (4) Hazard Management, via the application of System Safety, is applied to every design activity.
- (5) a Judgement of Significance is performed for every design activity, including substitutions, modifications and deviations in accordance with TAREG 3.4.5;
- (6) design specifications, including applicable statutory or regulatory requirements, are reviewed to ensure:
 - (i) all requirements and methods of verification are adequately defined and documented;
 - (ii) airworthiness standards as defined in TAREG 2 are adequately specified;
 - (iii) the application of System Safety; and
 - (iv) incomplete, ambiguous or conflicting requirements are resolved with the sponsor AEO or DAR as appropriate;
- (7) design output:
 - (i) is documented and expressed in terms that can be verified against specified requirements;
 - (ii) meets the design input requirements;
 - (iii) contains or makes reference to Design Acceptance criteria;
 - (iv) identifies those characteristics of the design crucial to the safe and proper functioning of the product including requirements for operation, storage, handling, maintenance and disposal; and
 - (v) is subject to review by authorised persons as provided in TAREG 3.4.4 prior to release.

- (8) design verification:
 - (i) measures meet specified requirements, and
 - (ii) measures and results are recorded.
- (9) Design Approvals are issued as provided in TAREG 3.4.3;
- (10) design activities are performed only by authorised personnel as provided in TAREG 3.3.2;
- (11) for commercial applicants, each design activity to be performed on behalf of the applicant's organisation by a subcontractor:
 - (i) is identified in the applicant's EMP as provided in TAREG 3.2.8; and
 - (ii) complies with the systems and procedures in the applicant's EMP and with the specified requirements for the design activity.

Proposed new TAREG 3.7.1

(Note: The extant TAREG text is in black. The new System Safety TAREGs are in red)

3.7.1. System Safety

- a. The application of System Safety must ensure:
 - (1) a System Safety Program Plan (SSPP):
 - (i) is issued by the SDE and approved by the TAR for ADF organisations;
 - (ii) is issued by a commercial SDE and approved by the Sponsor AEO for commercial organisations;
 - (iii) has any amendment resulting in a change to safety approved by the relevant authority as per (i) and (ii) above, and
 - (iv) is regularly reviewed at intervals not exceeding two years.
 - (2) a System Safety Group meeting:
 - (i) is convened with Stakeholder participation in safety risk management activities,
 - (ii) is chaired by the DAR or authorised delegate, and
 - (iii) is conducted at least annually.
 - (3) a Safety Assessment Report:

- (i) is produced, in accordance with TAR specified standard and time throughout the life of the aircraft.
- (4) a Hazard Log
 - (i) is produced, in accordance with TAR specified standard and time, used and updated throughout the life of the aircraft.
- (5) all Residual Risks
 - (i) must be initially accepted by the relevant acceptance authority in accordance with the approved SSPP, and
 - (ii) must be re-accepted annually by the relevant acceptance authority in accordance with the approved SSPP.

The following guidance is proposed to be inserted into AAP7001.053(AM1) Section 3 Chapter 22 as follows

SECTION 3

CHAPTER 22

SYSTEM SAFETY REGULATION GUIDANCE

Applicable Regulation:

TAREG 3.7.1 System Safety

INTRODUCTION

1. *System Safety* is defined in MIL-STD-882C as ‘The application of engineering and management principles, criteria, and techniques to optimize the safety of a system within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle’. The application of *System Safety* principles and practices to aircraft design therefore provides a systematic, pragmatic, technically orientated approach to risk management. These principles and practices also provide a functional methodology that helps remove ‘stove piping’ that may result from applying a solely standards based design approach to aircraft design. Figure 22-1 depicts the contribution that *System Safety*, when combined with a comprehensive aircraft certification basis and effective OH&S management, can make to aircraft safety.

