MOD

DEF STAN 00-49 Issue 3

Defence Standard:- Final

Publication Date ** February 2014

Standards for Defence

Reliability and Maintainability

MOD Guide To R&M Terminology Used In Requirements

WARNING

This is a Draft Document

Not to be Used as an Agreed

Defence Standard

Contents

Foreword ... iii
Introduction ... iv
1 Scope ... 1
2 Related Documents ... 1
3 Terminology Used In R&M Requirements ... 2
4 Warning ... 3
Annex A – Reliability ... 4
A.1 Introduction ... 4
A.2 IEC Definitions ... 4
A.3 Reliability Guidance ... 4
Annex B – Maintainability ... 9
B.1 Introduction ... 9
B.2 IEC Definitions ... 9
B.3 Maintainability Guidance ... 9
Annex C – Availability ... 14
C.1 Introduction ... 14
C.2 IEC Definitions ... 14
C.3 Availability Guidance ... 14
Annex D – Testability ... 17
D.1 Introduction ... 17
D.2 IEC Definition ... 17
D.3 Testability Guidance ... 17
Annex E – Defining Failure ... 20
E.1 Introduction ... 20
E.2 IEC Definition ... 20
E.3 Failure Definition Guidance ... 20

Foreword

AMENDMENT RECORD

Amd No	**Date**	**Text Affected**	**Signature and Date**

REVISION NOTE

This standard is raised to Issue 3 to update its content.

HISTORICAL RECORD

This standard supersedes the following:

Def Stan 00-49, Issue 2 Reliability and Maintainability MOD Guide to Terminology Definitions dated 6 June 2008.

a) This Def Stan is designed to offer guidance, primarily to Ministry of Defence (MOD) personnel responsible for setting and managing requirements, on the terminology used within R&M and how this terminology might be tailored in order to define Specific, Measurable, Achievable, Realistic and Timebounded (SMART) requirements for different programmes.

b) This standard has been produced on behalf of the Defence Material Standardization Committee (DMSC) and the Committee for Defence Equipment Reliability and Maintainability (CODERM).

c) This standard has been agreed by the authorities concerned with its use and is intended to be used whenever relevant in all future designs, contracts, orders etc. and whenever practicable by amendment to those already in existence. If any difficulty arises which prevents application of the Defence Standard, UK Defence Standardization (DStan) shall be informed so that a remedy may be sought.

d) Any enquiries regarding this standard in relation to an invitation to tender or a contract in which it is incorporated are to be addressed to the responsible technical or supervising authority named in the invitation to tender or contract.

e) Compliance with this Defence Standard shall not in itself relieve any person from any legal obligations imposed upon them.

f) This standard has been devised solely for the use of the MOD and its contractors in the execution of contracts for the MOD. To the extent permitted by law, the MOD hereby excludes all liability whatsoever and howsoever arising (including, but without limitation, liability resulting from negligence) for any loss or damage however caused when the standard is used for any other purpose.

Introduction

The MOD considers the term R&M to be generic and interprets it to encompass related specific concepts such as availability, supportability, testability etc.

IEC 60050-191 contains the R&M terminology to be used forthwith by the MOD in R&M Def Stans. However, as the first source of reference for R&M definitions, IEC 60050-191 is to be regarded as generic and without exception will require tailoring to specific programmes.

Defining an R&M parameter for a requirement can be problematic due to the proliferation of definitions, terms and variables, many of which are subjective.

Therefore, to ensure that exact and taut R&M requirements and specifications are consistently applied in MOD contracts, it is necessary to ensure that all stakeholders have the same common understanding of the terminology used and how the variables (within the terminology) can be applied.

Standards for Defence - Reliability and Maintainability - MOD Guide To R&M Terminology Used In Requirements

1 Scope

This Defence Standard is designed to offer guidance, on the terminology used within R&M and, using examples, how this terminology might be tailored in order to define SMART requirements for different programmes.

The role of the Standard is to provide the building blocks to assist those concerned with setting requirements to understand how to adapt appropriate definitions, primarily from IEC 60050-191, in order that suitable requirements can be derived. Consequently, the definitions in Def Stan 00-49 Issue 1 are deemed obsolete.

In all cases the requirement(s) must be demonstrable, through analyses and trials if appropriate, using the R&M Case methodology. If not it is likely that achievement of the requirement can not be verified/validated and/or the User will lack confidence in the delivered solution.

This Standard contains a number of examples based on specific definitions selected from IEC 60050-191. The definitions and related terms in each example are examined to provide guidance on how the variations in their meaning might affect and be utilised in R&M requirements.

The examples, being generic in origin, are not designed to be used in their current form; they represent only a small sample of the available terminology to be used when specifying R&M requirements. Further information is obtained in the Related Documents listed below and further guidance is available from the sponsor.

2 Related Documents

The following documents and publications are referred to in the text of this Standard:

REFERENCE	DESCRIPTION OR TITLE
IEC 60050-191	International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service
IEC 60706-5	Maintainability of equipment - Part 5: Testability and diagnostic testing
ADMP-01	Guidance For Developing Dependability Requirements
Def Stan 00-42/3	R&M Assurance Guide Part 3 - The R&M Case
Def Stan 00-42/6	R&M Assurance Activity Part 6 - Maintainability Demonstrations
Def Stan 00-44	R&M Data Collection and Classification
JSP 886	A Glossary of Defence Logistics Support Chain Terms and Definitions Used In JSP 886 – The Defence Logistics Support Chain Manual
ANSI/IEEE: 610.12	Standard Glossary of Software Engineering Terminology

Within this Standard, a Reference to any related document(s) means (for any invitation to tender or contract) the edition and all amendments current at the date of such tender or contract, unless a specific edition is indicated.

The documents listed below may be obtained from the sources shown:

DOCUMENT	**DOCUMENT SOURCE**
IEC 60050-191 IEC 60706-5	IEC Central Office 3, rue de Varembé P.O. Box 131 CH - 1211 GENEVA 20 Switzerland Phone: +41 22 919 02 11 Fax: +41 22 919 03 00 E-mail: IEC Central Office www.iec.ch
Defence Standard	Directorate of Standardization Stan 1 Kentigern House 65 Brown Street GLASGOW G2 8EX www.dstan.mod.uk
Joint Service Publication Joint Service Glossary (JSP 110)	Please refer to the relevant MOD Project Team.
ADMP-1	AC/250 Secretary Armaments Planning Programmes & Policy Directorate Defence Support Division NATO HQ 1110 Brussels Belgium www.nato.int/docu/stanag
Military Standard (MIL-STD) American National Standards Institute / BERKS RG12 4DW Institute of Electrical & Electronics Engineers (IEEE): 610.12 Glossary of Software Engineering Terminology	IHS Group Technical Indexes Ltd Willoughby Road Bracknell www.techindex.co.uk www.ansi.org

The above documents are listed in order of preference and hierarchy and hence infer the hierarchal order of preference of sources of MOD R&M terminology for MOD procurement.

