

Draft for Public Comment

Form 36



DPC: 12 / 30259311 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: + 44 (0)20 8996 9000

Fax: + 44 (0)20 8996 7400

www.bsigroup.com

Date: 23 January 2012
Origin: International

Latest date for receipt of comments: 20 March 2012

Project No. 2012/00260

Responsible committee: DS/1 Dependability

Interested committees:

Title: Draft BS EN 60300-1 ED.3 Dependability management

Part 1: Guidance for management and application

Supersession information: If this document is published as a standard, the UK implementation of it will supersede BSEN60300-1 : 2003 . If you are aware of a current national standard which may be affected, please notify the secretary (contact details below).

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 20 March 2012**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Customer Services, Tel: + 44(0) 20 8996 9001 or e-mail cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from the responsible committee secretary.

Cross-references

The British Standards which implement International or European publications referred to in this draft may be found via the British Standards Online Service on the BSI web site <http://www.bsigroup.com>.

Responsible Committee Secretary: **Mr A Ashrafi (BSI)**Direct tel: **020 8996 7205**E-mail: asghar.ashrafi@bsigroup.com

Introduction

This draft standard is based on international discussions in which the UK has taken an active part. Your comments on this draft are welcome and will assist in the preparation of the consequent standard. There is a high probability that this text could be adopted by CENELEC as a reference document for harmonization or as a European Standard. Recipients of this draft are requested to comment on the text bearing in mind this possibility.

UK Vote

Please indicate whether you consider the UK should submit a negative (with reasons) or positive vote on this draft.

Submission of Comments

- The guidance given below is intended to ensure that all comments receive efficient and appropriate attention by the responsible BSI committee. **Annotated drafts are not acceptable and will be rejected.**
- All comments must be submitted, preferably electronically, to the Responsible Committee Secretary at the address given on the front cover. Comments should be compatible with version 6.0 or version 97 of Microsoft Word for Windows, if possible; otherwise comments in ASCII text format are acceptable. **Any comments not submitted electronically should still adhere to these format requirements.**
- All comments submitted should be presented as given in the example below. Further information on submitting comments and how to obtain a blank electronic version of a comment form are available from the BSI website at: <http://www.bsigroup.com/en/Standards-and-Publications/Current-work/DPCs/>

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	-------------------------------

1	2	(3)	4	5	(6)	(7)
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/ Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



56/1459/CD

COMMITTEE DRAFT (CD)

IEC/TC or SC: TC 56	Project number IEC 60300-1 Ed. 3.0	
Title of TC/SC: Dependability	Date of circulation 2012-01-20	Closing date for comments 2012-04-20
Also of interest to the following committees	Supersedes document 56/1439/CD and 56/1448A/CC	
Proposed horizontal standard <input type="checkbox"/> Other TC/SCs are requested to indicate their interest, if any, in this CD to the TC/SC secretary		
Functions concerned: <input type="checkbox"/> Safety <input type="checkbox"/> EMC <input type="checkbox"/> Environment <input type="checkbox"/> Quality assurance		
Secretary: M Maghar – UK Email: mick.maghar@bsigroup.com	THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES. RECIPIENTS OF THIS DOCUMENT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.	

Title:

IEC 60300-1 Ed. 3.0: Dependability management - Part 1: Guidance for management and application

(Titre) :

