



**CEN Workshop 10 – European Handbook for Defence Procurement**

# **Expert Group 17 : Dependability & Safety**

**Final Report**

**Brussels, June 30, 2011**

# Contents

EG 17 members list .....	4
1- References and Vocabulary .....	5
2- Introduction .....	5
3. Scope.....	7
4- Reduction process.....	8
5 - Recommendations for Best Practice .....	9
6- Recommendations for Future Standardization .....	11
7- Conclusions .....	12
Annex A .....	13
A1 Vocabulary, definitions, mathematical expressions.....	13
A2 System level standards .....	14
A2.1 Management .....	14
A2.1.1 Dependability & Safety (RAMS) .....	14
A2.1.2 Dependability (RAM).....	14
A2.1.3 Safety.....	16
A2.1.3a General System:.....	16
A2.1.3b General for electric/electronic function: .....	16
A2.1.3c Vehicle electric/electronic function:.....	16
A2.1.3d Aircraft: .....	16
A2.1.3e Munitions: .....	17
A2.2 Requirement (RAM).....	18
A2.3 Engineering .....	18
A2.3.1 Techniques & Methods.....	18
A2.3.1a General.....	18
A2.3.1b Failure Mode, Effects and Criticality Analysis (FMECA) .....	19
A2.3.1c Fault Tree Analysis (FTA).....	20
A2.3.1d Reliability Block Diagram (RBD).....	20
A2.3.1e Reliability Prediction .....	21
A2.3.2 Design & Assessment.....	22
A2.3.2a Reliability .....	22
A2.3.2b Maintainability.....	23
A2.3.2c Testability.....	23
A2.3.2d Safety .....	24
A2.4 Test & Verification.....	25
A2.4.1 Reliability and safety in Service.....	25
A2.4.2 Reliability Growth.....	26
A2.4.3 Data collection & failure analysis.....	27
A2.4.4 Test method .....	28
A3 Electronic specific standards.....	29

A4 Software specific standards ..... 29

A5 Communication specific standards..... 31

## EG 17 members list

Members	Country	Full name organization e-mail address
	France	<b>Mr. BACHELIER Jacques</b> Nexter Group <a href="mailto:j.bachelier@nexter-group.fr">j.bachelier@nexter-group.fr</a>
		<b>Mr. DAVENEL Franck</b> MOD France <a href="mailto:franck.davenel@dga.defense.gouv.fr">franck.davenel@dga.defense.gouv.fr</a>
		<b>Mr. GIRAUDEAU Michel</b> Thales <a href="mailto:michel.giraudeau@fr.thalesgroup.com">michel.giraudeau@fr.thalesgroup.com</a>
		<b>Mrs. LEGENDRE Sophie</b> MOD France <a href="mailto:sophie.legendre@dga.defense.gouv.fr">sophie.legendre@dga.defense.gouv.fr</a>
		<b>Mrs. MARTIN Michelle</b> MBDA <a href="mailto:michelle.martin@mbda-systems.com">michelle.martin@mbda-systems.com</a>
	<b>Mr. PLATEAUX Laurent</b> MOD France <a href="mailto:laurent.plateaux@dga.defense.gouv.fr">laurent.plateaux@dga.defense.gouv.fr</a>	
	<b>Mr. THUAULT Michel</b> MOD France <a href="mailto:michel.thuault@dga.defense.gouv.fr">michel.thuault@dga.defense.gouv.fr</a>	
Italy	<b>Mr. BUCCINI Claudio</b> Finmeccanica <a href="mailto:claudio.buccini@finmeccanica.it">claudio.buccini@finmeccanica.it</a>	
	<b>Mr. GRASSO Alessio</b> MOD Italy <a href="mailto:alessio.grasso@aeronautica.difesa.it">alessio.grasso@aeronautica.difesa.it</a>	
	<b>Ms. BOTTIGLIERI Patrizia</b> Finmeccanica <a href="mailto:patrizia.bottiglieri@Finmeccanica.com">patrizia.bottiglieri@Finmeccanica.com</a>	
Germany	<b>Mr. MAYER Gerhard</b> MOD Germany <a href="mailto:gerhardmayer@bwb.org">gerhardmayer@bwb.org</a>	
Spain	<b>Mr. CORTES Ricardo</b> ITP <a href="mailto:ricardo.cortes@itp.es">ricardo.cortes@itp.es</a>	
UK	<b>Mr. PEARCE John</b> Atkins <a href="mailto:john.pearce@atkinsglobal.com">john.pearce@atkinsglobal.com</a>	
	<b>Mr. BARNETT Nicholas</b> MOD UK <a href="mailto:DESJSCTLS-Pol-Rel1@mod.uk">DESJSCTLS-Pol-Rel1@mod.uk</a>	

## 1- References and Vocabulary

- a. CEN/WS/10/EG17 N003: Framework paper: Guidance for expert groups on the selection of standards and provision of associated recommendations.
- b. IEC 60050-191 am 2 Ed 1 January 2002: International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service.
- c. ARMP-7 Ed 2 August 2008: NATO R&M Terminology applicable to ARMP's
- d. AOP 38 Ed 5 Oct 09: Glossary of terms and definitions concerning the safety and suitability for service of munitions, explosives and related products
- e. IEC 61508 part 4 Ed 2 April 10: Functional safety of electrical/electronic/programmable electronic safety- related systems – Definitions and abbreviations
- f. IEC 61703 Ed 1 September 2001: Mathematical expressions for reliability, availability, maintainability and maintenance support terms
- f. ISO 26262 part 1 Ed 1: Road vehicles -- Functional safety -- Part 1: Vocabulary

## 2- Introduction

**2.1 :** The European Commission requested the European Committee for Standardization to establish Workshop 10 to improve the efficiency and enhance the competitiveness of European Defence Industry. The European Handbook for Defence Procurement, EHDP, has been prepared by Experts Groups reporting to CEN Workshop 10. This document is a guide designed as a tool for anyone involved in the European defence procurement contractual negotiations.

The primary target audiences for the Handbook are:

- The staff in the ministries of defence who are producing procurement specifications and invitations to tender
- the staff in defence companies who are responding to those requirements

EHDP is designed to provide Defence Procurement Agencies and Defence Industries with a preferential list of selected recommended standards qualified as best practice ones to be included in contracts together with concise recommendations for an optimum use of those standards in such a Defence Procurement context.

Those types of resulting informative data could be used in the acquisition process by MoD and in the development process by Industry such that system will be built faster, better and cheaper. The aim of a recommendation is to develop good practices in the domain addressed by the Expert Group and to assist the final user in using recommended best practices standards in the best cost-effective way.

- Increasing the controlled use of existing standardization, a necessity to harmonise European practices used by defence procurement stakeholders.

- The objective is to deploy a common approach through Nations Procurement agencies about an optimized utilization of standards : civil ones and military ones, the possible limitations of civilian standards with respect to military applications,... to provide a useful guide to all stakeholders involved in defence procurement process
- Description of how to implement standards successfully in armament contracts
- The overall result will be a better use of standards in armament contracts

Recommendations are, during the drafting process, designed to allow EHDP final users to be provided with the right information for timely and quickly acquiring the best control in writing standards clauses related to the selected material, in armaments contracts. That's why the volume of recommendations will be accordingly fully compatible with respect to EHDP vocation and purpose.