3 Terminology Used In R&M Requirements

Previously R&M definitions have been spread across a number of standards. Endorsing IEC 60050-191 as the first source of definitions and terminology to be used in MOD programmes will reduce this anomaly. The examples contained in this Standard give guidance on how the selected definitions and related definitions and terminology can be applied to R&M requirements.

A requirement is a need or expectation that is stated, generally implied or obligatory; failure to meet a requirement is normally a non-conformance (see Annex E). User requirements are defined within the User Requirements Document (URD). The URD is translated into the System Requirements Document (SRD) which provides the basis for a contract between the MOD and a supplier.

Many other sources of reference for R&M definitions exist (see Section 2). It is acceptable to use related definitions where they aid the readers understanding of the terminology used. However, the common areas between the IEC publication and other definitions should remain paramount (i.e. the IEC definition is the first source of reference); all definitions used should include a clear reference to their origin.

Where IEC 60050-191 does not include a suitable definition, Basic Reliability for example, a suitable alternative source should be used.

Some fundamental terms that frequently occur throughout this Standard are:

Item [IEC 60050-191]. An item can be a part, component, device, subsystem, functional unit, equipment or system that can be individually considered. An item may consist of hardware, software or both. A group of items (e.g. a population of items or a sample), may be considered an item.

System [IEC 60050-191]. A system is a set of interrelated items considered together for a defined purpose. A system is generally defined with a view of performing a definite function. Typically it forms a hierarchical structure e.g. system, subsystem, component etc. A subsystem [IEC 60050-191] is a system that is part of a more complex system being considered.

Platform. Platform is used as a generic term in this Standard to refer to a solution; e.g. a vehicle, aircraft, ship, network, etc.

The definitions selected from IEC 60050-191 as worked examples are contained in the Annexes as follows:

Annex A	Reliability
Annex B	Maintainability
Annex C	Availability
Annex D	Testability
Annex E	Failure

Note that in order to fulfil the role of this Standard the use of actual definitions is avoided where possible, except at the beginning of each worked example. Subsequently, when a term is used for the first time, the source of a suitable definition, if appropriate, is included in parenthesis following the term; e.g. reliability [IEC 60050-191].

4 Warning

The Ministry of Defence (MOD), like its contractors, is subject to both United Kingdom and European laws regarding Health and Safety at Work. All Defence Standards either directly or indirectly invoke the use of processes and procedures that could be injurious to health if adequate precautions are not taken. Defence Standards or their use in no way absolves users from complying with statutory and legal requirements relating to Health and Safety at Work.

Annex A – Reliability

A.1 Introduction

It appears obvious that requirements should call for very high values of reliability, as this would mean that systems would fail less frequently and consequently cost less in service. However, the risks arising from new (often unproven) technologies and the potentially high costs of achieving and/or demonstrating high reliability must be balanced with what is realistically acceptable. In practice this means delivering to the User the capability to accomplish (and if necessary sustain) a mission at acceptable technical risk with the minimum cost (taking a risk based approach to requirements setting is ideal). Reliability requirements must be realistic and attainable - they should be what are required by the User not what might be desirable.

Therefore, it is important to specify the minimum acceptable levels of reliability and, in combination with maintainability and availability, to do so in a manner that does not impose undue constraints on the designer. It is important to avoid unnecessary limitations on the designers' capacity and flair to achieve a satisfactory balance between R&M, performance and cost.

A.2 IEC Definitions

IEC 60050-191 defines reliability as follows:

> Reliability (as a performance measure) is the probability of being **able to perform** as required under **given conditions** for the **time interval**
>
> Reliability (of an item) is the **ability to perform** under **given conditions** for a given **time interval**.

A.3 Reliability Guidance

A statistical parameter such as reliability cannot be measured directly and repeatably. It can only be measured to a level of confidence. Confidence Levels, and their use in requirements, can be a complex area to cover in a short example; further reading is therefore recommended. The list of Related Documents in this Standard provides suitable reference material.

Typically different levels of reliability will be set for different levels of functionality with critical functionality having higher levels. For vehicles this is typically set as:

> **Mission reliability** [IEC 60050-191] is the probability that an item will **perform** its **required functions** for the duration of a specified **mission profile**
>
> **Basic reliability** is the ability of an item to **perform** its **required functions** without **failure** or **defect** for the duration of a specified **mission profile**
>
> **Peacetime reliability** can be defined in similar terms to mission reliability however; the 'mission' could be any task that the User undertakes outside a theatre of war or operation other than war.

While for other systems it might be set as:

> **Critical reliability** is the ability of an item to **perform** its **Critical functions** without **failure** for the duration of a specified **mission profile**. Where Critical may refer to safety and/or mission critical function
>
> **Major reliability** is the ability of an item to **perform** without **lost of major functions** for the duration of a specified **mission profile**
>
> **Minor reliability** [IEC 60050-191] is the probability that an item will **not suffer minor failures** for the duration of a specified **mission profile**

Where mission profile is a “typical use profile” specifying how the system will be used and what functionality is needed during the mission. For a simple system this may be fully functioning for a given time, while for a more complex system this may show what functionality is required on an hour by hour basis over a long duration.

Generally speaking mission or critical reliability is the value used to denote the chances of a platform successfully completing an agreed given scenario which for a land based solution may be referred to as a Battle Field Mission (BFM), an aircraft a sortie, etc. Consequently it is the most important reliability characteristic in terms of evaluating operational effectiveness.

Basic or minor reliability relates to all other failures requiring maintenance or restore actions that do not directly affect the mission. All corrective maintenance actions are counted, from changing a main assembly to unscheduled minor adjustments. Basic reliability (which includes all basic and mission failures) determines the burden of effort, costs etc arising from corrective maintenance.

Peacetime reliability can be calculated from the combination of all attributable (mission/task) failures and all critical failures judged to contravene safety / environmental legislation. It is possible, depending on local legislative demands (and the User's obligations in meeting them), that a version of a peacetime failure definition must be specified for an operational deployment.

In order to tailor reliability requirements exclusively for each programme the available terminology (from IEC 60050-191 as a first source) must be fully understood. The following examples give guidance:

Able to Perform

Being able to perform, and performance in general, is concerned with the limiting boundaries of the required functionality of an item. In order to achieve the mission the User's limits (often the lowest acceptable limits, otherwise known as threshold values) are normally specified. For example:

> Maximum forward/reverse speed must be achievable
>
> Maximum rate of turn must be achievable
>
> The minimum specified number of communication channels must be available
>
> The minimum specified distance over which it is possible to detect and locate a threat must be sustained
>
> A minimum average speed of 30 km/h should be sustainable during the mission

Alternately, if measurable, a permissible amount of degradation (a typical threshold value) may be acceptable if the mission would otherwise be unaffected; for example:

> Degradation in engine power of <20% is acceptable
>
> The sustained achievement of <20% of the maximum attainable speed is acceptable

Alternately the inability (or failure) of an item to perform within the specified limits (or to achieve the threshold value) is the cause of non-conformance (see Annex E).

