



COMPARISON OF DEFENCE STANDARD 00-56
AND ARP 4761 / 4754*

ASSC/330/6/2 – Issue 1

* This report is published by the Avionic Systems Standardisation Committee (ASSC) to advance the role of standardisation in avionics. The use of this is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom is the sole responsibility of the user. Copies of this paper are obtainable from the ASSC Agency as an Avionic Systems Standardisation Committee publication.

Contents

	Page No.
1. Introduction	4
1.1 Background	4
1.2 Objective of Task	4
1.3 Previous Studies	5
2. Compatibility of the Methods	5
2.1 Introduction	5
2.2 Assessment Approach	6
2.3 Overview	6
2.4 Risk Levels	7
2.5 Integrity Levels	12
3. Guidance	16
3.1 Introduction	16
3.2 Table Of Contents	16
4. Conclusions	20
5. References	22

Abbreviations List

ALARP	As Low As Reasonably Practicable
ARP	Aerospace Recommended Practice
DAL	Development Assurance Level
Def Stan	Defence Standard
DERA	Defence Evaluation and Research Agency (Now QinetiQ)
FAA	Federal Aviation Regulations
FMECA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
IEC	International Electrotechnical Commission
JAA	Joint Aviation Authority
JSP	Joint Service Publication
PHA	Preliminary Hazard Analysis
SIL	Safety Integrity Level

1. Introduction

1.1 Background

The avionics industry has an array of standards in place to ensure safety and enable the setting of integrity levels for systems and aircraft. The high cost of aircraft and the shrinking military budgets mean that it is no longer practicable to build some aircraft (e.g. transports) only for the military market. Furthermore the need to sell aircraft in the global market where standards apply on both a national and international basis means some form of ‘standards’ harmonisation is required if global sales are to be achieved on a cost effective basis without safety being compromised.

Defence Standard (Def Stan) 00-56 (Ref 1) defines the safety programme requirements for defence systems. It specifically defines the safety programme management procedures, analysis techniques and safety verification activities applicable during the project lifecycle. Whilst compliance with the standard is mandatory it recognises that safety is system dependant and as such allows for the standard to be “adapted to suit the particular system implementation”. Def Stan 00-56 considers the system aspects with more detailed hardware and software issues being addressed in Def Stan 00-54 (Ref 2) and Def Stan 00-55 (Ref 3) respectively.

The Aerospace Recommended Practice (ARP) standards ARP 4754 (Ref 4) and ARP 4761 (Ref 5) were produced to provide guidance on how to achieve compliance with the Federal Aviation Regulations (FAR) and the Joint Airworthiness Requirements (JAR) for large fixed wing aircraft. The ARPs are therefore written in the context of FAR/JAR Part 25. ARP 4754 identifies a conceptual process, assurance levels and the deliverable's from each part of the process whilst ARP 4761 gives guidance on the detailed techniques that may be employed to generate the deliverable's. As with Def Stan 00-56 the emphasis in ARP 4754 is on the system aspects with the detailed hardware and software aspects being deferred to RTCA DO-254¹ (Ref 6) and RTCA DO-178B² (Ref 7) respectively.

1.2 Objective of Task

The objectives of this task were to extend the work done by DERA to determine whether ARP 4754 and ARP 4761 could provide a model for a guidance document on the application of Def Stan 00-56 to military avionic and weapons systems and if so to provide an outline for such guidance.

There was an implication that if this were possible then it might be possible to make a claim that a system built to ARP 4754 complied with requirements of Def Stan 00-56. Put another way the

¹ Design Assurance Guidance for Airborne Electronic Hardware.

² Software Considerations in Airborne Systems and Equipment Certification.

implication might be that, with some qualification, civil aircraft standards could be applied to military aircraft projects.

1.3 Previous Studies

A comparison of safety related software standards was carried out by York Software Engineering³ (YSE) and distributed under ASSC reference ASSC/330/3/425 (Ref 8). The YSE report compares three standards, International Electrotechnical Commission (IEC) 61508 (Ref 9), RTCA DO-178B and Def Stan 00-55. It was felt that this document was biased too far towards software issues to be of value at this higher 'system' level requirement.

A second standards comparison, this time of Avionics Standards, was carried out by DERA Malvern⁴ (now QinetiQ) and distributed under ASSC reference ASSC/330/2/167 Issue 2 (Ref 10). This report primarily considered ARP 4754 against Def Stan 00-56. This document was used as a starting point for this report.

This report draws on the findings of the previous comparison of avionics standards which was undertaken by DERA Malvern (Ref 10) and aims to provide an example of a possible table of contents for a generic standard. This report is only an example and further refinement through expert discussion of the categorisations detailed will be required in order to refine the methodology.