Introductory note

Copyright © 2012 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

1	Scope	8
2	Normative references	8
3	Terms, definitions and abbreviations	8
3.1	Terms and definitions	8
3.2	Abbreviations	11
4	Understanding dependability	12
5	Managing dependability	13
5.1	Management of dependability	13
5.2	Dependability management systems	14
5.3	Elements of a dependability programme	15
6	Application of dependability management	16
6.1	Implementation of dependability management	16
6.2	Tailoring of a dependability programme	17
6.3	Assessment and measurement	19
6.4	Assurance of dependability performance	20
6.5	Dependability management review	21
Annex A	(informative) Structure of dependability standards	23
A.1	Structure	23
A.2	Core standards	23
A.3	Process standards	23
A.4	Support standards	24
A.5	Associated standards	24
Annex B	(Informative) Performance element of a dependability management system	25
B.1	Performance requirements from an application perspective	25
B.2	Examples of performance requirements that include dependability	26
B.2.1	Requirements determined by both provider and user	26
B.2.2	Requirements determined by provider only	27
Annex C	(Informative) Process element of a dependability management system	30
C.1	Dependability processes within the life cycle	30
C.2	Dependability life cycle processes	33
Annex D	(informative) Organisational element of a dependability management system	37
D.1	Organisational structures	37
D.2	Organisation of dependability activities	37
Annex E	(informative) Checklist for management review of dependability	39
E.1	Introduction	39
E.2	Concept	39
E.2.1	Requirements definition	39
E.2.2	Requirements analysis	39
E.2.3	High-level architectural design	39
E.3	Development	40
E.3.1	Item design	40
E.3.2	Full-scale system development	40
E.4	Realization	40
E.4.1	Item realization	40
E.4.2	Item implementation	40

E.5 Utilization	41
E.6 Enhancement	41
E.7 Retirement	41
Figure 1 – Relationship of dependability to the needs and requirements of a product, system, process or service.....	12
Figure 2 – Implementation of dependability management	16
Figure A.1 – Framework for dependability standards.....	23
Figure B.1 - Example showing the relationship between functional and dependability requirements for a pipeline motor-driven pump	27
Figure B.2 - Example showing the relationship between functional and dependability requirements for a family car	29
Figure C.1 – Dependability processes and the life cycle	32
Table C.1 – Processes during the concept stage	33
Table C.2 – Processes during development stage.....	34
Table C.3 – Processes during the realization stage.....	35
Table C.4 – Processes during the utilization stage	35
Table C.5 – Processes during the enhancement stage.....	36
Table C.6 – Processes during the retirement stage	36

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 1: Guidance for management and application

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-1 has been prepared by IEC technical committee 56:

The text of this standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The National Committees are requested to note that for this publication the stability date is

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

INTRODUCTION

This standard describes the processes involved in managing dependability within an organisation and establishes a framework for managing dependability activities for the purpose of achieving dependability performance.

Dependability is the ability of an item to perform as and when required. “Item” is used throughout this standard as a general term to describe the subject being considered including products, systems, processes, and services involving hardware, software and human aspects.

Dependability is a term used to describe the time-dependent characteristics associated with the performance of an item. Dependability includes characteristics such as availability, reliability, maintainability and supportability under given conditions of use and maintenance support requirements.

Dependability advocates user trust and customer confidence from a value perspective in doing business. It affects the bottom line of an organisation in product development or service provision demanding attention to ascertain dependability performance value. Dependability has become a critical decision factor in project management where major resource commitments are required to move the project forward. Dependability value achievement is focused on effective planning and implementation of dependability activities from a life cycle perspective.

Dependability has a strong impact on the user’s perception of the value of an item developed or provided by an organisation. Poor dependability will affect the perception of the organisation’s capability and reputation to deliver its objectives. In this respect, dependability describes the extent to which something can be trusted to behave as expected. Dependability activities can be applied to in-house designs and outsourced products. Dependability needs to be taken into account when making management decisions and meeting dependability objectives is critical for successful project achievement.

Dependability is improved by systematically reducing the frequency of outages, product failures, service downtimes, and other undesired events and minimizing their effects. This is achieved by actions such as improving design, elimination of root causes of failure, simplification of complex processes, mitigation of anomalies, promoting fault tolerance in design and fitness for use, advocating fault avoidance and error prevention, management of maintenance activities and commitments to guarantee trust and integrity to ensure user confidence throughout the life cycle. Early consideration of dependability in the life cycle is crucial since rectifying a design that causes poor dependability will often be more difficult at a later time.