Note that R&M requirements are themselves vital performance characteristics that impact upon the operational availability, the effectiveness and the whole life costs of defence equipment.

Given Conditions

Environmental and operating conditions have a fundamental impact on reliability and should therefore be stipulated in the requirements. Platforms will typically exhibit different reliability values depending on the local environment / conditions. The related characteristic of durability [IEC 60050-191], which is an item's ability to resist the adverse effects of environment, use and maintenance with the progress of time, can be specified to complement a reliability requirement.

Environmental conditions can include temperature, pressure, chemical, dust etc and includes the way in which an item is used, stored and transported. Shelf life is often an important characteristic as the length of time an item can be stored under specified conditions and still meet specified (reliability) requirements can be crucial.

Operating conditions can vary from the environmental extremes found during operation on desert tracks to the relatively benign conditions on normal UK roads. Platforms intended for extreme use are normally designed or modified for such conditions.

Similarly, the mission profile, a time-phased description of the events and environments an item experiences from initiation to completion of a mission, should be specified. The profile identifies the tasks and events (ideally mission essential, critical and non-critical events), durations, operating conditions and environments for each phase of a mission.

Mission and basic reliability requirements are concerned with the environmental conditions to be expected during any mission, reflected in the scenario. Peacetime reliability is concerned with the environmental conditions that will be experienced in the conduct of any routine task in the specified theatre of peacetime operation.

Reliability tests and trials may be specified to mirror the intended in-service conditions (whether they are operational or peacetime in nature). Testing can be designed to imitate the in-service conditions for which the requirement is set however, any dissimilarity between the reliability trial and the real situation may require factoring.

In order to specify reliability growth (where failures are actually encouraged) and to induce them to happen more frequently, it may be necessary to overstress the item by testing in a harsher environment. Note however, if this route is taken the results should be viewed with caution as the harsher environment may cause different (unrealistic) failure modes to occur.

Similarly, the results presented to satisfy a requirement, if obtained from testing on the same or similar equipment (perhaps used by commercial operators in a similar physical environment, for example, aircraft or marine engines) should be treated with caution. Appropriate allowances may have to be made before the data is used, as it is possible that the operational and support environments, in which the results are based, may differ from the intended environment.

Time Interval

Time intervals are necessary in order to define the period of usage (normally the mission duration) that matters to the User. They can provide a framework to measure pass / fail criteria and against which to demonstrate that the requirements have been achieved. Typical examples are an operational sortie for an aircraft, a battlefield day for an armoured fighting vehicle, a 3-month deployment for a ship or a 12-month period for a headquarters based communication system.

For mission and basic, or equivalent, reliability the time interval is the expected operating time, defined by the mission/scenario. For peacetime reliability the time interval is the peacetime operating profile.

Operating time [IEC 60050-191] is the time period, during a mission, when it is essential that the item is required to be in an operating state.

Conversely, non-operating time [IEC 60050-191] is when an item is not required to perform a required function. This can be specified in order to optimise reliability (and availability). For example an item might be switched off (or to standby), to prolonging its life expectancy, and only switched on when required. This standby time [IEC 60050-191] is the time interval for which a standby (non-operating time) exists and the required time [IEC 60050-191] the time interval for which the User requires the item to be in an up-state (available).

Useful life [IEC 60050-191] is the time period from a given instant, typically first use, until an instant when a limiting state is reached, typically a failure event, physical condition, obsolescence or life limited point. Items that are life limited have a limited and predictable useful life, and can be considered for replacement on a pre-planned basis. Life limited items can impact reliability calculations and improve availability as downtime can be pre-planned (a life limited item cannot normally be classified as a failure if the life limit has been exceeded).

Inactive time is the time when an item is required to be inactive or non-operational. The distinction between inactive time and down time is that down time implies that the item is dysfunctional during a required period, whereas inactive time would only mean that the item is not required to be operational (available). Specifying inactive time should be used with caution. For example, specifications should be clear regarding start-up checks or deployment activities, as failures encountered during these periods can affect the mission that follows. Similarly, during a trials programme, the intervals between missions may be considered inactive if the mission reliability and any associated targets are adequately defined (i.e. the duration of the interval was deliberately considered/omitted from the target).

Required Functions

In order to set SMART requirements it is important, during concept studies of new equipment or a new capability, to establish fully what functions are required. Required functions, specified with their level of criticality, enable the successful completion of the task or mission.

Required functions [IEC 60050-191] are a characteristic or a combination of characteristics considered necessary to complete a mission or task. It may be described as the range of measurable characteristics of which an item is required to be capable in order to meet a requirement. The functions may be stated in a technical specification; but some expectation, such as what an item should NOT do, may be included.

In a complex system that is capable of many functions, some of which may not be continuously required during a mission, it is often necessary to introduce the concept of a mission essential function. In such a case a mission failure would result from a fault preventing the equipment from performing one or more of its mission essential functions.

For mission reliability the required function is that the equipment is able to sustain all mission essential functions during the scenario/agreed operating time. Importantly the specified failure criteria should define the conditions under which the equipment no longer carries out these functions.

For basic reliability, the required function is that the equipment shall sustain continuous usage either without the need for corrective maintenance or within specified limits.

For peacetime reliability the required function is that the equipment shall sustain continuous usage for the peacetime profile either without the need for corrective maintenance or within specified limits.

Whilst the specified mission/scenario should reflect the expected use of each platform, it is preferable where possible to maintain a standard mission/scenario from which to work, changing it (or aspects of it) only where the functions genuinely differ. This will increase the ease of comparison of achieved reliability across a fleet. The mission/scenario should cover all aspects of the requirement, not only movement but also special-to-role operations. The mission/scenario is therefore usually given in two or more parts; the first, typically, for the automotive functions and subsequent parts for the special-to-role function(s), defence aid suite and so forth.

Mission / Life Profile

Full consideration should be given to the nature of a platform's role before deciding its likely usage profile. This is true for both the operational and peacetime profiles. For instance, heavy tank transporters are specialised and expensive and high utilisation is therefore to be expected. Motorcycles, however, have limited peacetime functions and consequently experience low utilisation.

In peacetime operation the probability of some vehicles covering considerably more than the average usage, while others are stationary for long periods, must be recognised and the reliability implications considered. This may prove to be a characteristic of whole fleet management and should be factored into the requirements.

The life profile is a time-based description of the typical events and environments an item experiences from manufacture, to the out of service date. It normally includes, for the purposes of evaluation / requirement specification, one or more mission profiles.

See also Given Conditions above.

Failure / Defect

See Annex E – Defining Failure.

Annex B – Maintainability

B.1 Introduction

Normally, it is essential that high levels of reliability **and** maintainability are achieved to ensure adequate availability and acceptable through life costs. Whilst availability is likely to be the required parameter, if availability alone was specified there is a danger that this may be achieved by a low level of reliability and a high maintenance load, or vice versa. Consequently, specifying the minimum acceptable levels of reliability and maintainability should lead to the required availability.