2. Compatibility of the Methods

2.1 Introduction

The Joint Service Publications (JSP) 318 4th Edition (Ref 11- for aviation applications), JSP 430 (Ref 12 - for naval applications) and JSP 454 Issue 2 (Ref 13 - for land system applications) all require the application of the methodology outlined in the Def Stan 00-56 to be applied to all new Ministry of Defence (MoD) contracts. Indeed, some of the requirements are applicable where upgrades to legacy systems are procured. Def Stan 00-56 therefore has to support all UK defence requirements and as such is not aviation specific, applying equally to aviation, naval and land based systems irrespective of whether or not they contain weapons systems. As such Def Stan 00-56 is necessarily generic in its approach.

In contrast, ARP 4754, as its title suggests, is aimed very specifically at aviation (specifically large civil aircraft). The ARP documents provide a comprehensive aviation specific approach for implementing a safety process that should lead to the certification of an aircraft implying that the

³ Comparison of Standards for Safety Related Software Development – Dr A C Coombes CEng – YSE Ref.: CF171/3/53

⁴ A Comparison of Aviation Standards – C O Newton & CH Pygott

safety and integrity of that aircraft has been assured. The ARP documents provide guidance and explanation on all areas of civil aircraft safety assessment and assurance.

2.2 Assessment Approach

The DERA Malvern report identified seven main differences between the civil and military standards, these were:

- The procurement model.
- The status of the standards.
- Product versus process.
- Levels and values.
- Treatment of risk.
- Acceptance of formal methods.
- Treatment of COTS.

The DERA report did not consider the environment issue or any special requirements of military aircraft such as the need to carry weapons and operate continuously at high speed whilst at low level. These issues are not specifically referred to in the standards themselves but directly affect their content. It is therefore very important to recognise that, even when only considering aviation assets, that the platforms to which the standards apply operate in different environments and therefore the safety targets (and therefore standards) will differ.

The approach that this paper must therefore take is to abstract back to the common objectives of each standard and then compare the means of achieving them. Where there are differences it will then be necessary to try to identify a possible bridging solution.

2.3 Overview

Both standards set out to ensure that the asset, when brought into service is safe. The Def Stan goes further and requires consideration of the whole lifecycle from conception through to disposal. Both standards also require the system to be categorised and then establish what is required by virtue of that categorisation. Thus the top-level aim and the method of allocating requirements are essentially the same for both standards. The requirements detailed in ARP 4754 are more prescriptive than those outlined in Defence Standard 00-56, providing guidance on requirements, however unlike Def-Stan 00-56 they do not provide a structured methodology for calculating levels of system integrity. ARP 4754, is therefore more flexible in approach and enables greater scope for tailoring the analysis with regard to specific system and programme requirements. The main classification structure outlined by the ARP standards is detailed in Section 5.4 which describes the Development Assurance Levels (DAL's) and provides guidance on application and allocation. These like Safety Integrity Levels (SIL's) as prescribed by the Defence Standards provide an indication of the integrity of the system, however as detailed above they are not aircraft specific.

2.4 Risk Levels

The way the subject standards address the issue of Hazards and Risk is important with regard to a comparison of them. Any claim that one meets the requirements of the other would have to be in the context of them sharing common goals. The established aim of ARP 4754/4761 is to show compliance with FAR/JAR 25 whilst that of Def Stan 00-56 is to reduce the risks associated with all system hazards to a level that is ALARP. Initial inspection of these aims suggests they do not match well with the ARP having a fixed target and the Def Stan a less well defined one. However both establish requirements to deliver evidence to support their claims that is based on a combination of accident severity and the probability of that accident occurring (i.e. the risk associated). As a starting point it was therefore decided to compare how each standard establishes the risk level and whether there was some measure of similarity.

To do this it was initially necessary to "de-link" the nomenclature used to describe the assurance requirements of the standards and only consider how the standards require risk to be represented. Furthermore, in order to make informed judgements about any differences it was decided to compare other standards, namely Mil Std 882C and IEC 61508. Having included these two standards and carried out an initial review it was felt that in order to be fair the Air Traffic Services Standard SW01 (Ref 14) ought to be included also because its approach was similar to ARP 4754/4761.

Table 1 shows the comparison made. Three of the standards (Def Stan 00-56, Mil Std 882C and IEC 61508) classify the risk as a function of the severity of outcome against the predicted frequency of occurrence. The other two (ARP 4754 and SW01) only consider the severity of any possible outcome. Having established a 'level' (risk or outcome) all the standards then set a 'level' of achievement to be met (Development Assurance Level (DAL) for ARP and Safety Integrity Level (SIL) for Def Stan.