Dependability management is a systematic approach for addressing dependability and related issues from an organisational and business perspective. Dependability is often technology driven which requires the integration of new innovation with legacy products. Dependability applications in the life cycle process can be influenced by market dynamics, global economics and resource distributions, changing customer needs, and a competitive environment. Strategies need to adapt to anticipated changes to sustain viability in business operations. Dependability management focuses on the needs of stakeholders in optimizing dependability to enhance organisational objectives and return-on-investments.

This document is written specifically for application to technological products, systems, processes and services which are referred to in this standard by the general term “item”. However, much of the guidance provided is generic and can be adapted for application in various non-technological applications. In addition, the potential detrimental side effects on safety, environmental and other factors should be identified, analyzed and managed when optimizing dependability.

The intended audience for this standard ranges from users, owners and customers to organisations involved in and responsible for ensuring dependability requirements are being

met. Organisations include all types and sizes of corporations, public and private institutions such as in governments, business enterprises, and non-profit associations.

DEPENDABILITY MANAGEMENT – Part 1: Guidance for management and application

1 Scope

This part of IEC 60300 establishes a framework for dependability management. It provides guidance on dependability management of products, systems, processes or services involving hardware, software and human aspects or any combinations of these items. It describes the planning and implementation of dependability activities from a life cycle perspective taking into account functional and application requirements such as those relating to technology, mission critical, safety and the environment to optimize dependability performance.

This International Standard is intended for management and their technical personnel to assist them to achieve dependability objectives.

This standard is not intended for the purpose of certification.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-191, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

3 Terms, definitions and abbreviations

For the purposes of this document, the definitions given in IEC 60050-191 and the following apply.

3.1 Terms and definitions

3.1.1

availability (characteristic of an item)

ability to be in a state to perform as required

NOTE 1 Availability depends upon the combined characteristics of the reliability, recoverability, and maintainability of the item, and in some cases, on the maintenance support performance.

NOTE 2 Availability may be quantified using appropriate performance measures. See Section 191-48, Availability and related measures.

3.1.2

capability (of an item)

ability to meet a service demand of given quantitative characteristics under given internal conditions

NOTE Internal conditions may be any combination of sub-items with or without faults.

3.1.3

dependability (of an item)

ability to perform as and when required

NOTE 1 In addition to the dependability characteristics defined in this document, some applications include others, such as integrity, safety and security.

NOTE 2 The dependability characteristics considered for a particular item will depend upon its application.

NOTE 3 Dependability is also used as a collective term for the time-related quality characteristics of a product or service.

NOTE 4 The definition of dependability has been revised from that given in Ed.1, following consultations throughout the TC56 member nations. Whilst some applications use availability as a performance measure for dependability, the influencing factors vary with application, thus precluding generic standardization.

Recommended revised notes

NOTE 1 Dependability can be defined by characteristics such as availability, reliability, maintainability and supportability.

NOTE 2 The dependability characteristics considered for a particular item will depend upon its application.

NOTE 3 Dependability is used as a collective term for the time-related characteristics of a product, system, process or service.

3.1.4

dependability management

coordinated activities to direct and control an organisation with regard to dependability

NOTE Dependability management is part of an organisation's overall management.

3.1.4

dependability management system

set of interrelated or interacting elements of an organization to establish dependability-related policies, objectives and the processes to achieve those dependability objectives

NOTE 1 Dependability management system of an organisation is part of its overall management system and is not usually a separate management system.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning, procedures and processes.

NOTE 3 The organisational structure, responsibilities, procedures, processes and resources used for managing dependability are often referred to as the dependability programme.

3.1.6

dependability plan

minimum set of time scheduled activities required to achieve dependability targets of an **item** throughout its **life cycle**

3.1.7

dependability programme

organisational structure, responsibilities, procedures, processes and resources used for managing dependability

3.1.8**item**

subject being considered

NOTE 1 The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

NOTE 2 The item may consist of hardware, software, people or any combination thereof.

NOTE 3 An umbrella term which can be applied recursively throughout a system. The item is invariably comprised of elements that may each be individually considered. See sub-item (191-41-02) and indenture level (191-41-05).