B.2 IEC Definitions

IEC 60050-191 defines maintainability as follows:

> Maintainability (as a measure) is the probability that a given **maintenance action**, performed under **stated conditions** and using **stated procedures** and **resources**, can be carried out within a **stated time interval**.
>
> Maintainability (of an item) is the ability to be **retained** in, or **restored** to a state in which it can **perform as required**, under given **conditions of use** and **maintenance**

B.3 Maintainability Guidance

Maintainability is a measure of the ease and the time required to return systems to or keep them in their fully functioning state. At the highest level, maintainability can be viewed as an output of the overall support programme; for example if the design is maintenance tolerant; if the correct repair levels are stipulated, if appropriate training is delivered, if the correct technical information is distributed and if the supply chain is designed efficiently; achieved maintainability levels should be high.

Two types of maintenance are normally defined, preventive maintenance which is carried out at prescribed intervals or usages, and is intended to prevent the platform from failing, and corrective maintenance which is carried out after the item/system has failed.

In order to tailor maintainability requirements exclusively for each programme the available terminology (from IEC 60050-191 as a first source), must be fully understood. The following examples give guidance:

Maintenance / Maintenance Action

Maintenance [IEC 60050-191] includes all action taken in order to retain or to restore an item, system etc to a specified level of performance. It combines all necessary technical and administrative actions (see Annex C).

Maintenance action [IEC 60050-191] is the sequence of elementary steps taken by the Maintainer and includes fault diagnosis; fault localisation and restoration (see Annex E for fault terminology).

Note that the related term of perfective maintenance [IEC 60050-191] (of software) relates to software maintenance conducted to improve the performance, maintainability, or other attributes of a computer programme. In turn, software maintenance [IEC 60050-191] is any software modification for the purposes of fault removal, adaptation to a new environment, or improvement of performance of a computer programme.

Preventative Maintenance

Preventative maintenance [IEC 60050-191] is maintenance carried out to reduce the chance of failure or degradation (see Annex E). Preventative maintenance is ideally planned to take place at usage intervals as actual usage is generally associated with wear-out rates.

Alternately, scheduled maintenance [IEC 60050-191] can be specified. Scheduled maintenance is often time based for convenience (or where item failure is more directly related to time) or better still condition based (commonly referred to as on-condition maintenance). Conditioned based maintenance is conducted, if necessary, following an investigation to establish the condition of the item. Specifying condition based maintenance can realise cost savings through life as the objective is to extract the maximum useful life from items.

A preventative maintenance programme is often derived from a Reliability Centred Maintenance (RCM) [IEC 60050-191] approach. RCM is a systematic method that focuses on the reliability and consequences of failure when determining the respective maintenance tasks and frequencies.

Corrective Maintenance

Unscheduled maintenance [IEC 60050-191] is maintenance carried out at any time to correct a fault or a degraded condition. An unscheduled or corrective maintenance [IEC 60050-191] task would be carried out after a fault was recognised to effect restoration (see below). Note that corrective maintenance also applies to life limited items that have failed prematurely. Unless identified as life limited, all fitted items are normally assumed to have a life of at least the required life of the platform.

Basic reliability (see Annex A) can be viewed as a measure of the total corrective maintenance load. Generally speaking this means the total burden of corrective maintenance activity including active repair time, resources, facilities, spares and costs etc resulting from mission and non-mission failures.

Stated Conditions / Conditions of Use

The mission profile is the normal mechanism to define the in-service conditions of use, including any extremes. The profile identifies the operating tasks and events, durations, operating conditions and environments for each phase of a mission.

Environmental and operating conditions can have an impact on maintainability, and should therefore be stipulated in the requirements. Depending on the local environment / conditions (desert conditions for example) custom-built or customised facilities may be required by the Maintainer to ensure that established maintenance times (and therefore the expected availability requirements) can be achieved.

Operating conditions can vary significantly and include extremes of e.g. temperature, pressure, chemical, dust etc including any changes in operating methods due to these extremes (changing an engine oil to a product that has a more suitable temperature range). The Maintainer may require specialist clothing or personal protective equipment that in-turn constrains the Maintainer's ability to conduct a task. Platforms, intended for use in extreme environments, should have specified conditions of use detailing such extremes including any known measures taken by the User, or that might be required by the User, to function (e.g. specialist clothing and /or equipment).

Preventive maintenance is typically prohibited from the mission/scenario, and certainly during mission critical periods, when an item, system etc is required to be in an operating state. Similarly, the peacetime mission/task profile would normally exclude scheduled maintenance.

If appropriate, corrective maintenance may be permissible during a mission/scenario if the failure can be restored on time to allow the mission to conclude on time or be successfully restarted and concluded from that point.

The stated conditions also apply to the level/line at which maintenance is conducted (levels, lines and depths of maintenance are detailed in appropriate service doctrine). The maintenance level [IEC 60050-191] refers to a maintenance task categorised by its complexity. A line of maintenance [IEC 60050-191] is the position in an organisation (or echelon) where specified levels of maintenance are to be carried out. Each maintenance echelon is characterised by a combination of the level of skill of the personnel, the facilities available, the location etc.

Additionally, the conditions specified to allow effective maintenance may include accessibility to items and/or suitable space. Storage, including the conditions found in whole fleet management and humidity controlled environments, may require specifying in order to determine suitable and appropriate maintenance regime(s).

With an increasing dependence on Contractor Logistic Support, specifying maintainability requirements above User maintenance levels (i.e. at levels/lines/depths where the User has no direct role) may be unnecessary. Limiting the requirements to those levels/lines/depths where the User conducts maintenance can achieve the required availability levels; the contracted support being responsible for delivering the availability specified at the higher levels/lines/depths.

If necessary, a maintainability demonstration can be designed to imitate the in-service conditions for the intended environment. The trial conditions must be representative (i.e. accessibility, tools, technical documentation, lighting etc). Environmental chambers, for example, can be used to evaluate maintenance procedures in temperature extremes, however, not unlike reliability testing any dissimilarity between the trial conditions and the real situation should be considered.

Stated Procedures

The stated procedures relate to the documented processes and practices that the User must employ to correctly operate and maintain a system.

The processes typically originate from the Training Needs Analysis (TNA), and Operator and Maintainer tasks analyses, which should be specified for the programme. The former evaluates the target audience (the intended Operators / Maintainers), and establishes any skill pre-requisites, before identifying the gap in skills that must be addressed in the training programme.

A typical pre-requisite might recognise that a basic driving skill is required before the training programme can deliver the additional familiarisation or specialist training to the User on a particular platform. Alternately, a Maintainer may require a basic skill as a tradesman (e.g. vehicle mechanic), as a pre-requisite to attending a training course, that familiarises the tradesman with new maintenance techniques appropriate to a special-to-role equipment.

Task analyses will produce detailed processes that the User must employ to operate and maintain a system to achieve the optimum performance and availability. It will typically derive tasks to operate and maintain equipment (on a step-by-step basis), resources, tools, facilities, spare parts and all consumables required.