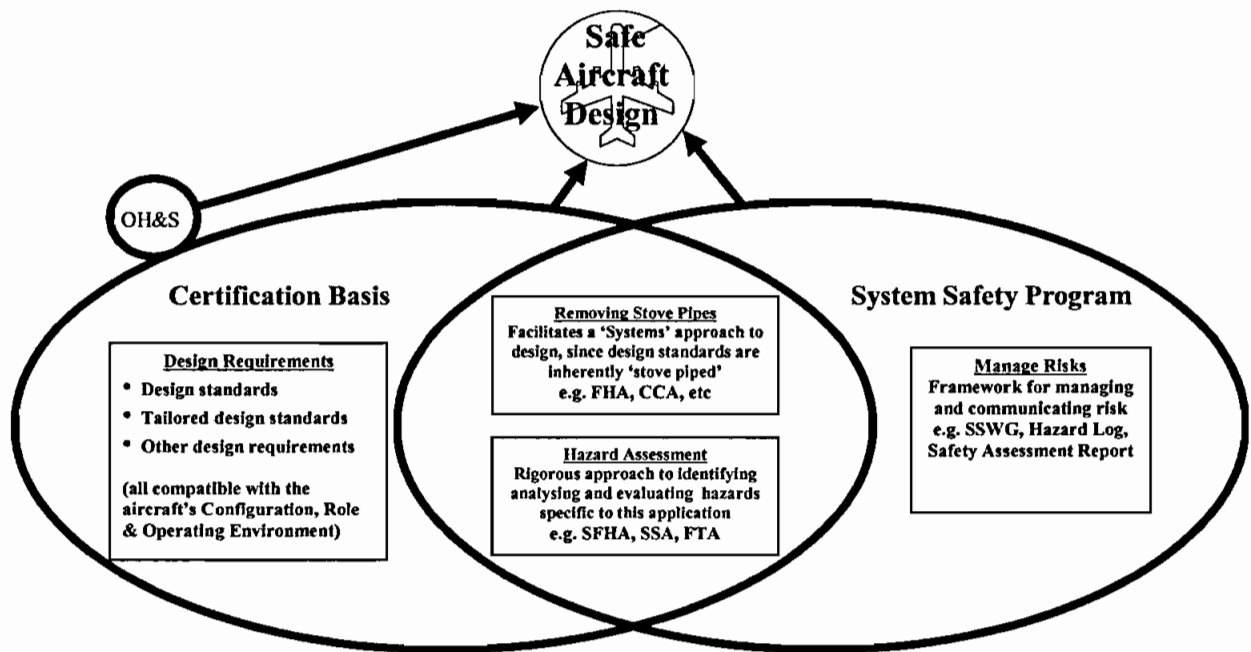


Figure 22-1 Achieving Safe Design of Aircraft

2. **System Safety Objectives.** The main objectives of a System Safety Program are to ensure that:

- a. safety goals consistent with world's best practice are established and documented;
- b. a safety management framework that clearly articulates the risk level to appropriate management authorities is established, implemented and maintained;
- c. safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner;
- d. hazards are identified, analysed, evaluated and eliminated or the associated risk reduced to an acceptable level throughout the lifecycle of a system;
- e. hazards identified in-service are evaluated against established safety goals;
- f. hazard elimination/reduction is formally documented;
- g. pragmatic risk treatments are appropriately considered;
- h. historical safety data, including lessons learned are continually assessed, considered and used; and
- i. safety is not assured by a reliance on design standards alone (as depicted in figure 22-1 above).

3. There are two key contributors to an effective System Safety Program, namely System Safety Engineering and System Safety Management. 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. System Safety Management is a management discipline that defines System Safety Program (SSP) requirements and ensures planning, implementation and completion of System Safety Engineering activities consistent with overall SSP objectives.

PURPOSE

4. The purpose of this chapter is to provide guidance on the application of *System Safety* within the Technical Airworthiness regulatory framework, by examining the following key elements of a successful System Safety Program:
- a. the System Safety Program Plan;
 - b. the System Safety Group;
 - c. the Safety Assessment Report;
 - d. the Hazard Log; and
 - e. the process for retention and management of residual risks.