All the standards use similar terminology for describing the severities (e.g. Catastrophic is used by all as the worst outcome) though the definition of these terms does vary. Some standards quote definitive values to be achieved others give examples but leave the choice of value to the user. Thus whilst the outcome categorisation at this point is broadly in line in descriptive terms numerically there is the possibility of wide disparities as shown in Table 2 below.

The issue of levels is taken one step further in the ARP, Def Stan and SW01 with the consideration of architectural solutions. SW01 allows for the 'reduction' of its Assurance Evidence Levels (AELs) by as much as 4 levels based on the number of defensive layers and the probability of them being breached (see [xxxx](#)). The Def Stan allows for apportioning of system SILs where sub-system independence can be demonstrated and where the combinatory function has a specified integrity. The ARP takes a similar approach to the Def Stan but without considering any combining function.

		ARP 4754 & ARP 4761			Def Stan 00-56 <i>(is not mandated by 00-56 only suggested)</i>			Mil Std 882C			IEC 61508		
		FAA	JAA	4754/4761	Severity Description	Frequency (Risk of Occurrence)	Standard Descriptor	Outcome Description	Frequency (Risk of Occurrence)	Standard Descriptor	Severity Description	Frequency (Risk of Occurrence)	IEC 61508-5
Severity Description	Frequency (Risk of Occurrence)	Severity Description	Frequency (Risk of Occurrence)	Standard Descriptor	Severity Description	Frequency (Risk of Occurrence)	Standard Descriptor	Outcome Description	Frequency (Risk of Occurrence)	Standard Descriptor	Severity Description	Frequency (Risk of Occurrence)	Standard Descriptor
Highest Assurance Requirement	Catastrophic Extremely Improbable ($X < 10^{-8}$)	Catastrophic	Extremely Improbable ($X > 10^{-7}$)	DAL A	Catastrophic	Frequent, Probable or Occasional ($> 10^{-7}$, $X > 10^{-7}$)	RC: A	Catastrophic (Category I)	Frequent, Probable or Occasional ($> 10^{-7}$, $X > 10^{-7}$)	RCA	Catastrophic	Frequent, Probable or Occasional	RC: I
					Critical	Frequent or Probable ($> 10^{-7}$, $X > 10^{-7}$)	RC: A	Critical (Category II)	Frequent or Probable ($> 10^{-7}$, $X > 10^{-7}$)	RCA	Critical	Frequent or Probable	
					Marginal	Frequent ($X > 10^{-7}$)	RC: A	Marginal (Category III)	Frequent ($X > 10^{-7}$)	RCA	Marginal	Frequent	
	Severe Major Improbable ($> 10^{-5}$, $X > 10^0$)	Hazardous	Extremely Remote ($> 10^{-7}$, $X > 10^2$)	DAL B	Catastrophic	Remote ($> 10^{-7}$, $X > 10^4$)	RC: B	Catastrophic (Category I)	Remote ($> 10^{-7}$, $X > 10^7$)	RC: B	Catastrophic	Remote	RC: II
					Critical	Occasional ($> 10^{-7}$, $X > 10^5$)	RC: B	Critical (Category II)	Occasional or Remote ($> 10^{-7}$, $X > 10^7$)	RC: B	Critical	Occasional	
					Marginal	Probable ($> 10^{-7}$, $X > 10^6$)	RC: B	Marginal (Category III)	Probable or Occasional ($> 10^{-7}$, $X > 10^7$)	RC: B	Marginal	Probable	
											Negligible	Probable	
	Major Improbable ($> 10^{-7}$, $X > 10^7$)	Major	Remote ($> 10^{-7}$, $X > 10^7$)	DAL C	Catastrophic	Improbable or Incredible ($> 10^{-7}$, $X > 10^7$)	RCC	Catastrophic (Category I)	Improbable ($> 10^{-7}$, $X > 10^7$)	RCC	Catastrophic	Improbable	RC: III
					Critical	Improbable ($> 10^{-7}$, $X > 10^7$)	RCC	Critical (Category II)	Improbable ($> 10^{-7}$, $X > 10^7$)	RCC	Critical	Remote or Improbable	
					Marginal	Occasional or Remote ($> 10^{-7}$, $X > 10^7$)	RCC	Marginal (Category III)	Remote or Improbable ($> 10^{-7}$, $X > 10^7$)	RCC	Marginal	Occasional or Remote	
					Negligible	Probable or Occasional ($> 10^{-7}$, $X > 10^7$)	RCC	Negligible (Category IV)	Frequent or Probable ($> 10^{-7}$, $X > 10^7$)	RCC	Negligible	Probable or Occasional	
	Minor Probable ($X > 10^7$)	Minor	Reasonably Probable ($> 10^{-7}$, $X > 10^7$)	DAL D	Critical	Incredible ($> 10^{-7}$, $X > 10^7$)	RC: D	Negligible (Category IV)	Occasional, Remote or Improbable ($> 10^{-7}$, $X > 10^7$)	RC: D	Catastrophic	Incredible	RC: IV
			Frequent ($X > 10^7$)		Marginal	Improbable or Incredible ($> 10^{-7}$, $X > 10^7$)	RC: D				Critical	Incredible	
											Marginal	Improbable or Incredible	
											Negligible	Remote, Improbable or Incredible	
Lowest Assurance Requirement	No Safety Effect all	No Safety Effect	all	DAL E	Negligible	Remote, Improbable or Incredible ($> 10^{-7}$, $X > 10^7$)	RC: D (SIL 1)						