Typical practices may include military standing operating procedures, or equipment support directives, that guide the User toward mandated procedures. The time constraints associated with each maintenance level/line/depth is one such practice.

The stated procedures and practices must be documented (electronically, in hard copy etc) in a manner that the User finds acceptable and effective. The requirements should state the preferred format or options.

Resources

The applicable resources should be prescribed in the maintainability specification and requirements. The personnel skill levels, trade types and numbers available and the applicable levels/lines/depths should be included.

Resources also include appropriate facilities, tools, test equipment and the spare parts and consumable items delivered by the supply chain.

The non-availability of resources is a major contributor to logistic delay (see Annex C).

It is also prudent, certainly at User maintenance levels, to specify the maximum available time for repair at each level; current doctrine and the Users requirements should inform the values to be used. Defining the maximum available maintenance time at each level, together with the number of Maintainers allowed to conduct a maintenance task, can ensure that the system can be supported and resourced at the appropriate echelon.

Related to the available time and number of Maintainers, maintenance manhours (MMH) [IEC 60050-191] can be specified. MMH includes the sum of the individual personnel times taken to carry out a maintenance action. MMH is a therefore a measure of resource use, and not the duration of maintenance.

Stated Time Interval

Maintenance time [IEC 60050-191] is the time taken to perform maintenance and includes the active preventative and active corrective maintenance time as well as all time due to logistic delays.

Active maintenance time [IEC 60050-191] is that part of the overall maintenance time taken to physically perform a maintenance action and therefore includes fault isolation, diagnosis of failure and subsequent testing; logistic delays are excluded.

It follows that active preventative maintenance time [IEC 60050-191] is the part of active maintenance time taken to physically perform preventative maintenance and active corrective maintenance time [IEC 60050-191] that part of the maintenance time taken to physically perform corrective maintenance.

Correspondingly, preventative maintenance time [IEC 60050-191] is a part of the maintenance time, and is the whole time taken to complete preventative maintenance, including the logistic delays affecting a task or combination of tasks. Similarly, corrective maintenance time [IEC 60050-191] is the whole time taken to perform corrective maintenance, including logistic delays.

Mean Time To Restoration [IEC 60050-191] also known as Mean Time To Repair is the sum total of the average of the maintenance times for an equipment (normally limited to corrective maintenance), factored by the frequency of each repair (typically the failure rate). It can be problematic to specify as logistic delays are included, which are often difficult to quantify or measure.

More often maintainability requirements are specified in terms of a Mean Active Repair Time or Mean Active Corrective Maintenance Time [IEC 60050-191], the former including both scheduled and corrective maintenance. The expected values result from the sum total of the average active scheduled/corrective maintenance times respectively factored with their frequency of repair.

Retained / Restored

Restoration [IEC 60050-191] re-establishes an items ability to perform as required after a failure. Normally an unsatisfactory condition, because equipment is unlikely to be available for the duration of the restoration activity, an item can be permitted to fail if the cost of doing so is justified and the impact on availability is acceptable. Note that in certain instances, where standby redundancy exists for example, restoration may be carried out whilst the system is still operating. Repair [IEC 60050-191] is the direct action taken to conduct restoration.

Retaining the system in an operational state is normally preferable and relies on scheduled or on-condition maintenance during periods when equipment need not be operational, to deliver high availability. The RCM methodology can be used to determine a maintenance regime that considers scheduled downtime and promotes high availability. Systems incorporating Health and Usage Monitoring Systems (HUMS) e.g. MIMIC (an asset condition monitoring system) as fitted to RN platforms, and prognostics can improve availability still further. HUMS and prognostics should be specified if appropriate as through life costs can be reduced, availability increased and data capture (for R&M evaluation) improved.

Perform as Required

Being able to perform is concerned with the limiting boundaries of the required functionality of an item.

Ideally, scheduled or corrective maintenance would be expected to return an item to an as new condition. However, this may not always be operationally feasible or financially sound. Overhaul typically involves the complete disassembly inspection, rework and reassembly, of an item and is required to restore the item to a `like new' condition.

Corrective repair / restoration activities by the User are primarily designed to return an item to a condition where it can function for the duration of the mission. This is particularly true when battle damage repair techniques are employed by the User. These techniques can be specified as an option to hasten repair time so providing immediate, if short term availability. The longer term impact of battle damage repair, the potential accumulation of maintenance tasks required to address the shortcomings of each battlefield repair, should, if possible, be considered in the requirements and when evaluating a maintenance concept.

Whilst the User's objective is normally to complete a repair to a high engineering standard (particularly when repairs are carried out 'in barracks' or on training) the reality is often constrained by the time, resources etc available on an operation and at first line in particular. Consequently, maintenance techniques and maintenance requirements should recognise that restoration to the threshold values of performance, if identifiable, may be satisfactory.

For example, from Annex A, a typical repair technique might deliver acceptable performance if, following a repair, an engine delivers power in excess of a specified 80% threshold level, meeting the requirement.

Annex C – Availability

C.1 Introduction

There are many inter-related issues that affect availability, and making a judgement on what is an acceptable level can be a complex process.

Contractor Logistic Support (CLS), Contracting for Availability (CfA) and even Contracting for Capability (CfC) are increasingly taking over from the more traditional 'spares and repair' acquisition programmes. CLS, CfA / CfC contracts present a challenge when setting requirements and specifications. However benefits could include reduced costs and higher availability.

Understanding the terminology takes on increasing significance if SMART requirements are to be specified. Availability requirements are normally Key User Requirements (KURs) due to their direct relationship to mission success. The requirements must be operationally justified as well as technically and economically achievable.

C.2 IEC Definitions

IEC 60050-191 defines availability as follows:

> The availability (of an item) is the ability to be in a **state to perform as required**, under **given conditions**, at a **given instant,** or over a **given time interval**.
>
> Intrinsic/inherent availability is the value determined when **maintenance** and **operational conditions** are assumed to be ideal.

C.3 Availability Guidance

Availability can be defined in a number of ways, notably an unquantifiable definition of availability used on a programme is of little use. Availability is normally defined for a single platform or system but modelling tools can evaluate or define availability for a given fleet size.

For MOD requirements the terms in most common use are Intrinsic (or Inherent) Availability (Ai) and Operational Availability (Ao); importantly:

> **A_i** includes the **downtime** under the control of the designer and therefore excludes **logistic delays**.
>
> **A_o** includes all contributions to **downtime**, including **logistic delays**.

Ao is the actual level of availability achieved in the routine operation of the system (routine including deployed operations if applicable). It takes account of the effectiveness of the maintenance echelons and the logistic supply chain.

With the arrival of contracted support, availability can also be defined in other ways, for example, within the context of readiness; where readiness levels may be used in place of availability. In a service provision (for example a private finance initiative or CfC), a contractor may assume responsibility for a vehicle fleet for the greater part of its life; responsibility for the operation and maintenance of the fleet passing to the User for relatively short periods of time; typically for an operation or peacetime task.