SCOPE

5. This chapter is applicable to all aerospace AEOs and POs involved in the acquisition of new aircraft, or in the engineering management of in-service aircraft.

TAREG 3.7.1.a (1) – A System Safety Program Plan (SSPP)

Philosophy and Concept

6. **System Safety Key Concept.** *System Safety* aims to better disclose the technical risk inherent in an aircraft system, to promote informed risk treatment decisions. *System Safety* is implemented through a System Safety Program (SSP), as documented in a System Safety Program Plan (SSPP). No two SSPs will be identical, since the scope of the SSP is fundamentally linked to an aircraft's Configuration, Role and Operating Environment (CRE), as well as the current lifecycle phase. Indeed, it is the *System Safety* objectives that will decide the scope of SSP and documentation required, not the other way round. For example, during acquisition and modification projects, the overarching *System Safety* objective is to procure an aircraft with an acceptable level of safety, as defined in AAP7001.054(AM1) Section 2 Chapter 1. Once in service, the overarching *System Safety* objective is to ensure that the aircraft's inherent level of safety is at least maintained (preferably improved).

7. The SSP focuses on the identification and mitigation of aircraft system hazards (including consideration of missionised hazards - see paragraph 16 below) that impact airworthiness. This includes hazards directly and indirectly associated with the aircraft systems and their reliability, degraded states, failure modes, and complex interactions. All aircraft system hazards are composed of combinations of hardware, software and/or human factors causes; the omission of any one of these aspects will lead to a SSP that is only considering part of the overall hazard picture, and may therefore provide a false sense of safety. The SSP should therefore incorporate activities and analyses to predict and evaluate the inherent safety of each of these three elements in the integrated product. Hardware, software and human causal factors are examined further in the following paragraphs.

8. **Hardware Causal Factors.** Generally, the concept of hardware causal factors is well understood by aerospace engineers. *System Safety* provides a suite of processes and tools for analysing and evaluating hardware causal factors. These processes and tools are equally applicable to aircraft acquisitions and in-service support, and are covered in the various *System Safety* standards (eg MIL-STD-882C) and AAP7001.054(AM1) Section 2 Chapter 1.

9. **Software Causal Factors.** Historically, the analysis of software causal factors has either been overlooked or considered too late in the design cycle to have any real positive influence. However, aircraft designers are relegating more and more system functions to software, so 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. AAP7001.054(AM1) Section 2 Chapter 7 provides detailed guidance on the analysis and evaluation of software causal factors.

10. **Human Causal Factors.** Traditionally, human design requirements for aircraft systems are considered adequately through the use of commercial or military guidance documents, supplemented by Commonwealth human design and subject matter experts at DSTO, AOSG, AMAFTU, AVMED and operational squadrons. However, care must be taken when hazards are

analysed and mitigated on a per-hazard basis, particularly where the mitigations themselves also require human input (i.e. aircrew work-arounds, procedures, or training). After all, during a worst credible hazard scenario, a combination of hazards will probably be present. A Human Factors Workload Assessment on the integrated system will ensure average-skill aircrew can continue to safely fly and land the aircraft. Further information on human factors in aircraft system design and system integration activities is contained in AAP7001.054(AM1) Section 2 Chapter 13.

11. Summarised, System Safety requires an integrated approach to identifying, analysing and mitigating hazards due to hardware, software and human causal factors. The following paragraphs provide guidance on how to identify, analyse and mitigate these hazards.

12. Hazard Identification Guidance. The TAR does not mandate specific hazard identification analysis techniques for aircraft SSPs as each has its merits for specific applications, and is therefore dependent on circumstances. At a minimum, however, the use of an appropriate Hazard Identification Checklist should be employed as a starting point to broadly identify potential hazards. The DGTA-ADF internet website contains a generic aircraft Hazard Identification Checklist. For aircraft acquisition and major modification projects, a more rigorous approach to hazard identification will inevitably be warranted, and AAP7001.054(AM1) Section 2 Chapter 1 provides relevant guidance.