Table 1 – Comparisons of risk categorisations

Standard	Objective	1	10 ⁻¹	10 ⁻²	10 ⁻³	10 ⁻⁴	10 ⁻⁵	10 ⁻⁶	10 ⁻⁷	10 ⁻⁸	10 ⁻⁹	10 ⁻¹⁰	10 ⁻¹¹	10 ⁻¹²
IEC 61508	Failure on demand													
Low demand	Failure on demand	Not defined	SIL1	SIL2	SIL3	SIL4	Not Defined							
High demand or continuous	Failure per hour		Not Defined				SIL1	SIL2	SIL3	SIL4	Not Defined			
Mil Std-882C	Failure per flight	Frequent	Probable	Occasional	Remote		Improbable							
Def Stan 00-56	Failure per operating hour	Frequent	Frequent	Probable	Probable	Occasional	Remote	Remote	Improbable	Improbable	Incredible			
ARP 4754 (FAR)	Failures per flight hour	Probable			Probable		Improbable							
ARP 4754 (JAR)	Failure per flight hour	Frequent	Frequent	Reasonably Probable	Remote	Remote	Remote	Extremely Remote	Extremely improbable					
SW-01 *	Failures per operating hour	AEL 1	AEL 2	AEL 3	AEL 4	AEL 5								

* SW-01 does not give any figures. The values here are the author's extrapolation in the 'AEL Offset' table contained in SW-01.

Table 2 : Comparison of Frequencies

Reduction of AEL	-1	-2	-3	-4
Characteristic				
Number and strength of defensive layers	Requirement is monitored	Requirement is met independently in a redundant channel	At least two forms of mitigation which are not part of the requirement	Many forms of mitigation such that a failure of the requirement is extremely unlikely to result in the hazard
The probability of the failure of all architectural and operational defences	$10^{-2}/\text{hr}$	$10^{-3}/\text{hr}$	$10^{-5}/\text{hr}$	$10^{-7}/\text{hr}$

Table 3 : SW01 – AEL Offsets due to Architectural and Operational Defences

Level	Implemented by:			Combinator (where appropriate)
	Component 1	Other components		
S4	S4	None	None	None
	S4	S2*	S4	S4
	S3*	S3*	S4	S4
S3*	One or more S3*			
S3	S3	None	None	None
	S3	S1*	S3	S3
	S2*	S2*	S1	S1
S2*	One or more S2*			
S2	S2	None	None	None
	S1*]S1	S2	S2
S1*	One or more S1*			
S1	One or more S1*			

Table 4 – Def Stan 00-55 Apportionment of Safety Integrity Levels⁵

⁵ The ‘*’ marking indicates the strict requirements for independence that shall be maintained between the components through specification, design, development and maintenance. A component shall be deemed independent only if it is conceptually different from and relies on different design properties from all the other components. Components with common specifications or subcomponent types shall not be deemed to be independent.

2.5 Integrity Levels

The main difference between the ARP and Defence Standard 00-56 is with regard to the setting of integrity levels where there is a difference in terminology and application. The ARP standards outline the need for Development Assurance Levels (DAL's) whereas the Defence Standard provides a means of ascertaining a systems Safety Integrity Levels (SIL's). Although both standards provide guidance on methods of allocation and both processes are similar there are slight differences in approach which, could lead to differences in application both qualitatively and quantitatively making functional comparisons difficult.