**2.2** : Dependability is a relatively new overarching term that is used to pull together a number of more specific subject areas, for example availability, reliability, maintainability, durability and fault tolerance that, when executed effectively, help to ensure that any new product has the ability to perform as and when required.

Safety is a large topic with many sub sets including health and safety, airworthiness, product safety, ammunition / explosive safety, many of which have legislative documents which have to be taken into account when considering a new project. Some of these areas are already covered by other working groups within WS10.

Prior to any work being undertaken by this working a group a proposal was put forward to include product safety within its scope as many of the tools methods and data used to provide assurance that a product will be dependable are the same as those used to provide assurance of product safety. This specific area of the safety domain has not been covered elsewhere in WS10 and thus the proposal was accepted by the WS10 secretariat.

The more traditional areas of reliability, maintainability and safety are very well documented and as a result there are a multitude of standards available in the public domain to assist staff engaged in working in those areas. These range from national standards, both civil and defence, through multi national standards, typically NATO standards, to international standards, IEC and ISO. Many of these standards were first published in the 1980's and 1990's and whilst some of them have been reviewed, updated, and are still extant and relevant today, many have been withdrawn or cancelled or in some cases just published and forgotten about.

Many of these standards are still in common usage today with different contractors in different countries choosing standards that suit them, or which they understand even where that standard has not been updated for many years or in some cases withdrawn and / or cancelled. It is not unknown for staff in differing locations within the same multi national company to be using different standards to achieve similar results. When contracting in a multi national collaborative project it is often very difficult to get agreement on a single set of standards to work to, and a single agreed set of outputs.

### 3. Scope

Dependability and safety are both massive subjects in their own right, each covering many sub domains and having large numbers of standards and standard type documents associated with them. One of the early decisions made by the group was where the boundary should lie.

The dependability of an item is defined as ‘its ability to perform as and when required.’ It is also used descriptively as an umbrella term to cover the more traditional subjects including availability, reliability, testability, fault tolerance, durability and maintenance support. Many other disciplines have links in to dependability those most typically included being Human Engineering (commonly referred to as Human Factors Integration (HFI)) and environmental testing.

This section of the European Handbook only covers the more traditional areas of reliability, availability and maintainability including testability (RAM) both in terms of engineering design assessment and verification techniques. Although a number of the members of the working group identified standards in the maintenance, reliability centred maintenance, human engineering and environmental areas it was agreed that due to time limitations and the relatively small number of active participants it was not possible to include these areas in the scope of this work. It should be noted that the environmental aspects were covered by a separate working group and are detailed in another part of the Handbook

Product safety is the engineering science that assures systems behave as needed when systems fail and uses very similar techniques to those applied during any assessment of dependability.

The final agreed scope of work for standards is reflected in the perimeter definitions that have been selected and are shown in Table 1 below:

1. Vocabulary, definitions, mathematical expressions
2. System level standards
  - a. Management
    - i. Dependability
    - ii. Safety
  - b. Requirements
  - c. Engineering
    - i. Techniques and Methods
      1. General
      2. FMECA
      3. FTA
      4. RBD
      5. Prediction
    - ii. Design and Assessment
      1. Reliability
      2. Maintainability
      3. Testability
      4. Safety
    - iii. Test and verification
      1. Reliability and Safety in Service
      2. Reliability Growth

3. Data Collection and Failure Analysis
4. Test Method
3. Electronic Specific Standards
4. Software Specific standards
5. Communications Specific Standards

**Table 1 – Perimeters used for classification of standards**

#### **4- Reduction process**

Each member of the Dependability and Safety working group was invited to submit a list of the relevant standards which are commonly used in their country, be they working for Ministries of Defence or commercial industry. This initial activity was undertaken by 5 nations, France, Germany, Italy, Spain and the UK, and resulted in a list of 230 standards, or in some cases standards like documents.

Each standard from the original list was then considered by the group for relevance to the agreed perimeters and marked as either approved to be analysed or out of scope which immediately reduced the total of documents from 230 to 200. From this list the proposing country was then invited to draft a recommendation explaining why the standard was felt to best practise and should be included within the European Handbook. Where a standard was recommended by more than one country a lead nation was selected to draft the recommendation which would then be reviewed, if necessary amended and then agreed by all of the recommending nations.

During this process a number of standards were found to have been withdrawn and or replaced by more up to date documents whilst upon review, others were not considered appropriate to be recommended as best practise and have not been taken forward.

When all of the recommendations had been received the group reviewed each one forming a consensus opinion on which standards should be included in the handbook as best practice and which ones were to be excluded. There were a couple of cases where a clear consensus could not be reached and in these cases it was agreed that the convenor of the group would make the final decision.

Preference was given to international standards where possible and where the group agreed that these standards were representing best practices. Where international standards were not available or not considered to be best practices then multinational or national standards were recommended.

Following the completion of the reduction process a total of 77 standards were selected for inclusion in the Dependability and Safety part of the European Handbook for Defence Procurement.

## **5 - Recommendations for Best Practice**

Specifying Dependability and safety Requirements and Programmes in contracts is essential to ensure that the delivered product is capable of being operated as required in the specified environment and in safe condition. As a minimum, a dependability and safety programme of work as detailed in the recommended management standards should be specified.

Current best practice is to contract for progressive assurance that the design will meet the requirements, with evidence / assurance being presented through dependability and safety cases / reports that document the individual engineering techniques / methods / tests that have been undertaken and use the results as the basis for claims to show that the requirements will be achieved.

One of the three principals of progressive assurance requires ‘a programme of activities to be planned and implemented to satisfy the requirement, and investigate the risks’. Previous standards provided a list of engineering techniques / methods / tests that all had to be considered, requiring explanation of why that particular item was being included or excluded from the programme. Each of these techniques / methods / tests has dedicated standards (as seen in the EG17 recommendation list) which were then added to the contract.

The move to progressive assurance saw the removal of this requirement to address every task, and thus inclusion of all of the standards in the contract, preferring instead an approach where the contractor proposes which tasks will add benefit and value to the design based on the identified risks for the equipment under purchase.

Where a need is identified for a specific technique / method / test to be applied to the project then the standard(s) identified as best practice in this document should be invoked and applied to the contract.

Annex A presents a short description of standards selected for inclusion in the dependability and product safety area of the handbook and in areas where it is possible a recommended best practise standard is outlined.