13. Hazard Analysis Guidance. Once again, 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. At a minimum, hazard analyses should consider hazards associated with the baseline aircraft system, and departures from that certified baseline. When considering the latter, hazard analyses should address hazards associated with:

- a. legacy aircraft systems;
- b. new and modified aircraft system's design, integration, maintenance, operation and disposal;
- c. the interface between new and legacy aircraft systems; and
- d. complex system interactions, including Common Cause (Common Mode, Zonal Safety Analyses and Particular Risk) Analyses.

For aircraft acquisition and major modification projects, where more complex systems and interactions are likely to be present, *System Safety* provides a range of processes and tools for hazard analysis. AAP7001.054(AM1) Section 2 Chapter 1 provides relevant guidance.

14. Hazard Mitigation and the System Safety Order of Precedence. A core element of a System Safety Program is an approved Hazard Risk Index (HRI) matrix, which provides a framework for promoting informed risk treatment decisions. Where a hazard is assessed as unacceptable, and therefore mitigation is required, engineers should pursue solutions, being mindful of the System Safety Order of Precedence. This concept recognises that some methods of mitigating hazards are often less effective than others, and therefore preference should be given to the most effective pragmatic solution. The order of precedence is as follows:

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

- b. incorporate safety devices to reduce the hazard risk to an acceptable level (e.g. automatic override on Terrain Following Radar), or
- c. provide warning devices to reduce hazard risk to an acceptable level (e.g. Ground Proximity Warning System audio and visual indications), or
- d. develop procedures and training to attempt to avoid the hazard (e.g. pilot verification required of the accuracy of automated weight and balance calculations).

15. Hazard mitigations should be documented, including the reason(s) why the higher order precedence solution (as listed above) was not implemented. Often, the incorporation of hazard mitigations will alter the probability rather than the severity of a mishap (i.e. the hazard will still cause a Catastrophic mishap, but its probability of occurrence may be reduced), however there are exceptions. Importantly, the least preferred of the four mitigation options (ie developing, procedures and training) should not be used as the sole mitigation for Hazard Severities involving the loss of life (typically Catastrophic and Critical severities IAW MIL-STD-882) due to the over reliance on Human Factors alone to prevent the loss of life.

16. **‘Missionised’ Hazards.** With few exceptions, aircraft systems on ADF aircraft have military-specific roles, including specialised wartime functions. Under hostile operational conditions, malfunction of these systems may have a more significant effect on safety than similar malfunctions under benign operational conditions. These additional military-unique hazards must also be managed via the System Safety Program. Further information on ‘missionised’ hazards is provided in AAP7001.054(AM1) Section 2 Chapter 1.

17. **SSP Audits.** SSP audits should be conducted within the context of on-going Commonwealth AEO or AMO audits required as part of periodical Engineering Management System or Quality Management System reviews. ADF and Contractor staff involved in aircraft acquisition or major modifications should refer to AAP7001.054(AM1) Section 2 Chapter 1 for further detailed guidance. Staff involved in Minor modifications and in-service support may also find this guidance useful.

Cross References

18. The following references are relevant to the requirements of this regulation:
- a. AAP7001.054(AM1) Section 2 Chapter 1, and
 - b. DGTA-ADF website.

Explanation and Amplification

19. **Clause (i).** The applicable ADF SDE must present the SSPP to the TAR for approval. The TAR will confirm that appropriate safety objectives have been established, and that the SSP will employ appropriate processes and tools for achieving those objectives. The TAR will also confirm the acceptability of the Hazard Risk Index matrix, since this is a key tool for managing hazards and informing risk treatment decisions. In-service SSPPs (ISSPPs) must be approved by the TAR prior to the system being introduced into service. SSPs for aircraft acquisition and major modification projects should be approved by the TAR prior to the commencement of design activity.

20. Clause (ii). The applicable commercial/contractor SDE must present the SSPP to the Sponsor AEO for approval. Similar criteria will be employed as described for clause (i) above, plus the sponsor AEO will confirm there is a consistent 'roll up/down' of safety objectives between organisations.