In order to identify whether there is possible overlap between the standards, and more specifically whether the civil aircraft requirements from the ARP Standards could be used as a basis for an aircraft/avionic specific Defence Standard type methodology, the requirements detailed in both standards have been compared to ensure that both provide a comparable process of safety assessment.

The ARP Standards identify the following tasks with regard to the Safety Assessment Process:

- Functional Hazards Assessment.
- Preliminary System Safety Assessment.
- System Safety Assessment.
- Common Cause Analysis.
- Safety Related Flight Operations of Maintenance Tasks.

In comparison Defence Standard 00-56 provides a framework detailing the required method, which should be implemented through the life of a project to ensure that systems enter service with acceptable safety characteristics. The standard applies to all phases of the project lifecycle, from initiation through to disposal.

The mandatory activities required by Defence Standard 00-56 are outlined below:

Risk Class	Activities	Alternatives (by Agreement)
All	Preliminary Hazard Identification Preliminary Hazard Analysis (PHA) System Change Hazard Analysis	Modification of existing PHA where there is an incremental change in circumstances
All	Hazard Log Establishment	
All	Safety Review	
A,B or C	System Hazard Analysis System Risk Assessment	Design standards or rules safeguarding hazards identified in the PHA
A or B	Independent Safety Audit	

Both standards provide similar high level guidance and comparable methods, although the Defence Standard methodology is less specific. In addition the Defence Standard provides a high level-overarching framework by which a Safety Management process can be implemented. The standard is less comprehensive when dealing with the system levels safety process and doesn't give guidance on Availability, Reliability and Maintainability issues for example, which are included in ARP 4761 appendices D, E, and F. The Defence Standard refers to additional specific standards for the application of ARM calculations and studies and therefore, in order to determine whether the key requirements of the Defence Standards are comparable to the ARP standards, there needs to be agreement on the key safety processes which need to be conducted in order to provide assessment of aircraft. A possible example table of contents of such a guidance paper is provided in Section 3.2 of this report.

Both approaches follow a structured process in order to attain an accurate integrity level for the system, through the identification and quantification of the critical system functions. The definition of DAL's derived from the ARP standards deals primarily with the effect a failure would have on the aircraft or sortie and does not define in any depth specific human loss unlike Defence Standard 00-56 (See **Table 5**). Therefore, application of the ARP standard to military aircraft would result in severities being more aircraft and flight specific as opposed to the current definitions, which concentrate on human loss. An agreed standard definition for the main accident classes would enable easier understanding of the requirements and would enable dual application of the standards. It is anticipated that the UK MOD would be reluctant to follow the ARP civil approach of classifying severities with regard to their effect on operational aircraft characteristics as opposed to the specific human loss probabilities.

The primary differences arise during application where the two standards differ in the setting of integrity requirements and the allowable required level of mitigation and risk reduction. The ideology of the Defence Standard methodology is similar to the ARP standards although the latter requires a less quantitative approach. The allocation of risk and the risk classes provided by the two standards provides the most difficult area for standardisation of integrity allocation. Although both standards provide a framework for assessing and ensuring system integrity as has been previously mentioned, the two integrity ranking methods are reliant upon application to ensure that both have been assessed using the same base line.

Differences in terminology and impetus between the two standards, with regard to risk reduction may also have an affect the integrity level applied to a system. The general practise advocated by Defence Standard 00-56 to reduce risk, is to apply the ALARP principle, which details acceptable levels of risk and highlights the boundaries where further risk reduction may be required. The Defence Standards place reliance upon the ALARP, principle where risks must be reduced to a tolerable level. The ARP standards do not include reference to the ALARP or a similar principle and instead require reduction of risk to an acceptable level. This is a clear difference between the two approaches due to the fact that ALARP, which is mandated that risk is mitigated to a point where no further mitigation is viable be applied, therefore providing a system assessment where all risks have been individually assessed and reduced as much as is possible. This differs to the requirement that risks be reduced to an

acceptable level, which infers that a safety level or target is set and once that level has been reached no further reduction is required even if the ALARP principle would require further mitigation. This issue of risk reduction raises the problem, what is considered acceptable for civil aircraft may not be acceptable for military aircraft. Therefore an acceptable means and method for risk reduction needs to be applied to enable the application of a civil standard to military aircraft to ensure compliance with the ALARP principle.

The report undertaken by DERA (Ref 10) identified the primary differences between the two approaches, and suggested that the key requirement is for a universal definition of integrity levels to be agreed, taking account of both ARP 4754 and Defence Standard 00-56. to enable easier and universal application of an aircraft specific integrity level, providing a standardised and uniform level of classifying the integrity of aircraft and aircraft systems.