A complete list of standards selected for inclusion in the handbook is given at table 2 below:

### **1 Vocabulary, definitions, mathematical expressions**

AOP 38, ARMP7, IEC 60050-191, IEC61508 part 4, IEC 61703, ISO26262 part1

### **2 System level standards**

#### **2.1 Management**

##### **2.1.1 Dependability & Safety (RAMS)**

RG Aero 00027

##### **2.1.2 Dependability (RAM)**

ARMP1, JA 1000 & 1000-1, JA 1010 & 1010-1, IEC 60300-1&2, STANAG 4174, MIL HDBK 470A, BS5760 part18, Def Stan 00-40 part 1, Def Stan 00-42 part 3

### **2.1.3 Safety**

ED 79, MIL-STD 882, IEC 61508 part 1, ISO26262 parts 2&3, STANAG 4297, Def Stan 00-56, AOP 52, AOP-42

### **2.2 Requirements**

ARMP4, IEC 60300-3 part4

### **2.3 Engineering**

#### **2.3.1 Techniques & Methods**

##### **2.3.1.1 General**

IEC 61165, IEC 61508 part 7, MIL-STD 882, ISO26262 part 4, ARP 4761, MIL HDBK 338

##### **2.3.1.2 FMECA**

IEC 60812

##### **2.3.1.3 FTA**

IEC 61025

##### **2.3.1.4 RBD**

IEC 61078

##### **2.3.1.5 Reliability Prediction**

IEC61709, UTEC-C 80811, NSWC-94/L07, NPRD95

#### **2.3.2 Design & Assessment**

##### **2.3.2.1 Reliability**

MIL HDBK 251, MIL HDBK 338, IEC 60319

##### **2.3.2.2 Maintainability**

MIL-HDBK 470, MIL-HDBK 472, MIL HDBK 2084, IEC 60300-3 part 10, DOD HDBK 791, IEC 60706 part 2

##### **2.2.2.3 Testability**

IEC 60706-5, Mil-HDBK 2165

##### **2.3.2.4 Safety**

MIL STD 882, IEC 61508 all parts, AER P-6, ISO 26262 all parts

### **2.4 Test & Verification**

#### **2.4.1 Reliability and Safety in Service**

ARMP6, ISO 26262 part 7, STANAG 4158

#### **2.4.2 Reliability Growth**

IEC 61014, IEC 62429, MIL-HDBK 189, IEC 61164

#### **2.4.3 Data collection & failure analysis**

ATA Spec 2000, RG Aero 00033, STANAG 4158, IEC 60300-3 part 2, Def Stan 00-44

#### **2.4.4 Test method**

MIL-HDBK 781, ARMP6, MIL STD 690D, IEC 61163-1, IEC 61650, IEC 60300-3-5

### **3 Electronic specific standards**

IEC 61508 part 2, MIL-HDBK 338, ISO 26262 part 5, ED80

### **4 Software specific standards**

ARMP9, IEC 61508 part 3, ED12, 26262 part 6, BS5760-8, IEEE 1633

### **5 Communication specific standards**

IEC 61907

Table 2 – List of standards for inclusion in the handbook by perimeter category.

## **6- Recommendations for Future Standardization**

No specific areas of the dependability or product safety disciplines have been identified as not being covered by at least one standard, be it civil or defence, national or international level. The reliability, maintainability and product safety parts of the dependability subject are covered by a plethora of standards and future work needs to rationalise them not expand them further.

In the dependability and safety (RAMS) management area there many standards including a US Military Standard, UK Defence Standard, French Defence Standards, US Civil Standard, UK civil standards, NATO Standard and an International (IEC) standard, all of which detail very similar, if not identical, processes but none of which cross refer to each other. Most of these standards have been updated in the recent past and thus are not planned to be updated again any time soon.

In the Engineering areas many of the standards, although written as many as twenty years ago, are still representative of current thinking and acceptable to use. Where they were published over ten years ago there is a need for a structured update programme and for conversion from country specific standards to international standards. Where standards are reviewed without any modification, it is not obvious that this review has been carried out because the issue status and the date of issue are not updated. When standards are reviewed it is recommended that a statement advising users that review has been carried out and a future review date should be included at the front of the document.

In many cases older country standards eg. US Mil standards are still widely used even though more up to date international standards, which are equally good, exist. These older standards, in

particular US military standards are available free of charge from many websites while the newer international standards can only be acquired at considerable costs which can prevent smaller companies from adopting them. Whilst it is accepted that the issuing standards body needs to be a profit making organisation there needs to be some sort of mechanism to make the newer and better standards available at a lower cost.

There is a need for an expert working group, similar to those set up for the EHDP work, to actively review standards, promote the newer ones and ensure that the older ones are removed from general availability.

## **7- Conclusions**

There are many standards covering the Dependability and Safety domains and the group found it very difficult to recommend just one standard or set of standards even when the individual domains were split into low level and in some cases unique sub domains. The group recognised very early on that it would be necessary to ensure the sub domains were at a low enough level to minimise the number of standards within them, and a lot of time was spent to ensure this breakdown was as efficient as possible.

It was also recognised early on that many standards are either inter-related or complementary to each other and that the recommendation of one standard meant that a number of others need to be included as well. This is particularly so in the management areas where multi-national standards, typically NATO, are based on civil standards and purely add those bits required for Military only application.

Despite the fact that some standards cover very specific domains, for example road vehicle safety, they often contain generalisations and lists of activities that need to be tailored for the particular project that is being undertaken. Following any standard without a thorough understanding can often lead to the inclusion of unnecessary tasks often at considerable cost. Even where a standard has been recommended as best practice it is vital to ensure that it is applied intelligently and adds value to the project that is being undertaken.

The Dependability and Safety domains are changing rapidly as a result of new legislation, incidents that occur with equipment that is in service and as research provides new and better methods for achieving safe and dependable products. The list of standards contained within this report will rapidly become out of date, thus constant review is recommended.

There are a vast number of standards in the Dependability and Safety domains, both civil and military, and the group felt there is an urgent need for a review of all the standards in each domain to both remove old and obsolescent standards, and merge the best parts of some 'complementary' standards, both civil and military in to single documents.

## Annex A

The standards given hereafter are recognized as the “best practice” in their domain and where possible a single recommended standard will be indicated.

The standard issues are not given here. They will be found in the specific Standard Recommendations spreadsheet.

### **A1 Vocabulary, definitions, mathematical expressions**

Specific standards recommended for terminology and definitions are:

#### **IEC 60050-191 (International Electrotechnical Vocabulary - Part 191: Dependability)**

It gives a comprehensive list of definitions of the terms that can be used when defining Dependability; many national and international standards refer to this standard for common terms

#### **ARMP-7 (NATO Reliability and Maintainability terminology applicable to ARMPs)**

This glossary is only relevant to terms included in Allied Reliability and Maintainability Publications (ARMPs) which are not explicitly defined in the IEC document listed above.

#### **IEC 61508 part 4 (Functional safety of electrical/electronic/programmable electronic safety-related systems)**

It contains the definitions and explanation of terms that are used in parts 1 to 7 of this standard relative to functional safety related to electrical/electronic/programmable electronic systems.

#### **ISO 26262 part1 (Road vehicles - Functional safety)**

It specifies the terms, definitions and abbreviated terms for application in all parts of ISO 26262 relative to functional safety in sector of road vehicles.

#### **AOP 38 (Glossary of terms and definitions concerning the safety and suitability for service of munitions, explosives and related products)**

It contains the specialist acronyms, terms and their definitions related to the work of the NATO Group on Safety and Suitability for Service of Munitions and Explosives

#### **IEC 61703 (Mathematical expressions for reliability, availability, maintainability and maintenance support terms)**

It gives practical definitions and recommendations for mathematical expressions of reliability, availability, maintainability and maintenance characteristics with small example for each of them and should be used with IEC60050-191

**Comment: IEC 60050-191 is the most general standard for dependability and should always be used. For safety, there is no one dedicated standard that covers all domains; the applicable standards will be specific to the domain that is being worked.**

## **A2 System level standards**

### **A2.1 Management**

#### **A2.1.1 Dependability & Safety (RAMS)**

Reliability, Availability, Maintainability and Safety (RAMS) management of a product, its components and the production resources and processes employed, is a key activity which cannot be separated from other product performance control or programme management. RAMS management is to be considered as a whole, and it is a preponderant part of RAMS activities to coordinate the required trade-offs between the corresponding aptitudes for obtaining a product that is "robust" with respect to the specified undesirable events: reliability versus availability, dependability (RAM) versus safety, etc.