21. Clause (iii). Amendments to an SSPP resulting in a change to safety must be presented for approval by the relevant authority as identified in clauses (i) and (ii) above prior to formal release. Amendments subject to this clause would likely include changes to:

- a. the safety baseline i.e. safety goals/HRI matrix,
- b. the risk acceptance authority,
- c. the acquisition strategy,
- d. the fundamental nature, structure and roles of the System Safety Group, Safety Assessment Report, and Hazard Log,
- e. the in-service support strategy,
- f. any element of SSPP that would invalidate the TARs extant understanding of the SSP.

22. Clause (iv). The SSPP must be reviewed (assessed for adequacy) and appropriately maintained at an interval not exceeding two years. TAR/ADF approval is only required for amendments resulting in a change to safety as defined in clause (iii) above.

TAREG 3.7.1.a.(2) – A System Safety Group Meeting

Philosophy and Concept

23. The System Safety Group (SSG) is an essential element of a successful System Safety Program, since it facilitates communication and decision making between the operators, engineers and maintainers. The primary objectives of the in-service SSG are to:

- a. allow key internal and external Subject Matter Experts (both technical and operational) to discuss hazards and their mitigation options,
- b. review the SSP status, including results of technical or operational risk assessments of relevance,
- c. summarise hazard analyses including identified problems, status of resolution, and residual risk,
- d. develop and/or validate *System Safety* requirements and criteria applicable to the SSP,
- e. proactively identify safety program and platform deficiencies and provide recommendations for preventative action or re-occurrence as applicable,
- f. allow for the agreed mitigation of hazards as early as possible, and
- g. provide Commonwealth management with consensus recommendations on *hazards* and safety issues.

The SSG objectives for aircraft acquisition and major modification projects are similar to the above, but are tailored to focus on the early identification and management of emerging design issues that may impact safety. AAP7001.054(AM1) Section 2 Chapter 1 provides relevant guidance. Staff involved in minor modifications and in-service support may also find this guidance useful.

24. The SSG is particularly useful for gaining agreement of particular hazard mitigation strategies where only qualitative data and subjective opinions are available. 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. Each of these hazards 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.

25. For maximum effectiveness, SSGs need to include Defence and Contractor representatives from the following stakeholder groups: users (operations), engineering (including System Safety Engineering/management), maintenance, and, if required, OH&S. Further, these representatives need to be empowered by their parent organisations to either make decisions on the organisation's behalf, or to get priority endorsement/veto of SSG recommendations. An SSG charter should be created to establish aims, membership, agenda procedures, voting rights, and responsibilities, thus maximising SSG discussions towards achievement of the primary objective of hazard issue resolution. A sample SSG Charter is provided on the DGTA-ADF website.

Cross References

26. The following references are relevant to the requirements of this regulation:

- a. AAP7001.054(AM1) Section 2 Chapter 1, and
- b. DGTA-ADF website.

Explanation and Amplification

27. Clause (i). During aircraft acquisition, a SSG should be established as soon as practicable after contract signature, and certainly before the commencement of design activity. An in-service SSG should be established prior to the granting of AMTC and SR. An SSG Charter should be produced and maintained to detail how the meeting will aid in the conduct and closed loop monitoring of the System Safety Program. Stakeholders are those Defence and Contractor persons with a close association with safety considerations in design, integration, operation, maintenance and disposal of the system.

28. Clause (ii). Flexibility is afforded to the DAR in who will chair the SSG. Some DARs will elect to personally chair the group, to facilitate their involvement with an activity that directly contributes to aircraft safety. However, the DAR may authorise an appropriately knowledgeable system safety expert, normally the System Safety Manager, to chair the SSG. The chairperson must assign all action items and endorse the accuracy and completeness of the meeting's minutes. The DAR should approve the SSG minutes, regardless of who chairs the meeting.