Category	Definition	ARP 4761
Catastrophic	Multiple deaths.	All failure conditions, which prevent continued safe flight and landing.
Critical	A single death; and/or multiple severe injuries or severe occupational illnesses.	Large reduction in safety margins or functional capabilities. Higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely. Adverse affects on occupants.
Marginal	A single severe injury or occupational illness; and/or multiple minor injuries or minor occupational illnesses.	Significant reduction in safety margins or functional capabilities. Significant increase in crew workload or in conditions impairing crew efficiency. Some discomfort to occupants.
Negligible	At most a single minor injury or minor occupational illness.	Slight reduction in safety margins. Slight increase in crew workload. Some inconvenience to occupants.

Table 5: Table of Accident Severities

Table 1 of Defence Standard 00-56 provides details on the method of applying accident severities and provides quantified examples, which are more pessimistic than those provided in ARP 4761 Table 3.1-1. The values in Defence Standard 00-56 are provided only as examples of possible frequencies. On comparison of the banding for those probabilities rated improbable and incredible, the potential difference is less important due to the fact that generally very low probabilities do not contribute greatly to the resultant SIL or DAL allocation and it is impossible to accurately validate the probabilities. The main area where there may be a significant difference is in the probable and remote ranges where the example data provides a difference of 2 and 1 orders of magnitude. Therefore, a

DAL rated system, will generally have a higher rated integrity if the example frequencies have been applied, than a similar process using the Defence Standard frequencies.

It is noted that the association of qualitative (“Remote”, “Probable”, etc.) and quantitative probabilities as detailed in Defence Standard 00-56 is not fixed, but instead depends on the operational profile of the relevant system. Hence, direct comparison with the ARP where fixed probabilities are set is not straightforward.

DEF STAN 00-56 Table 1; Part 2		ARP 4761		Orders of Magnitude Difference
Probability	Quantification	Accident Frequency	Accident Frequency / Worst Case	
Frequent	10000×10^{-6} /operating hour	Frequent	1.000	2
Probable	100×10^{-6} /operating hour	Reasonably Probable	1.000E-03	1
Occasional	1×10^{-6} /operating hour			
Remote	0.01×10^{-6} /operating hour	Remote	1.000E-05	3
Improbable	0.0001×10^{-6} /operating hour	Extremely Remote	1.000E-07	3
Incredible	0.000001×10^{-6} /operating hour	Extremely Improbable	1.000E-09	4

Table 6 : Frequencies

The probability range categories are the same for the two standards, however interpretation and applications may differ between the two approaches. The primary difference between the two approaches is the specific nature of the ARP standards, which are for application to civil aircraft. In contrast Defence Standard 00-56 provides definitions for accident frequencies which are then used in calculating the SIL level for the system.

Standardised terminology, probabilities of failure and periods of failure are required to ensure compliant system integrity level allocation. However, it should be noted that application of the ARP quantification may be applied to the Defence Standard methodology for calculating accident probabilities, due to the requirement that the quantification applied is correct and appropriate to the project and requirement.

3. Guidance

3.1 Introduction

Section 3.2 details an example of a possible table of contents, which could be included in a guidance document, which looks to provide generic aircraft safety assurance methods. A key requirement of the document should be that it is not too prescriptive and allows users and practitioner's sufficient flexibility to apply the processes suggested with specific regard to specific requirements. As requirements differ flexibility is essential to ensure that any guidance reports are sufficiently flexible to enable application across a range of aircraft.

Detailed below is an example and brief definition of the contents of a potential guidance methodology. In order to provide an accurate and appropriate methodology users and practitioners should be involved in the drafting of the document to ensure that the approach provides a workable method, which ensures that safety processes are adequately covered in the light of the requirements outlined in the ARP and Defence Standards.

3.2 Table Of Contents

Section 4 of this report contains an example of a possible table of contents for a guidance document.

A. Introduction

This should provide guidance on the method and an overview of the approach, which could be applied.

B. Scope and Applicability

The scope and of the standard should be outlined giving details on the platform specific requirements necessary to ensure safety of the system and compliance with the requirements of the standard. This section could provide guidance on the boundaries of the approach and which requirements are necessary. Possible areas of guidance could be:

- Domain
- System Boundaries
- System Interfaces
- Limitations
- Exclusions
- Configuration Baseline

C. Related Documents

Links to other source documents e.g. other relevant Defence Standards such as Defence Standard 00-55 or BS5760 (Reliability of systems and components).

D. Definitions

This should include a list of possible abbreviations and a glossary of terms.