##### **RG Aero 000 27 (Programme management – Guide to RAMS management)**

It specifies the principles to be implemented to manage the RAMS of any product. The purpose of this recommendation is to provide customers and their suppliers with a document specifying the notions of "construction" and "management" of product RAMS, RAMS aptitudes being managed as a whole set of characteristics, which are considered in the same way as the expected functional performance of this product.

#### **A2.1.2 Dependability (RAM)**

Dependability affects product costs and processes. It is an inherent product design property influencing product performance. A dependable product is achieved through the implementation of dependability disciplines in the early concept and design phases of the product life cycle to provide cost-effective product operations. Like other technical and engineering disciplines, dependability needs to be managed in order to deliver high-value products to customers.

Dependability, like safety, is managed in such a way as to provide assurance in a progressive way that the requirements are being, and will ultimately be met, by the product design. Progress is reported through a number of Dependability Case reports, delivered at critical points in the product development cycle, each giving an overview of progress to date with an insight into any additional future work that will be required.

Standards about dependability management provide assistance for developing reliability and maintainability programs according to the requirements. Suppliers and customers need answers to questions such as:

Who is responsible for reliability and maintainability goals, planning, etc?

What reliability and maintainability methods are most effective, and how are they applied?

When are reliability and maintainability methods used most effectively in the product development cycle?

Where can we get more detailed information and instructions on how to use the reliability and maintainability methods?

### **IEC 60300-1&2 (Dependability management)**

These two standards provide an overview of how a dependability programme should be developed in order to deliver a system or equipment that will be able to deliver high operational availability along with a high probability of mission success. Part 2 contains a list of 'dependability tasks' that could be undertaken to mitigate risks that have been identified in the programme being undertaken. This task list should be tailored to ensure only tasks that add value, and thus mitigate specific risk, are included.

### **STANAG 4174 <sup>1</sup>(Allied Reliability and Maintainability Publications)**

#### **ARMP-1 <sup>2</sup>(NATO Requirements for Reliability and Maintainability)**

#### **SAE JA 1000 (Reliability Program Standard), SAE JA 1000-1 (Reliability Program Standard Implementation Guide), SAE JA 1010 (Maintainability Program Standard), SAE JA 1010-1 (Maintainability Program Standard Implementation Guide)**

This set of documents is the NATO equivalent of the IEC detailed above. They provide information on how to manage reliability and maintainability programmes providing guidelines and methods for achieving high Availability and the required mission success for all military materiel using a RAM case approach. As with the IEC, the methodologies listed should be tailored to mitigate the identified risks of the programme.

### **MIL-HDBK-470A (Designing and developing Maintainable Products and Systems)**

It provides task descriptions for maintainability program. Software maintainability is not covered by this standard.

### **BS 5760-18 (Guide to the Demonstration of Dependability Requirements - The Dependability case)**

This document provides an overview of the assurance case approach to design and delivery of dependable systems. It provides guidance on how to implement and manage a programme of activities through the life of the system / equipment.

### **DEF Stan 00-40 part 1 (Reliability and Maintainability: Management responsibilities and requirements for programmes and plans)**

It is a general introduction to the means of achieving reliable and maintainable equipment detailing the specific measures to be adopted by the MOD Sponsors, the Project Managers and the Contractors.

### **DEF Stan 00-42 part 3 (Reliability and Maintainability Assurance Activities – Reliability and Maintainability Case)**

It provides a description of the principles of progressive assurance in R&M, and provides guidance on the content and the ownership of the R&M Case through the life of a system.

**Comment: IEC 60300 1&2 are the best standards to use when implementing a dependability programme. The STANAG, NATO, SAE, BS and UK Defence Standards are all 'local' interpretations based around the dependability assurance case approach.**

---

<sup>1</sup> STANAG 4174 calls ARMP 1, 4, 6 & 7

<sup>2</sup> ARMP-1 calls out SAE JA1000, SAE JA1000-1, SAE JA1010 and SAE JA1010-1

### **A2.1.3 Safety**

#### **A2.1.3a General System:**

##### **MIL-STD-882 (Standard Practice for System Safety)**

The system safety practice as defined in this standard provides a consistent means of evaluating identified risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority and compliant with laws and regulations, Executive Orders, treaties, and agreements. MIL-STD-882 is recommended by other working group as EG 9, EG10 and EG13.

##### **Def Stan 00-56 (Safety Management Requirements for Defence Systems)**

This Standard specifies the safety management requirements for defence systems. The level of effort expended on safety management and the detail of the analysis shall be commensurate with the potential risk posed by the system (i.e. the risk that would be posed in the absence of mitigation), the complexity of the system and the unfamiliarity of the circumstances involved, such that the resultant Safety Case is sufficient to demonstrate that the system is safe, so far as is reasonably practicable.

#### **A2.1.3b General for electric/electronic function:**

##### **IEC 61508 part 1 (Functional safety of electrical/electronic/programmable electronic safety-related systems)**

IEC 61508 defines appropriate means for achieving functional safety. It applies to safety-related systems when one or more of such systems incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices.

This part 1 of the IEC 61508 series of standards includes general requirements that are applicable to all parts.

#### **A2.1.3c Vehicle electric/electronic function:**

##### **ISO 26262 parts 2&3 (Road vehicles - Functional safety)**

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles. This adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic, and software elements that provide safety-related functions.

Part 2: This part of ISO 26262 specifies the requirements on functional safety management for automotive applications. These requirements cover the project management activities of all safety lifecycle phases and consist of project-independent requirements, project-dependent requirements to be followed during development, and requirements that apply after release for production.

Part 3: This part of the International Standard specifies the requirements on the concept phase for automotive applications. These requirements include the item definition, the initiation of the safety lifecycle, the hazard analysis and risk assessment and the functional safety concept.

#### **A2.1.3d Aircraft:**

### **ED79 (Certification considerations for highly-integrated or complex aircraft systems)**

Embedded systems are more and more complex. It presents opportunities for development error and undesirable, unintended effects.

For complex systems, it could be not possible / practical to test exhaustively and to demonstrate there is no development error. Since these errors are generally not deterministic and suitable numerical methods for characterizing them are not available, other qualitative means should be used to establish that the system can satisfy safety objectives.

Development assurance establishes confidence that system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety.

### **A2.1.3e Munitions:**

#### **STANAG 4297/AOP-15 (Guidance on the assessment of the safety and suitability for service of munitions for NATO armed forces)**

The aim of this STANAG is to promote the use, updating and application of AOP-15

The purpose of AOP 15 is to:

Provide a uniform guide for the assessment of the safety and suitability of non-nuclear munitions for use by NATO armed forces.