29. Clause (iii). SSG meetings should be held as required, but at least once per year. Program complexity, operational/acquisition tempo, frequency of hazard log changes, etc, should all be drivers for SSG frequency. Typically, in-service platforms would normally warrant two to four

meetings per year. The frequency of meetings for major acquisition projects will generally be driven by project phase and activity.

TAREG 3.7.1.a.(3) – A Safety Assessment Report

Philosophy and Concept

30. The Safety Assessment Report (SAR) is a comprehensive evaluation of the safety risks being assumed prior to ADF operation of the system, typically via issue of an SFP or AMTC. It identifies the design and procedural hazards that may be present in the system and specific procedural controls and precautions that should be followed. In the ADF context the SAR is most useful when tailored to present a summarised, easy to read list of the noteworthy residual risks. SAR guidance is contained in DI-SAFT-80102B, which is available on the DGTA-ADF website. A SAR template, tailored to the ADF context, is also available on the DGTA-ADF website.

31. A Safety Case Report (SCR), as defined in MIL-STD-882C, may be employed in lieu of a SAR. A SCR is a well-reasoned summary document detailing what the original SSP aims were versus what was actually achieved (read compliance assessment), and a risk analysis (with recommendations) of the differences (read SAR). Generally, for in-service, the use of a Safety Case Report may not be required due to TAREGs 3.2.5 (Audits) and 3.3.9 (EMS Internal Evaluation System) fulfilling the ‘compliance assessment’ components of the SCR. In this case only a SAR will be required. However, for acquisition projects, the use of an SCR may be a useful approach. Further clarification on the purpose and use of an SCR and possible confusion surrounding the use of the UK MoD defined term ‘Safety Case’ is provided in AAP7001.054(AM1) Section 2 Chapter 1.

32. Noteworthy Residual Risks. Noteworthy residual risks are those residual risk levels requiring DAR or higher retention in accordance with the TAR-approved SSPP, i.e. typically these risk levels are those equivalent to MEDIUM and above as defined by MIL-STD-882C. The identification of noteworthy residual risks presents an easy and consistent method of focussing management attention, and therefore resources, on those areas of greatest safety concern.

Cross References

33. The following references are relevant to the requirements of this regulation:

- a. AAP7001.054(AM1) Section 2 Chapter 1, and
- b. DGTA-ADF website.

Explanation and Amplification

34. Clause (i). A SAR should be produced in accordance with DI-SAFT-80102B. For aircraft acquisition and major modification projects, a SAR must be produced prior to submitting an application for an SFP and/or AMTC/STC. Throughout the in-service phase of the aircraft lifecycle, the SAR must be updated to remain current, so that the Commonwealth remains cognisant of the noteworthy risks being retained. At a minimum, the SAR should be updated and presented as part of the submission to the annual Airworthiness Board (AwB), to facilitate an informed and independent review of all noteworthy risks being retained by the Commonwealth.

TAREG 3.7.1.a.(4) – A Hazard Log

Philosophy and Concept

35. Hazard Tracking. Hazards should be tracked throughout the aircraft's lifecycle, using a closed loop hazard tracking system or database of all identified hazards and their associated risks (ie a Hazard Log). All hazards identified during SSP analyses, whether during initial design or 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. At a minimum, the Hazard Log should include the following fields:

- a. a unique identifying reference number;
- b. a short title that captures the nature of the hazard (when and where 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 (e.g. test report, inspection, etc);
- i. confirmation that the residual risk has been accepted at the appropriate level, in accordance with HRI criteria (e.g. correspondence reference); and
- j. status of the hazard (open, closed or in-work with an expected close-out date).

36. Over the lifecycle of an aircraft, the Hazard Log can become a very large entity. For ease of oversight, the SAR may simply extract and summarise all noteworthy hazards, and hazards that have changed status since the last SAR update. AAP7001.054 contains further detailed information on the use and layout of a Hazard Log.

37. Hazard Closure. For a hazard to be 'closed', the Contractor and/or Commonwealth must 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. Further, the hazard's residual risk must be accepted, in writing, in accordance with agreed HRI sign-off levels. Further information on residual risk is provided in paragraphs 40–45 below.