E. Safety Requirements

Guidance on the method of determining safety requirements. The base tables from the report produced by DERA (Ref 10) may be used as an initial base for this section. The allocation of safety requirements will be derived from the hazard identification and risk assessment process.

F. Top Level Safety Target

The setting of top level safety targets will be a difficult subject to attain consensus on due to the varying flight profiles undertaken by different platforms and national and international requirements. In addition it may not be viable to set a uniform target for civil and military aircraft and therefore two targets may be needed. The current top-level safety targets set up in the Regulation Of The Airworthiness Of Ministry Of Defence Aircraft are detailed in JSP 318B, 4th Edition.

G. Management Safety Requirement

Guidance could be provided on how to review the safety activities to be carried out at each phase of the project, to provide a structure detailing how to ensure that:

- Newly identified hazards are incorporated in the hazard log.
- Appropriate risk assessments are carried out.
- Relevant tasks are completed in line with the drafted standard and other internationally agreed standards.
- Ensure compliance with safety audit.
- Hazards are mitigated appropriately.

H. Integrity Level

An agreed method of determining Integrity Levels, with a comparable method of quantifying system safety requirements. This should provide a means of assessing system integrity and include an means of ensuring compliance with ARP and Defence Standard SILs and DALs.

I. Human Error Probabilities

Here the definitions already outlined in Def-Stan 00-56 may be used, as there is no equivalent in the ARP Standards. However if following discussion and review more specific aircraft human error probabilities are available, then they may be included in the method replacing the generic Defence Standard probabilities. The means of quantifying human error is a contentious issue with most aircraft operators having access to historical data and ergonomic assessments. These tend to be platform specific and as such it is not considered viable to provide a catagoric list of human error probabilities, particularly due to the fact that each aircraft operates in different sortie profiles, particularly with regard to military and commercial aircraft. However the Def Stan approach

categorises defining the nature of the risk are considered sufficiently flexible to allow application to both military and commercial aircraft if appropriate probabilities are available.

J. Hazard Analysis

The purpose of the hazard analysis is to determine the relationship between hazards and accidents and to determine the associated risk of each hazard. A typical analysis could include the following steps:

- Assessment of the severity of each accident.
- Assessment of the severity of each hazard, normally the severity of the most severe accident which can result from the hazard.
- Analysis of the events leading from a hazard to an accident, known as the ‘accident sequence’, to determine the likelihood of a hazard leading to an accident.

Measures of both frequency will be required for hazard analysis. It is possible to use a quantitative approach with numerical frequencies and numerical assessment of deaths and injuries. However, more qualitative approaches, with categories of frequency and severity, as detailed in Defence Standard 00-56.

Accident sequence analysis to assess the likelihood of a hazard leading to an accident should take into account the mode of flight and type of aircraft and any other sources of information available to the pilot and the performance which can reasonably be expected from a trained pilot.

The methodology should also accommodate the provision of guidance on the creation and management of a hazard providing a safety record for the platform. This should include details of HAZOP methodologies. The hazard log shall hold itemised information derived, including but not limited to

- Hazard ID, which is a unique number to identify a hazard.
- Hazard description, which is a short but comprehensive description of the hazard.
- Hazard grouping.
- Hazard referencing.
- Hazard traceability, e.g. links to FTA etc.
- Details on how to deal with actions which have been planned but not yet carried out.
- Ensuring that all relevant hazards, even though ‘closed’ are reviewed in the event of changes etc.

K. Risk Assessment

Subsequent to the hazard identification and categorisation, further risk assessment activities will be carried out to show that all the intolerable risks have been removed and any tolerable risk identified has been reduced to as low as reasonably practicable (ALARP).

The purpose of Risk Assessment is to set targets for the occurrence of the hazards of the system. These targets are determined by consideration of acceptable levels of risk and the risk arising from each hazard.

Risk is defined as a combination of frequency and severity of an accident. The acceptability of risks is often reckoned in three categories: unacceptable, intermediate and acceptable. The importance of the risk assessment is to consider the cumulative risk, especially that arising from the intermediate category of risks. The cumulative risk needs to be taken into account when setting targets for the occurrence of each hazard and is one of the drivers for aircraft safety.

A generic structured checklist could be developed to enable practitioners to apply the method, including cross-references to the ARP and Defence Standards to enable reference to specific requirements if further clarification is required.

L. Project Lifecycle

The project lifecycles are similar in the two standards, however a generic framework should be provided, as an example.

M. Safety Lifecycle

The safety programme that will be followed by the project is compliant with the safety lifecycle described in Def Stan 00-56

N. Standards, Legislation and Regulation

This section could list appropriate standards and legislation which, may also need to be referred to.