Recommend system safety design and development criteria for munitions systems, subsystems and components. Recommend system design and development criteria for the safety and suitability for service of munitions systems, subsystems and components and the associated weapon system interfaces.

Present a methodology to identify and to reduce risks related to munitions and refer to analysis and test methods to demonstrate that the risks related to munitions are acceptable.

#### **AOP-52 (Guidance on Software Safety Design and Assessment of Munitions-Related Computing Systems)**

The purpose of the AOP is to provide management and engineering guidelines to achieve a reasonable level of assurance that the software and software-like devices will execute within the system context and operational environment with an acceptable level of safety risk.

This AOP is both a reference document and management tool for aiding managers and engineers at all levels, in any government or industrial organization

#### **AOP-42 (Integrated design analysis for munition initiation systems and other safety critical systems)**

This document explains how to improve safety analysis quality and compliance analysis to safety design standard (e.g. STANAG 4187) for safety critical item (e.g. ammunition fuze).

**Comment: There is no specific recommendation of best practice standard for this section as each domain has its own requirements.**

## **A2.2 Requirement (RAM)**

For defence systems, two requirements are essential to succeed the mission and to be safe. To define technical requirement, you need to define before how to proof it and method of assessment (analysis, trials and support).

### **IEC 60300-3-4 (Dependability management - application guide - Guide to the specification of dependability requirements)**

It provides guidelines to define dependability requirements, advices for the customer to ensure that the requirements are met and advices for the purchaser to satisfy the requirements. This standard is applicable when specification are produced either by the customer, either by the supplier or mutually agreed between the customer and the purchaser.

### **ARMP-4 (Guidance for writing NATO Reliability and Maintainability Requirements Document)**

It provides guidance on writing R&M requirement documents during the life cycle of a project. It also contains the necessary information and advice to write quantitative reliability and maintainability requirements, and availability and risk requirements which are derived there from.

**Comment: IEC 60300-3-4 and ARMP-4 are the best practice standards to define RAM requirements.**

## **A2.3 Engineering**

### **A2.3.1 Techniques & Methods**

#### **A2.3.1a General**

This chapter covers all the general method used in dependability and safety studies. Following standard cover different domains:

#### **MIL-STD-882 (Standard Practice for System Safety)**

It is a standard for Military system Safety studies. The system safety practice as defined in this standard provides a consistent means of evaluating identified risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority and compliant with laws and regulations, Executive Orders, treaties, and agreements.

#### **IEC 61508 part 7 (Functional safety of electrical/electronic/ programmable electronic safety-related systems)**

It is a standard for Safety techniques and Methods for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/ programmable electronic systems (E/E/PESs)) Overview of techniques and measures. Part 7 contains an overview of various safety techniques and measures relevant to IEC 61508. The references should be considered as

basic references to methods and tools or as examples, and may not represent the state of the art.

**ISO 26262 (Road vehicles - Functional safety) part 4**

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles. This part “Product development: system level” specifies the requirements on product development at the system level.

**ARP 4761 (Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment)**

This standard from the Society of Automotive Engineers (SAE) is a common international basis for demonstrating compliance with airworthiness requirements as it is largely referenced in ARP4754 : for various safety assessments detailed guidelines and methods. Each safety activity is detailed and examples provided.

**IEC 61165 (Application of Markov Techniques)**

This International Standard provides guidance on the application of Markov techniques to model and analyze a system and estimate reliability, availability, maintainability and safety measures

**MIL-HDBK-338 (Electronic Reliability Design Handbook)**

This Handbook is actually an introduction and complete guide to Reliability and other Logistic engineering disciplines related to it, such as Maintainability and Testability. It addresses design processes, design guidelines, project verification methodologies, etc. providing both theoretical approaches and practical guidelines. The handbook may be even used as training reference for these disciplines since it also includes theory and mathematical models behind any reliability aspect.

**Comment: There is no specific recommendation for this section as each technique is unique and has its own standards.**

**A.2.3.1b Failure Mode, Effects and Criticality Analysis (FMECA)**

The FMECA Failure Mode, Effects and Criticality Analysis is a method of dependability and safety analysis which systematically evaluate and document, by item failure mode analysis, the potential impact of each functional or hardware failure on mission success, personnel and system safety, system performance, maintainability, and maintenance requirements. Each potential failure is ranked by the severity of its effect in order that appropriate corrective actions may be taken to eliminate or control the high risk items.

**IEC 60812 (Analysis Techniques for system Reliability – Procedure for Failure Mode and Effect Analysis (FMEA))**

This International Standard describes Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects and Criticality Analysis (FMECA), and gives guidance as to how they may be applied to achieve various objectives by providing the procedural steps necessary to perform an analysis; identifying appropriate terms, assumptions, criticality measures, failure modes; defining basic principles; providing examples of the necessary worksheets or other tabular forms.

All the general qualitative considerations presented for FMEA will apply to FMECA, since the last one is an extension of the other.

**Comment: IEC 60812 is the best practice standard to perform FMECA.**

#### **A2.3.1c Fault Tree Analysis (FTA)**

Fault Tree Analysis is method of safety analysis which consist in a failure analysis in which an undesired state of a system is analysed using Boolean logic to combine a series of lower-level events. This analysis method is mainly used in the field of safety engineering to quantitatively determine the probability of a safety hazard.

##### **IEC 61025 (Fault tree analysis)**

This International Standard describes fault tree analysis and provides guidance on its application as follows:

Definition of basic principles;

Describing and explaining the associated mathematical modelling;

Explaining the relationships of FTA to other reliability modelling techniques;

Description of the steps involved in performing the FTA;

Identification of appropriate assumptions, events and failure modes;

Identification and description of commonly used symbols.

**Comment: IEC 61025 is the best practice standard to perform FTA**

#### **A2.3.1d Reliability Block Diagram (RBD)**

Reliability Block Diagram is a method of dependability and safety analysis. Its purpose is to evaluate by an analyst the reliability and availability of a given system by studying its architecture.

A reliability block diagram (RBD) is a pictorial representation of a system's reliability performance.

It shows the logical connection of (functioning) components needed for successful operation of the system.

##### **IEC 61078 (Analysis Techniques for system Dependability - Reliability Block Diagram and boolean methods)**

This International Standard describes procedures for modelling the reliability of a system and for using the model in order to calculate reliability and availability measures. A standard set of symbols related to reliability parameters is given and some formulae are given in the annexes.

**Comment: IEC 61078 is the best practice standard to perform RBD.**

### **A2.3.1e Reliability Prediction**

Reliability Prediction is currently recognized as an essential need especially in military systems. Calculation of a reliability prediction for non-redundant equipment is the very first step in any complete reliability study. The most beneficial use of a reliability prediction is as an aid to equipment designers. The predicted failures are crucial when calculating system availability and testability. Reliability predictions are also used as a basis for maintenance (components and equipments spare) and safety assessment

Numerous handbooks provide information needed to calculate electronic component and equipped printed circuit board and mechanical components failure rates.

### **Electronic reliability prediction**

#### **UTE-C 80811 (Reliability Methodology for Electronic Defence Systems - Fides Guide)**

It's more recent methodology developed and the last version is from December 2010.

This FIDES method covers items varying from an elementary electronic component to a module or electronic subassembly including COTS.