Cross References

- 38.** The following references are relevant to the requirements of this regulation:
- a. AAP7001.054(AM1) Section 2 Chapter 1, and
 - b. DGTA-ADF internet website.

Explanation and Amplification

39. Clause a.(4).(i). A Hazard Log containing the information in paragraph 35 above must be produced for all ADF aircraft types, and managed throughout the lifecycle of the aircraft. For aircraft acquisitions, a Hazard Log should be produced prior to Preliminary Design Review and updated as soon as practicable after each hazard is identified. For aircraft entering in-service, the 'acquisition Hazard Log' must be transitioned to the responsible in-service agency/agencies to ensure in-service hazard management is performed. Further, transitioning the Hazard Log will ensure the Hazard Log remains as an historical status document for all hazards i.e. (closed, open or in-work). The provision for a Hazard Log must be established for in-service aircraft where no acquisition-produced Hazard Log exists or was transitioned. All identified hazards must be tracked throughout the aircraft's remaining lifecycle.

TAREG 3.7.1.a.(5) – All Residual Risks

Philosophy and Concept

40. Residual risk, in the context of an individual hazard, is the risk remaining when all agreed mitigation measures have been implemented. The level of authority required to accept residual risk is to be commensurate with the residual risk level. Further, to standardise the level of residual risk acceptance authority, DARs should not accept/retain a level of risk greater than that equivalent to MEDIUM (per MIL-STD-882C). Risk levels above MEDIUM (per MIL-STD-882C) should be transferred by the DAR (typically through the TAR) to the relevant Operational authority i.e. OAAR/OAA per the TAR approved SSPP for treatment. Use of an Issue Paper is an appropriate mechanism for capturing and communicating risk treatment where TAR and OAAR/OAA decisions are required.

41. Hazard Risk Index (HRI) Matrices. Robust technical risk management is fundamental to achieving the objectives of *System Safety* and larger TAMM intent of optimising safety with minimum constraint. RHI matrices are often an important tool in evaluating and communicating risk, but unfortunately the ADF has a myriad of different HRI matrices. While the TAR recognises the potential for confusion and difficulty in comparing risks across platforms, the TAR's preference is to continue to employ the 'parent' risk matrix that was created during the original aircraft design. This ensures consistent treatment of hazards throughout the aircraft's lifecycle, and also permits unambiguous communications with the aircraft OEM and other aircraft users.

42. Risk Communication. To promote unambiguous understanding within the SSG, participants should adopt the HRI likelihood and consequence levels, and resultant risk levels, as a common communications medium. However, this medium may not be suitable for communications with stakeholders outside the SSG. The following approach to external communications is suggested:

- a. ***Communicating to the operational fraternity.*** When communicating risks to the operational fraternity (eg operators outside the SSG, the OAAR/OAA and their staff, etc), Aviation Risk Management (AVRM) will likely be the preferred medium for communication. However, this translation must always occur as the penultimate step, after the completion of all technical assessments. Note that some engineering issues are not well suited to the AVRM tables, in which case qualitative (as opposed to quantitative) assessments are generally necessary;

- b. ***Communicating with other ADF members or external organisations.*** Without the proper context, HRI matrices can be meaningless (or worse, misleading). Accordingly, when communicating risks to members other than ADF operators or engineers, a qualitative description should be presented. The depth of the qualitative description will depend on the audience.

Cross References

43. The following references are relevant to the requirements of this regulation:
 - a. AAP7001.054(AM1) Section 2 Chapter,
 - b. Defence Aviation Safety Manual, and
 - c. DGTA-ADF website.