Ready (available) in the context of a service provision normally includes a guaranteed commitment by a contractor to achieve the agreed readiness states (see below).

In order to tailor availability requirements exclusively for each programme the available terminology (from IEC 60050-191 as a first source), must be fully understood. The following examples give guidance:

State to Perform as Required

The ability to be in a state to perform as required depends on the combined aspects of the reliability and maintainability of the item, and the maintenance support performance or recoverability [IEC 60050-191] of the item. Recoverability is the ability to achieve restoration (with or without repair) following a failure, for example:

A computer system may automatically reboot requiring no further intervention

External action such as a corrective maintenance task might be required to restore the item to an operational state.

A reliable system will tend to perform as required, where the required performance was initially achieved. Early life failures (infant mortality), acceptable (low) steady state failure during the useful life, and age related wear, all impact this ability. Specifying reliability requirements that address all of these areas will deliver satisfactory performance and acceptable availability.

Similarly the ability to retain a platform in an operational state, or to restore an item quickly to its operational state following failure, can deliver high availability when correctly specified in the maintainability requirements.

Alternately, to meet a readiness state, a system/platform/fleet is typically considered ready for use when it is:

Compliant with legislation;

Maintained in accordance with the contractor’s technical documentation;

Has an initial or priming spares pack to the agreed contractual levels;

Is of a type and specification that has passed the relevant demonstration tests and

Is delivered (in the correct quantities) on time to an agreed (User) handover point.

The exact number of platforms would normally be specified, perhaps at different readiness states e.g. readiness state 1 might require 20 platforms (from a fleet) to be in a state in which they could be ready (for handover) within 3 days. Readiness state 2 might require the remaining fleet to be ready (for handover), possibly with trained Operators and Maintainers (who may be reservists) within 20 days.

See also Annexes A and B

Given / Stated Conditions

Environmental and operating conditions can have a fundamental impact on R&M, and in turn availability, and should therefore be stipulated in the requirements.

The mission profile is the normal mechanism to define the in-service conditions of use, including any extremes. The profile identifies the operating tasks and events, durations, operating conditions and environments for each phase of a mission, and should be specified.

Peacetime availability is concerned with the conditions that will be experienced in the conduct of any routine task in the specified theatre(s) of peacetime operation. The peacetime operating profile should identify the scope of expected tasks, events, durations, operating conditions and environments that can be encountered, and should be specified.

See also Annexes A and B

Availability and Time

Availability is normally a measure of the proportion of total time that a platform/fleet is available for use, but may also be used to determine for example how many platforms must start an operation/task (in order to theoretically execute a mission/objective).

Readiness is more closely associated with availability at any given instant. The availability of an item will change with time. It may always be 100% available (or ready) at the start of a mission but will tend to a steady-state value over time.

The operational and maintenance conditions in Ai are assumed to be ideal. Therefore any free time, storage time, Administrative Logistic Delay Time (ALDT) and logistic delay time are not considered.

Specifying the operating conditions is vital to achieve the desired availability. The required operating time (the time period, during a mission that an item is required to be in an operating state) should be specified and, if appropriate, any critical operating time or allowances for maintenance.

Ao includes all causes of downtime [IEC 60050-191], the time interval for which a downstate [IEC 60050-191] exists; it excludes disabled time due to a lack of external resources, but includes maintenance. An item/system is in a downstate when it is unable to perform as required due to a fault or maintenance activity.

Conversely, up-time is the time interval for which the item is in an up-state [IEC 60050-191]. The up-state represents the time when an item/system is able to function as required.

Consequently, the maximum Ao comes from achieving as little downtime as possible for a given uptime. Measures to be considered/specified to maximise Ao can include additional platforms; redundancy; the use of diagnostics, prognostics and HUMS; additional spares carried forward (reducing logistic delays); up skilling the User (reducing time waiting for resources) and on-line technical support (to assist User diagnostics / reduce restoration time).

Similarly, the higher the reliability achieved (or specified) the less influence downtime (due to maintainability) has on Ao (not forgetting the risks involved due to either the potentially high costs involved or the reverse situation where high availability can be achieved with low reliability and correspondingly 'high' maintainability).

Logistic delay [IEC 60050-191] is the accumulated time, excluding administrative delay, taken to provide the resources needed for maintenance to proceed. It includes travelling time, awaiting spare parts, specialists, facilities, test equipment, information or suitable environmental conditions. Logistic delay has been shown to be the most significant logistic support metric that impacts on Ao; it is time lost and directly impacts Ao. As logistic delays can, depending on the programme, be problematic to quantify or agree, Ao requirements are often avoided in favour of a combination of Ai, reliability, maintainability and other related requirements.

Logistic delays are made up of a combination of factors therefore, and the elimination of some, coupled with the balance of others, needs to be investigated. Reducing logistic delay can be achieved through the formation of an efficient support chain, i.e. having the right resources (support/materiel) in the right place at the right time. For example, reduction of logistic delay can be achieved by the use of HUMS to reduce latency. Reductions can also be realised by having a radical re-think of the support policies (using CLS, CfA or CfC for example) or by determining the most efficient location to hold spares or to conduct maintenance.

ALDT is the accumulated time for which maintenance cannot proceed due to administrative reasons. An example is awaiting authorisation to proceed/or to access the item to be maintained. ALDT represents an additional factor affecting downtime.

Annex D – Testability

D.1 Introduction

Testability [IEC 60050-191] is an important design feature that can have a significant impact on availability. Testability affects reliability as defects not detected by tests can lead to failure in service. Testability is an important feature in the operation and maintenance of a system or equipment, and has a significant effect on its maintainability.

Items that are difficult to test are more likely to be inadequately or incorrectly repaired. The design of electronic systems for improved reliability and maintainability should be specified in requirements. Good testability will avoid the need for adjustments, or ensure that necessary adjustments are easily conducted, maximising the commonality of items and offering diagnostics that identify items/sub-assemblies that can be easily replaced, improving maintainability.

D.2 IEC Definition

IEC 60050-191 defines testability as follows:

> The degree to which an item facilitates the establishment of **test criteria** and the **performance of tests**.

IEC 60706-5 Ed 2.0 defines testability as:

> A design characteristic which determines the degree to which an item can be **functionally tested** under **stated conditions**

D.3 Testability Guidance

Through life costs is an increasingly important aspect in evaluating the quality of any design. In addition to the immediate acquisition cost, it is important to understand the costs associated with day to day operation, maintenance and logistic support. These costs are primarily influenced by the product's reliability, maintainability and maintenance support characteristics.

The efficient and cost effective operation and maintenance of systems is improved by ensuring that testability is considered during design. Diagnostic testing [IEC 60050-191] methods are then incorporated into the system as a component of the maintenance concept. Implementation of testability and diagnostic testing are accomplished throughout the life cycle of a product.

Testability is a design characteristic of a product which guarantees that its functional capability can be assessed in a timely and efficient manner and that faults can be recognised and, where necessary, localised. It is a primary component in ensuring good maintainability of a product.