Calculation models take directly into account the influence of the real operational environment and the real constraints like temperature, thermal cycling, vibration or humidity rate seen by cards. The models can handle permanent working, on/off cycling and dormant applications.

Moreover, failures related to intrinsic origins to the studied items (item technology or manufacturing and distribution quality) and extrinsic (specification and design of the equipment, selection of the equipment procurement, production and integration system) are included in component failure rate.

#### **IEC 61709 (Electronic components - Reliability - Reference conditions for failure rates and stress models for conversion)**

This standard is aimed to organizations that have their own data and describes how to state and use that data to perform reliability predictions. It also describes how reliability data can be used to predict failure rates at equipment level.

This guide does not contain failure rates, but it describes how they can be stated and used to assess prediction at different stress levels.

Very few military organizations have representative reliability data which can be used with these models. Moreover, this guide enables only operating reliability prediction.

Note: There is a proposal to form a working group within the IEC to merge IEC 61709 and IEC TR 62380.

**Comment: For military electronic systems reliability prediction, UTE-C-80811 methodology now provides realistic values of reliability levels, similar to usually observed average values (and not pessimistic or conservative values). More than a simple reliability calculation guide, it is a genuine reliability engineer guide. This methodology is recommended as a best practice for new electronic equipments.**

### **Mechanical reliability prediction**

#### **NPRD95 (Non-Electronic Parts Reliability Data)**

It is the only document which provides failure rate data on a wide variety of electrical, electromechanical, and mechanical parts/ assemblies edited by the Reliability Information Analysis Center (RIAC). For almost parts/ assemblies, this document has data only in specific environments/temperatures. Thus, it's quite difficult to assess calendar failure rate with a realistic life profile. (NPRD2011 is now available but has not been reviewed by EG17)

### **NSWC-94/L07 (Handbook of Reliability Prediction Procedures for Mechanical Equipment)**

The handbook presents a new approach for determining the reliability and maintainability (R&M) characteristics of mechanical equipment (NSWC-09 Jan2009 is now available but has not been reviewed by EG17).

**Comment: For mechanical reliability prediction, we recommend using as much as possible in service data if statistically representative or strength/stress method.**

## **A2.3.2 Design & Assessment**

### **A2.3.2a Reliability**

A traditional definition of reliability is the ability of an item to perform a required function under stated conditions for a specified period of time.

Reliability engineering is the doing of those things which insure that an item will perform its mission successfully. It will be influence not only by the way the equipment / system is used and maintained but also by the way it is specified, designed and built.

### **IEC 60319 (Presentation and specification of reliability data for electronic components)**

It provides guidance for the collection and presentation of data relating to the reliability of electronic components and their reliability characteristics. It also provides guidance to users as to how they should specify their reliability requirements to manufactures.

### **MIL-HDBK-338 (Electronic Reliability Design Handbook)**

It provides procuring activities and development contractors with an understanding of the concepts, principles, and methodologies covering all aspects of electronic systems reliability engineering and cost analysis as they relate to the design, acquisition, and deployment of equipment/systems

### **MIL-HDBK-251 (Reliability/Design Thermal Applications)**

It has been prepared specifically to guide engineers in the thermal design of electronic equipment with improved reliability. The primary purpose is to permit engineers and designers to design electronic equipment with adequate thermal performance

**Comment: There is no specific recommendation for this section as each discipline has its own standards.**

### **A2.3.2b Maintainability**

Maintainability as a design characteristic, concerns the relative ease and cost of preventing failures (retaining an item in a specified condition) or correcting failures (restoring an item to a specified condition) through maintenance actions. Maintainability is important to operations, or mission accomplishment, because it directly affects product availability.

#### **IEC 60300-3-10 (Dependability management - application guide – Maintainability)**

It provides guidance on how the maintenance aspects of the tasks should be considered in order to achieve optimum maintainability and can be used to implement a maintainability programme covering the initiation, development and in-service phases of a product.

#### **IEC 60706 – part 2 (Maintainability of Equipment - Maintainability requirements and studies during design and development phase)**

It contains information relating to the setting of and designing for maintainability requirements, activities that can be undertaken to provide confidence that the requirements can be met

#### **MIL-HDBK-470 (Designing and Developing Maintainable Products and Systems)**

It defines maintainability, describes its relationship to other disciplines, addresses the basic elements common to all sound maintainability programs, describes the tasks and activities associated with those elements, and provides guidance in selecting those tasks and activities.

#### **MIL-HDBK-472 Notice 1 (Maintainability Prediction)**

It presents 2 prediction methods, one for a early prediction and an other one for a detailed prediction, both applicable at any equipment or system level, at any level of maintenance, and for any maintenance concept pertinent to avionics, ground electronics, and shipboard electronics

#### **MIL-HDBK-2084 (Maintainability of Avionic and Electronic Systems and Equipment)**

It covers the common maintainability design requirements to be used in military specifications for avionic and electronic systems and equipment.

#### **DOD HDBK-791 (Maintainability Design Techniques)**

It provides guidelines to assist designers in incorporating maintainability into Army materiel early in research and development. It also illustrates the design principles that result in maximum maintainability.

**Comment: There is no specific recommendation for this section as each discipline has its own standards.**

### **A2.3.2c Testability**

The testability of a system is the measure of its ability to be known if it is in a state of operational operating (detection function) and, in case of damage, identify which is the Weakening element (localization function).

The testability usually confronts by the rate of detection, the precision of localization and the rate of false alarm. These performances are relative to a given level of maintenance. Testability is an important feature in the operation and maintenance of a system or equipment and has a significant effect on its availability and maintainability.

**IEC 60706-5 (Maintainability of equipment - Part 5: Testability and Diagnostic Testing)**

This standard has been developed and verified by technical committee 56 which contains representation from many nations. The technical content is good and the document is applicable to all staffs, whether in industry or in government, who are involved in development of defence equipment where there is a need to show that faults / failures can be detected and repaired within a given time frame. The results / outcomes of the activities / tests should be used to either refine the design where the requirements are shown not to have been met or to provide evidence that the requirements have been met.

**Mil-HDBK-2165 (Testability Handbook For Systems And Equipments)**

This military standard prescribes a uniform approach to testability program planning, establishment of diagnostic concepts and testability requirements, testability and test design and assessment, and requirements for conducting testability program review.

**Comment: There is no specific recommendation for this section as each discipline has its own standards.**

**A2.3.2d Safety**

A traditional definition of safety is the aptitude of a product, throughout its lifecycle, to guarantee acceptable levels of a risk of accident likely to injure personnel or lead to a major deterioration of the product or its environment.

**IEC 61508 all parts (Functional safety of electrical/electronic/programmable electronic safety-related systems)**

It is a standard for Safety techniques and Methods for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/ programmable electronic systems (E/E/PESs)). It applies to the entire E/E/PE safety-related system, providing system requirements, but also hardware (IEC 61508 part 2) and software (IEC 61508 part 3) refined requirements in a sole standard. The whole parts define the entire design and assessment process, from the system level, to the hardware or software component level, from requirements specification, to methods and measures to be used to implement and verify those requirements.

**ISO 26262 all parts (Road vehicles - Functional safety)**

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles. It covers the same range of activities.