Explanation and Amplification

44. **Clause (i).** All residual risks must be initially accepted by the relevant acceptance authority in accordance with the applicable TAR approved SSPP. All Residual Risk acceptance must be formally documented and traceable.
45. **Clause (ii).** The Hazard Log and associated residual risks are dynamic. All noteworthy residual risks (refer to paragraph 32) must therefore be formally re-accepted annually by the relevant acceptance authority in accordance with the TAR approved SSPP. Annual residual risk re-acceptance will ensure appropriate management oversight of hazards is maintained and that the residual risk remains valid and the decision(s) for re-acceptance is pragmatic. For example, residual risk accepted on the premise of 'high operational importance' 12 months ago may no longer be valid if the operation has finished. Budget changes, technology advancements, organisational risk appetite, change in policy, and so on, may also affect residual risk retention.

SYSTEM SAFETY TRAINING

46. The following *System Safety* training is provided by DGTA-ADF:
 - a. **Technical Risk Management and System Safety Course (Awareness Course)** – This 1-day course is designed for managers and staff either not directly involved with SSPs, or with minimal involvement, and desirous of generic risk management and SSP concept exposure within the ADF context. This course is also ideally suited as a refresher course. The course will provide an overview of the tools and techniques commonly adopted in conducting *System Safety* engineering for aircraft; address the application of *System Safety* engineering processes to aircraft acquisition and in-service support; and provide familiarity with the ADF *System Safety* engineering requirements as they relate to technical airworthiness and risk management.
 - b. **ADF Aircraft System Safety Engineering Course** – This 5-day course is designed for Commonwealth or Contractor staff directly involved with SSPs, or in the review of related documentation. The course includes recent ADF aircraft accident statistics, basic system reliability analysis, risk management, human factors engineering, approaches to *System Safety*, relevant international and Australian standards, software systems safety and prescribed ADF requirements. The course will provide an intermediate level of understanding of the tools and techniques commonly adopted in

conducting *System Safety* engineering for aircraft; address the application of *System Safety* engineering processes to aircraft acquisition and in-service support; and provide familiarity with the ADF *System Safety* engineering requirements as they relate to technical airworthiness.

- c. **Advanced/Practitioner Course(s)** – Commonwealth and Contractor staff with frequent and in-depth involvement in *System Safety* should undertake advanced/practitioner course(s) to develop a detailed understanding of the application of all *System Safety* methodologies and tools. These courses will generally only be useful to a limited number of Defence personnel.

Further information on all courses is available on the DGTA-ADF website.

NPRM DGTA 03-11

COMMENT SHEET

Please return this response sheet by {insert date}, via email attachment to DGTANPRM@defence.gov.au.

Please indicate your acceptance or otherwise of this proposal by ticking the appropriate box below. Additional comments, suggested amendments or alternative action are welcome and may be provided on this response sheet or by separate correspondence.

- The proposal is **acceptable without change**.
- The proposal is **acceptable but would be improved if the following changes were made:**
- The proposal is **not acceptable but would be acceptable if the following changes were made:**

LSN	NPRM Reference: (i.e Regulation number, NPRM paragraph etc)	Comment or suggested change	Explanation
1			
2			
3			

RESOURCE IMPLICATIONS

Please provide specific comment on any significant resource implications that this proposal may have for your organisation, for both its implementation and ongoing compliance. Your comments should address both financial and human resource considerations.

Resource implications – Proposal implementation	
Resource implications – Proposal sustainment	

DRAFT

RESPONDENT DETAILS

Your name:	
Submission date:	
Your organisation:	
Email address:	
Postal address:	
Phone:	
Whose views are represented in your response? i.e. Is your response the authoritative response from your organisation?	Responding on behalf of : Individual [<input type="checkbox"/>] ADF AEO/AMO [<input type="checkbox"/>] Commercial AEO/AMO [<input type="checkbox"/>] Wing HQ [<input type="checkbox"/>] Group HQ [<input type="checkbox"/>] ADF Regulatory, Technical or Logistics policy agency [<input type="checkbox"/>] Other commercial entity [<input type="checkbox"/>], Other [<input type="checkbox"/>] Please describe:-
Consent to publish your name as an NPRM respondent within the DGTA-ADF Summary of Responses:	YES [<input type="checkbox"/>] NO [<input type="checkbox"/>]