In order to tailor testability requirements exclusively for each programme the available terminology (from IEC 60050-191 as a first source and IEC 60706-5) must be fully understood. The following examples give guidance:

Test Criteria

In order to enable optimum design, development and supply of diagnostic test procedures, a detailed specification of testability requirements and constraints should be provided in a testability specification.

In the assessment and development phases, testability features and characteristics should be incorporated into the design in accordance with the results of related initial trade-off studies.

Testability can be characterised by a number of features including fault recognition, fault localisation [IEC 60050-191] and diagnostic testing.

The possible procedures which can be applied for diagnostic testing range from the purely manual measurements and evaluation of mechanical characteristics, to the fully automated diagnoses of entire processes and installations, with the testing of single components and complex systems. The broad diagnostic methods applied fall into two main categories:

> External diagnosis that utilises test equipment, discrete from the product, which is only connected when required. The test equipment used may be of a general purpose nature, adapted for the purpose from standard, or specially designed for the equipment to be tested. Computer controlled Automatic Test Equipment (ATE) may also be involved.
>
> Internal diagnosis utilising permanently Built-In Test Equipment (BITE) [IEC 60706-5] which may be continuously or intermittently operated during the operation of the system. In addition, special tests, in the reduced or non-operating state of the system, may also be performed.

Performance of Tests

BIT is the integrated capability of a test item enabling automatic fault recognition and fault localisation. BIT forms part of the range of functional tests conducted on a system and is divided into on-line and off-line tests. On-line tests are those that are conducted continuously while a product is in operation. BITE is the hardware and/or software assigned to the BIT.

Where external test equipment is needed, then accessibility is normally provided (specified) via test inputs (e.g. test connectors).

Specific consideration should be given to diagnostic testing techniques as these have the potential to improve the system's maintainability and minimise downtime, thus increasing availability and decreasing support costs. In the case of items with inherent wear-out characteristics, improvements primarily affect the cost of preventive maintenance, which can be significantly decreased by diagnostic test procedures.

In addition to diagnostic testing, which tests for discrete faults, many systems also benefit from condition monitoring [IEC 60050-191]. This is performed as a part of preventive maintenance to monitor degradation of condition and performance.

Condition monitoring is closely related to diagnostic testing and is intended to track the condition of equipment that degrades over time. Methods used for condition monitoring will vary with the type of equipment and may be sufficiently diverse to include vibration analysis; fluid/lubricant analysis; ultrasonic detection, or alarms and shutdowns built into the control system.

Diagnostic testing is a test procedure carried out in order to make a diagnosis. It aims to provide the most cost effective, rapid and unambiguous method of fault identification to a level determined by the maintenance concept for the equipment under test.

Diagnostic testing consists of two steps:

> Fault recognition is when a fault of a function or item is recognised on-line or off-line; it identifies whether a fault exists.
>
> Fault localisation determines the specific nature of the fault and allows the fault location to be confidently determined (after the recognition of a fault).

Functionally Tested

A function is always associated with an item of a given level in the system breakdown structure. A function is a manifestation of the physical characteristics with the associated parameters.

For a product to retain its functionality, the functional status of each sub-function should be known at any time while the product is in its operating condition. All the expected functions/functionalities, including testability, should be specified including all the functional requirements related to testing.

Functional testing is testing of all the specified functions of hardware units (design elements which represents functions and/or sub-functions in the form of hardware, possibly including software components) to prove their functional capability.

It is a basic principle in the design of testability that all functions developed should be verifiable. It should, however, be noted that test coverage of 100 % is not necessarily desirable, as testing can create failures that manifest themselves during operation, which may be worse than not testing, e.g. real failures may be introduced by testing or false alarms.

The false alarm rate is one of a number of parameters that characterise testability and represents the number of declared failures that are later identified as not being failures over a defined period. A maximum false alarm rate would normally be specified.

Testability is the design characteristic of a system which guarantees that its functional capability can be assessed in a timely and efficient manner and that faults can be recognised and, where necessary, localised. It is a primary component in ensuring the maintainability of a product.

The main objective of testability is to address the following questions for each of the system functions:

> Can the function’s failures be detected by a diagnostic test?
>
> Is it practical to test? The criticality of the function’s failure, the test costs (the test equipment cost, the test equipment maintenance costs as well as the test activity costs) and the use of better and cheaper alternatives may result in the conclusion that it is not cost effective to test.
>
> To what depth should it be tested? The depth of test is also an important criterion and is closely aligned to the maintenance concept. The depth of test specifies the agreed level to which the failed item or sub-assembly is to be identified. For example, a system test may identify the item to be replaced, but may also identify the sub-assembly that needs to be replaced with little or no impact on the cost. This may reduce the costs associated with the test or test equipment required.

Diagnostic testing typically consists of functional testing with the purpose of verifying that a function can still be performed. BIT tests form part of all the functional tests conducted on a product.

Stated Conditions

Diagnostic testing activities are closely interconnected with the system's intended operating and maintenance environments. Therefore, these environments are important factors to be specified when diagnostic testing requirements are established.

A system can be used in different environments, depending on the User's requirements. As far as testability is concerned, a distinction is made between the system environment (operating conditions) and the test environment corresponding to the required maintenance conditions. In the latter, the product is typically operated in a system/product simulation. Here, all the parameters set for testing the hardware unit should correspond to those in the system.

Annex E – Defining Failure

E.1 Introduction

Clear and precise failure definitions (including definitions for different classes of failure) and environmental and operating conditions are a fundamental part of the R&M requirements. The R&M requirements have no meaning without explicit definitions of failure and intended conditions.

Failure definitions must be established early and included in R&M requirement specifications. Discussions between the R&M stakeholders and the requirements team should begin as early as the concept phase. Endorsed failure definitions that are clear, unambiguous and reflect what the User requires, should be a deliberate outcome from the R&M Panel and requirements team.

E.2 IEC Definition

IEC 60050-191 defines failure as follows:

> **Failure** (of an item) is the **loss of ability** to **perform as required**.

E.3 Failure Definition Guidance

Failure definitions have to be clear, concentrate on objective criteria and be based on effects rather than on causes if the true impact of failure is to be understood.

A major problem lies in ensuring that failure criteria are unambiguous and reflect what the User requires. It is strongly recommended that the guidance in Def Stan 00-44 R&M Data Collection and Classification is followed, and expert advice is obtained.

It is much cheaper to remove potential causes of failures during design and development than to live with recurring failures in service, or to pay for the introduction of fixes into equipment already delivered. Effective failure (or more accurately incident) management begins with a closed-loop Data, Reporting, Analysis and Corrective Action System (DRACAS).

In order to correctly specify failure criteria exclusively for each programme the available terminology (from IEC 60050-191 as a first source) must be fully understood. The following examples give guidance:

Failure / Loss of Ability

A failure of an item is an event (i.e. something has happened), as distinct from a fault of an item which is a state (i.e. the item is in a certain condition). When the loss of ability is caused by the inability to perform a pre-defined function, the failure can occur when a particular set of circumstances is encountered.