**MIL-STD-882 (System Safety Program Requirements)**

It is a standard for Military system Safety studies which aims at imposing design requirements and management controls to prevent mishaps. The system safety program addresses hazards from many sources to include system design, hazardous materials, advancing technologies, and new techniques.

MIL STD 882E included details for tasks such as RAMS program and plan; interfaces and co-ordination; monitor and control of sub-contractors and supplier; integration and implementation; risk management; reviews/audits), for Safety Engineering (included tasks as engineering; hazard analysis; requirements; criteria analysis; tools/methods) and for Safety Assessment/Verification (included tasks as feedback information, test and verification).

#### **AER P-6 (Instructions for the Definition of Technical Requirements for Military Aircraft)**

It contains the instructions to be followed when drawing up Technical Specifications for military aircraft. It lists the minimum safety requirements to be addressed within an aeronautical contract, to define and describe the methodology to calculate the safety High Level Objectives taking into account the “Through Life” approach.

**Comment: There is no specific recommendation for this section as each domain has its own standards.**

## **A2.4 Test & Verification**

### **A2.4.1 Reliability and safety in Service**

In order to provide assurance that defence materiel meets and continues to meet its Reliability & Maintainability (R&M) objectives, there may be a requirement to assess and improve its In-service R&M performance.

When the compliance assessment with quantitative requirements is assessed by tries, the reliable level or the trial plan to be realized must be specified. In the case of the trial plan, the specification should include the duration of tries and the criteria of acceptable and refusal.

#### **ARMP-6 (Guidance for Managing in-service Reliability and Maintainability)**

ARMP 6 is guidance for managing in-service Reliability and Maintainability. This guide is dealing with contractual arrangements for assuring R&M performance, in-service R&M plan, assessing in-service R&M performance, identifying and prioritising opportunities for in-service R&M improvement, broader exploitation of in-service R&M data and limitations of cots equipment on monitoring and managing in-service R&M.

#### **STANAG 4158 (Guidelines for classifying incidents for reliability estimation of tracked and wheeled vehicles)**

It establishes standard definitions and criteria for classifying incidents observed.

#### **ISO 26262 part 7 (Production and operation)**

It specifies the requirements on functional safety management for automotive applications on production as well as operation, service and decommissioning. The most adapted standards depend on the need.

#### **A2.4.2 Reliability Growth**

Reliability improvement by a growth programme should be part of an overall reliability activity in the development of a product. This is especially true for a design that uses novel or unproven techniques, components, or a substantial content of software. In such a case the programme may expose, over a period of time, many types of weaknesses having design-related causes. It is essential to reduce the probability of failure due to these weaknesses to the greatest extent possible to prevent their later appearance in formal tests or in the field. At that late stage, design correction is often highly inconvenient, costly and time-consuming. Life-cycle costs can be minimized if the necessary design changes are made at the earliest possible stage.

The cost-effective solution to these challenges is a reliability growth programme fully integrated in both the design and evaluation phase as well as the testing phase.

##### **IEC 61014 (Programmes for reliability growth)**

It specifies requirements and gives guidelines for the exposure and removal of weaknesses in hardware and software items for the purpose of reliability growth. It applies when the product specification calls for a reliability growth programme of equipment (electronic, electromechanical and mechanical hardware as well as software) or when it is known that the design is unlikely to meet the requirements without improvement. It describes a process where the reliability growth programme is integrated into the design or product development process, known as integrated reliability engineering, is driven by limited time to market, programme costs and striving for product cost reduction.

##### **IEC 62429 (Reliability growth - Stress testing for early failures in unique complex systems)**

This International Standard gives guidance for reliability growth during final testing or acceptance testing of unique complex systems. It gives guidance on accelerated test conditions and criteria for stopping these tests. "Unique" means that no information exists on similar systems, and the small number of produced systems means that information deducted from the test has limited use for future production. This standard concerns reliability growth of repairable complex systems consisting of hardware with embedded software. It can be used for describing the procedure for acceptance testing, "running-in", and to ensure that reliability of a delivered system is not compromised by coding errors, workmanship errors or manufacturing errors. It only covers the early failure period of the system life cycle and neither the constant failure period, nor the wear out failure period. It can also be used when a company wants to optimize the duration of internal production testing during manufacturing of prototypes, single systems or small series.

It is applicable mainly to large hardware/software systems, but does not cover large networks, for example telecommunications and power networks, since new parts of such systems cannot usually be isolated during the testing.

##### **IEC 61164 (Reliability Growth - Statistical test and estimation methods)**

This International Standard describes models and numerical methods for reliability growth assessments based on failure data, which was generated in a reliability improvement programme. These procedures deal with growth, estimation, confidence intervals for product reliability and goodness-of-fit tests. There are several reliability growth models available, the power law model being one of the most widely used and

this standard specifically describes the power law reliability growth model and related projection model and gives step-by-step directions for their use. Two types of input are required, the first one for reliability growth planning through analysis and design improvements in the design phase in terms of the design phase duration, initial reliability, reliability goal, and planned design improvements, along with their expected magnitude. The second input, for reliability growth in the project validation phase, is for a data set of accumulated test times at which relevant failures occurred, or were observed, for a single system, and the time of termination of the test, if different from the time of the final failure.

#### **MIL-HDBK-189 (Reliability Growth Management)**

It provides procuring activities and development contractors with an understanding of the concepts and principles of reliability growth, advantages of managing reliability growth, and guidelines and procedures to be used in managing reliability growth

**Comment: There is no specific recommendation for this section. There is much development work in this area with Mil Hdbk 189 being the most recently updated.**

#### **A2.4.3 Data Collection & Failure Analysis**

Data collection and failure analysis are essential for several reasons :

- identify design deficiency for new product (or not new)
- improve RAMS criteria when they are not reached
- demonstrate these criteria during development or in service
- adjust logistic support
- contribute towards global cost management

Therefore it is used for development tests and in service.

It is necessary to define an efficient process.

#### **IEC 60300-3-2 (Dependability management - Part 3-2: Application guide - Collection of dependability data from the field) and RG Aero 00033 (Programme management - fracas : failure reporting analysis and corrective actions system)**

They are good guides to define this process with plan, responsibility, which data, process of collection and analysis, entry data, analysis method, exit data, critical point, indicators...

#### **STANAG 4158 (Guidelines for classifying incidents for reliability estimation of tracked and wheeled vehicles)**

It establishes standard definitions and criteria for classifying incidents observed during tests for reliability estimation of tracked and wheeled vehicles.

#### **ATA spec 2000 (Reliability Data Collection/Exchange)**

It standardizes record formats for collecting and exchanging aircraft reliability data. This document is for aircraft only but the mind of this document would be adapted for other systems.

**Def Stan 00-44 (Reliability and Maintainability Data Collection and Classification)**

The document is an effective guide to the processes that should be adopted for Data Collection, Incident Sentencing, Data Classification for air, land and sea products.

**Comment: These documents are complementary.**

**A2.4.4 Test method**

**ARMP-6 (Guidance for Managing In-service R&M (Reliability and Maintainability))**

It provides guidance on managing in service R&M for defence materials and annexes provide test methods.