4. Conclusions

The key requirement and benefit of developing a uniform method of classification would be the provision of a standard safety model by which to compare procurement options enabling manufacturers and system procurers to operate on a level playing. To this end the impetus of each of the standards needs to be understood and compared to ensure that any harmonisation or standardisation of classification does not make the assessment process either too rigorous, or onerous.

Section 2 outlines the key differences between ARP 4761 / 4754 and Defence Standard 00-56. It is clear that although there is some overlap between the two methods, it is not clear whether the civil aircraft specific ARP requirements are sufficiently robust to ensure compliance with the corresponding Defence Standard 00-56 methodology. One of the key differences between the two approaches is that current UK MOD requirements require a structured and uniform procedure for allocating SIL levels to systems to ensure the safety of all military systems. The ARP standards on the other hand are only applicable to civil aircraft and therefore the methodology has not been written for application to military aircraft taking account of specific development environments.

The report undertaken by DERA (Ref 10) identified the main differences between the two types of standards and concluded that it considered that the DAL's and SIL's were sufficiently flexible to be accepted as comparable. Although both provide four levels of integrity, it is the application of the standards, where some degree of discrepancy between DAL's and SIL's may arise. It is understood that the application of standards generally is reliant upon engineering judgement when it is being applied. However, in order to provide a degree of standardisation, in depth aircraft specific guidance on the application and implementation of safety principles for aircraft in accordance standards may prove useful if widely applied. This should provide generic guidelines on the implementation and assessment of avionics systems in accordance with national and international requirements and standards. As discussed in Section 1.1 both methods are comparable in impetus, however more difficult compare with regard to specific requirements.

The fundamental difference being the allocation of SILs and DALs. A key requirement is to determine whether the ARP quantification and method is sufficiently robust to be applied to military aircraft. As detailed in Section 2.4 a DAL A classification is not compatible with a SIL 4 system due to differences in definition. Indeed it is not possible to compare Failure Rates, Risk Classifications and Criticalities, due to significant differences in definition and application. Therefore it is not possible to state that a DAL A system is comparable to a SIL 4 system. A more viable option would be to compare the available safety evidence analysing the development processes and procedures adopted for system developed to both standards to identify correlation and deficiencies.

The ARP standards provide guidance on methods of ensuring that aircraft achieve certification, and as such they are very comprehensive in their scope and application. They are the preferred standards used by the French civil aviation industry. The Defence Standards on the other hand provide a structured methodology for determining SIL levels and provide reference to standards such as MIL HDBK 217 for reliability issues such as FMECAs etc. It is not practical due to national requirements

and practises to mandate for all areas of aircraft safety, however a uniform method of classifying system safety requirements could provide a useful tool.

Although there is commonality between the ARP and Defence Standard, there appears to be insufficient commonality and flexibility to allow the drafting of a standard guidance document at this stage.

5. References

- Ref 1. Defence Standard 00-56
Safety Management Requirements for Defence Systems
Issue 2, 13 December 1996
- Ref 2. Defence Standard 00-54
Safety Critical Hardware Development
Issue 1, 19 Mar 1999
- Ref 3. Defence Standard 00-55
Safety Critical Software Development
Issue 2, 1 Aug 1997
- Ref 4. ARP 4754
Certification Considerations for Highly Integrated or Complex Aircraft Systems
ASSC/020/3/40-Issue 04
27th June 1996
- Ref 5. ARP 4761
Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne
Systems and Equipment
Draft #17, 6th May 1996
- Ref 6. RTCA DO-254
Design Assurance for Electronic Hardware
19th April 2000
- Ref 7. RTCA DO-178B
Software Considerations in Airborne Systems and Equipment Certification
December 1, 1992
- Ref 8. YSE Report
Comparison of Standards for Safety Related Software Development
CF171/3/53
ASSC/330/3/425
25th February 1999
- Ref 9. IEC 61508
Functional safety of electrical / electronic / programmable electronic safety-related systems
Issue 1, 2002
- Ref 10. DERA Malvern (C Newton & C Pygott)
A Comparison Of Avionics Standards
DERA/CIS/CIS3/TR990319/1.0, August 1999
- Ref 11. JSP 318B
Regulation Of The Airworthiness Of Ministry Of Defence Aircraft
4th Edition, November 1999

- Ref 12. JSP 430
Ship Safety Management System Handbook
Issue 1, January 1996
- Ref 13. JSP 454
Procedures For Land Systems Equipment Safety Assurance
Issue 2, January 2000
- Ref 14. SW01
Regulatory Objectives for Software Safety Assurance in ATS Equipment