Primary failure [IEC 60050-191] is failure not caused either directly or indirectly by a failure or fault of another item. Secondary failure [IEC 60050-191] is caused by a failure or a fault state of another item.

The failure effect [IEC 60050-191] is the consequence of a failure, in terms of operation, function or status of the item and higher system levels.

A failure would therefore result from an incident preventing the equipment from performing one or more of its functions. A fault is often the result of a failure of the item itself, but may exist without prior failure.

It is critical that the nature of failures is defined and agreed when setting reliability requirements. This may be achieved through a classification scheme which typically includes failure effects and causes addressing mission, basic and/or peacetime failures. Failures causes are either systematic or random in nature. These are expanded below.

Failure Effects

A mission failure results when an item/system fails to perform its required mission essential functions for the duration or specified period during a mission profile. Critical failure normally relates to failure that could result in injury to persons, or that prevents an item from performing an essential mission.

A basic failure results when an item/system fails in its ability to perform its required functions for the duration of its life profile. Basic failures relate to all failures requiring maintenance actions that do not directly affect the mission (all corrective maintenance actions are counted, from changing a main assembly to unscheduled minor adjustments).

A peacetime failure typically results when an item/system fails to perform those functions specified as mission/task essential or those that are required to comply with safety / environmental legislation.

Failure Causes

Systematic and random failure conditions are quite different and the distinction is important when specifying failure criteria and understanding failure classification.

Systematic failure [IEC 60050-191] has its cause inherent in the specification, design, manufacture, operation, or maintenance and is precipitated by the particular conditions associated with an items handling, storage, use or maintenance. A systematic as opposed to a random failure, can be reproduced by deliberately inducing the same conditions in order to verify the cause. Consequently, a change to the specification / design / manufacturing process / operation or maintenance procedures is normally required to eliminate the failure cause.

The term random failure [IEC 60050-191] is applied when the time of occurrence is predictable only in a probabilistic sense (i.e. statistical in nature and having an element of chance) rather than a deterministic way (which can be measured/replicated repeatably).

Incident Reporting, Analysis and Correction

Incidents are not confined to those 'known' faults and failures which affect the ability of equipment to perform or be operated satisfactorily (this would be to pre-judge an incident as a fault/failure). Other events, such as observed deterioration, may also be reported as incidents as well as actions, such as modifications, scheduled maintenance and the repair/replacement of faulty items. Collecting such 'data' in the DRACAS provides important information on all occurrences and observations which arise during a reporting period and facilitates sentencing, classification, failure and trend analysis.

A function of DRACAS, recording incidents and submitting them to an incident sentencing committee typically results in incidents being sentenced/classified against effects and causes as discussed above.

Data classification is a general term used to describe the process by which incidents are examined and classified for the purpose of R&M assessment. It is performed to quantify R&M from the recorded data in accordance with predefined criteria such as mission or basic reliability.

The classification of incident data for the purpose of R&M assessment requires incidents to be examined and grouped into categories (e.g. cause, significance, maintenance requirement, etc) applicable to the R&M parameters being assessed. This is achieved by first sentencing the raw incident data according to formal rules and then sorting the sentenced incident data into the required classifications.

Perform / Perform as Required

A system is generally defined with a view of performing a definite role with a function(s) clearly defined. A fault [IEC 60050-191] is characterised by an inability to perform as required. However, inability to perform due to preventative maintenance, other planned actions, or lack of external resources does not constitute a fault.

A software fault [IEC 60050-191] or bug is a condition of a software item that may prevent it from performing as required, whereas a software failure [IEC 60050-191] is a manifestation of a software fault.

A latent fault [IEC 60050-191] is an existing fault that has not been revealed or made observable but may eventually be discovered by diagnostic methods, or revealed by a failure.

A faulty item can cause an error, e.g. a computing error made by faulty computer equipment. An error [IEC 60050-191] is a discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition. Error recovery [IEC 60050-191] (designed is to avoid a failure of the whole system, following a failure of one of the subsystems or components) will automatically detect, contain and correct an internal erroneous state.

Items that become degraded [IEC 60050-191] are in a state in which one or more performance characteristics do not meet requirements. Limits of acceptable degradation may be pre-determined beyond which the item is declared as being down (not available).

Similarly, a defect [IEC 60050-191] results from the non-fulfilment of a requirement which is related to an intended, specified use.

Importantly however, there is a distinction between the concept of defect and non-conformity as a defect has legal connotations associated with product liability. Consequently, the term defect should be used with extreme caution.

Specified Limits

The environment in which a system is expected to function will impose limitations on its reliability, affecting its tendency to fail. A bolt installed inside a building, experiencing no vibration or extremes of environment, will likely be more reliable, and less prone to failure, than one installed on the exterior of a vehicle which will suffer vibration and environmental conditions. If installed on the exterior of a ship, where the vibration and environment could be extreme, the bolt is more prone to failure.

An early failure period [IEC 60050-191] is the time interval in early life of a system (often called the infant mortality period) during which the failure probability for a repairable item, or the failure rate for a non-repairable item, is significantly higher than that of the subsequent (typically the useful life) period.

Burn-In is a typical reliability conditioning procedure which is a method of ageing an item by operating it under specified environmental and test conditions in accordance with an established procedure, in order to eliminate early failures and age or stabilise the item prior to final test and shipment. Specifying burn-in can address many of the consequences of early life failure.

The constant failure intensity period [IEC 60050-191] in the life (normally useful life period) of a repairable item is when the failure probability is approximately constant. The same is true for non-repairables and the constant failure rate period [IEC 60050-191].

Failure criteria [IEC 60050-191] are predefined conditions or limits to be accepted as conclusive evidence of failure. In a post-failure scenario, the conclusive evidence may be regarded (and recorded) as proof. The evidence is useful to measure against contractual pass/fail criteria.

Defence Standards are Published by and Obtainable from:

Defence Procurement Agency

An Executive Agency of The Ministry of Defence

UK Defence Standardization

Kentigern House

65 Brown Street

GLASGOW G2 8EX

DStan Helpdesk

Tel 0141 224 2531/2

Fax 0141 224 2503

Internet e-mail enquiries@dstan.mod.uk

File Reference

The DStan file reference relating to work on this standard is D Stan 21/49.

Contract Requirements

When Defence Standards are incorporated into contracts users are responsible for their correct application and for complying with contractual and statutory requirements. Compliance with a Defence Standard does not in itself confer immunity from legal obligations.

Revision of Defence Standards

Defence Standards are revised as necessary by an up issue or amendment. It is important that users of Defence Standards should ascertain that they are in possession of the latest issue or amendment. Information on all Defence Standards can be found on the DStan Website www.dstan.mod.uk, updated weekly and supplemented regularly by Standards in Defence News (SID News). Any person who, when making use of a Defence Standard encounters an inaccuracy or ambiguity is requested to notify UK Defence Standardization (DStan) without delay in order that the matter may be investigated and appropriate action taken.