**MIL-HDBK-781 (Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production)**

This standard specifies the general requirements and specific tasks for reliability testing during the development, qualification and production of systems and equipment. It establishes the tailorable requirements for reliability testing performed during integrated test programs as identified and specified in MIL-STD-785 (Reliability Program For System And Equipment Development And Production)

**MIL-STD-690D (Failure Rate Sampling Plans and Procedures)**

This standard provides procedures for failure rate (FR) qualification, sampling plans for establishing FR levels at selected confidence levels, and lot conformance inspection procedures associated with FR testing for the purpose of direct reference in appropriate military electronic parts established reliability (ER) specifications. Figures and tables throughout this standard are based on exponential distribution. Weibull distribution will be acceptable in certain components such as capacitors. Use of Weibull distribution for any component must be approved by the qualifying activity. This standard also provides guidance to specification writers in the use of this standard (see appendix A) and references material for users of ER parts

**IEC 61163-1 (Reliability stress screening - Part 1: Repairable assemblies manufactured in lots)**

It describes particular methods to apply and optimize reliability stress screening processes for lots of repairable hardware assemblies, in cases where the assemblies have an unacceptably low reliability in the early failure period, and when other methods, such as reliability growth programmes and quality control techniques, are not applicable

**IEC 61650 (Reliability data analysis techniques - Procedures for the comparison of two constant failure rates and two constant failure (event) intensities)**

The standard describes procedures to compare two observed failure rates, failure intensities, or rates/intensities of relevant events to determine apparent differences between the two sets of data and contains simple practical examples

**IEC 60300-3-5 (Dependability management - Reliability test conditions and statistical test principles)**

This part of IEC 60300-3 provides guidelines for the planning and performing of reliability tests and the use of statistical methods to analyse test data. It describes the tests related to repaired and non-repaired items together with tests for constant and non-constant failure intensity and constant and non-constant failure rate

**Comment: There is no specific recommendation for this section as each test method has its own standards.**

### **A3 Electronic specific standards**

The following standards are dedicated to systems that consist of electrical and/or electronic elements, including programmable electronic elements (E/E/PE). They relate to activities from specification, to manufacture through design

#### **IEC 61508 part 2 (Functional safety of electrical/electronic/programmable electronic safety-related systems)**

It specifies how to refine the E/E/PE system safety requirements specification and all requirements for activities that are to be applied during the design and manufacture of the E/E/PE safety-related systems

#### **ISO 26262 part 5 (Road vehicles - Functional safety)**

It specifies the requirements on product development at the hardware level. These include requirements on the initiation of product development at the hardware level, the specification of the hardware safety requirements, hardware design, hardware architectural metrics, and evaluation of violation of the safety goal due to random hardware failures and hardware integration and testing

#### **MIL-HDBK-338 (Electronic Reliability Design Handbook)**

This Handbook provides procuring activities and development contractors with an understanding of the concepts, principles, and methodologies covering all aspects of electronic systems reliability engineering and cost analysis as they relate to the design, acquisition, and deployment of equipment/systems

#### **ED80: (Design assurance guidance for airborne electronic hardware)**

It is intended to be used by aircraft manufacturers and suppliers of electronic hardware items for safety and certification concerns. It has been prepared to assist organizations by providing design assurance guidance for the development of airborne electronic hardware such that it safely performs its intended function, in its specified environments

**Comment: There is no specific recommendation for this section as each domain has its own standards.**

### **A4 Software specific standards**

Computers of all kinds are now widely used in systems. Thus, in RAMS activities, software topics are to be taken into account from the very beginning of the program, in order to complement other topics such as electronic, mechanic, etc

Software activities take place after system level RAMS activities, which allow specifying the necessary software development risk reduction required to achieve RAMS and functional aptitudes of a product. The system level analyses, identifying the participation of software implemented functions, can be related to safety or mission failure risks.

Software specific standards either deal with the whole process, from systems analyses to software specific activities, either focus on software activities, assessing that the system level activities have been done previously.

#### **ARMP9 Guide to the management of software R&M**

This ARMP provides an oversight of the issues / methodologies / tests / tasks that can be used when a defence product includes a software element. It recognises that software should be managed as an integral part of the whole system but acknowledges the fact that software is different, that it does not fail in the same way as hardware and requires different techniques to ensure that it is reliable. The guide is applicable to all staffs, whether in industry or in government, who are involved in development of defence equipment that contains a software element. It applies to all phases of R&M programme and all acquisitions whether acquired from design and development efforts, from production efforts, from existing stocks, or any combination of these. It discusses and presents concepts and ideas about how to develop software that has the potential to be reliable.

#### **IEC 61508 part 3 (Functional safety of electrical/electronic/programmable electronic safety-related systems)**

This standard applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. It requires that the software safety functions and software systematic capability are specified within the system analyses which identify whether functional safety is necessary to ensure adequate protection against each significant hazard. If so, then part 3 of IEC 61508 standard establishes requirements for safety lifecycle phases and activities which shall be applied during the design and development of the safety-related software.

#### **ISO 26262 part 6 (Road vehicles - Functional safety)**

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles. ISO 26262 part 6 covers, for software components in automotive systems, the same activities than IEC 61508 part 3.

#### **ED12 (Software considerations in airborne systems and equipment certification)**

This certification standard aims at ensuring a degree of rigor in the software practices, and ultimately assuring the safety of airline passengers, by following a disciplined and documented process. ED12 describes three key processes: planning, correctness and development. To assure quality yet remain flexible, ED12 defines objectives for the correctness and development processes, and the software developers must document in a planning process how the other processes meet the objectives. Despite its avionic designation, the flexibility of ED12 allows it to be used in other domains: failure condition categorization is thus to be specified for the applied domain.

#### **IEEE 1633 (Recommended Practice on Software Reliability)**

This recommended practice prescribes methods for assessing and predicting the reliability of software, based on a lifecycle approach to software reliability engineering. It

provides information necessary for the application of software reliability (SR) measurement to a project, lays a foundation for building consistent methods, and establishes the basic principle for collecting the data needed to assess and predict the reliability of software.

**BS5760-8 (Guide to the Assessment of Reliability of Systems containing Software)**

This document deals with the reliability assessment part of the software development process. It describes management techniques, statistical methods of analysis, mathematical models linked to a methodology to follow in order to assess the reliability of systems containing software.

**Comment:        There is no specific recommendation for this section.**

## **A5 Communication specific standards**

Network dependability is the ability of a network to perform as and when required and to meet users' communication needs for continuous network performance and service operation. From a user's perspective, dependability infers that the provision of network service functions is trustworthy and capable of performing the desirable service upon demand. Network dependability is characterized by its performance attributes including availability of network performance and quality of service.

The network requires specific performance characteristics in order to deliver both its service functions and communication services. Network dependability engineering is a specific risk based technical discipline intended to deal with the diverse applications and deployment of essential communication services. Unlike the system life cycle where system retirement exists, a network seldom reaches retirement. A network evolves with time to accommodate innovative feature applications and provision of continual communication service needs.

**IEC 61907 (Communication network dependability engineering)**

This International Standard gives guidance on dependability engineering of communication networks. The communication network includes telecommunications networks, Internet and intra-networks utilizing information technology. This standard describes the influence of dependability attributes and their impact on network performance. It provides the criteria and methodology for network technology designs, security service functions, dependability assessment and quality of service evaluation.

**Comment:        The need for network dependability standardization is essential to achieve cost-effective development and implementation of communication networks.**