NOTE 4 Ed.1 identified the term "entity" as a synonym, which is not true for all applications.

NOTE 5 The definition for item in Ed.1 is a description rather than a definition. This new definition provides meaningful substitution throughout this document. The words of the former definition form new note 1.

3.1.9**life cycle**

series of identifiable stages through which an item goes, from its conception to disposal

NOTE The stages identified will vary with application.

EXAMPLE A typical system lifecycle consists of: concept and definition; design and development; construction and commissioning; operation and maintenance; mid-life upgrading, or life extension; and decommissioning and disposal.

Recommended revised note

EXAMPLE A generic lifecycle can consist of: concept; development; realization; utilization; enhancement; and retirement.

3.1.10**maintainability** (characteristic of an **item**)

ability to be retained in, or restored to a state in which it can perform as required, under given conditions of use and maintenance

NOTE 1 Given conditions would include aspects that affect maintainability, such as: location for maintenance, accessibility, procedures and resources.

NOTE 2 Maintainability can be viewed as the time to diagnose and effect repair assuming resources are available, and may be quantified using appropriate performance measures. See Section 191-47, Maintainability and maintenance support: activities and measures.

3.1.11**maintenance support**

resources to maintain an item under a given maintenance concept

NOTE Resources include human resources and specialist skillsets, support equipment, materials and spare parts, maintenance facilities, documentation, information and maintenance information systems.

3.1.12**organisation**

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

NOTE 1 The concept of organisation includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

NOTE 2 For organisations with more than one operating unit, a single unit may be defined as an organisation.

3.1.13**product**

result of a process

[ISO 9000:2005, 3.4.2]

3.1.14**reliability** (characteristic of an **item**)

ability to perform as required, without failure, for a given time interval, under given conditions

NOTE 1 Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

NOTE 2 Reliability may be quantified using appropriate performance measures, see Section 191-45, Reliability related concepts: measures.

3.1.15**requirement**

need or expectation that is stated, generally implied or obligatory

[ISO 9000:2005, 3.1.2]

3.1.16**service**

set of functions offered to a user

3.1.17**stakeholder**

person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity

3.1.18**supportability** (characteristic of an **item**)

ability to provide the required reliability and availability with a defined operational profile and specified logistic and maintenance resources

NOTE 1 Supportability is dependent on the maintainability of the item, combined with factors external to the item that affect the provision of maintenance and logistic support.

NOTE 2 Supportability is principally a function and outcome of the design and in-practice resourcing of the item's support concept and systems (including maintenance and logistic support).

NOTE 3 Supportability can be viewed as the time to provide and use the technical data, skill sets, tools and spare parts so that maintenance can be effected, and may be quantified using appropriate performance measures.

3.1.19**system**

defined set of items that behave collectively to satisfy a requirement

NOTE 1 A system is considered to have a defined boundary.

NOTE 2 External resources (from outside the system boundary) may be required for the system to operate.

NOTE 3 A system structure may be hierarchical, e.g. system, subsystem, component, etc.

NOTE 4 Conditions of use and maintenance should be expressed or implied within the requirement.

3.1.20**tailoring (process)**

process to adapt, adjust or alter an organisation's set of established processes and activities to fulfil, satisfy or meet requirements as they apply to dependability

3.2 Abbreviations

COTS Commercial Off-The-Shelf

4 Understanding dependability

Dependability is the ability of an item to perform as and when required. Dependability creates value in that the item retains its performance characteristics, operates successfully, and satisfies customer needs and expectations. An item represents an individual part, component, device, functional unit, equipment, subsystem, or system. It can consist of hardware, software, people or any combination thereof. For simplicity, the term item is used hereafter instead of product, system, process and service. An item goes through the life cycle stages from initial identification of its need to retirement or disposal of the item.

Dependability is often used as a collective term to describe the time-related characteristics of an item where time refers not only to elapsed time, but also time-related aspects such as operating time, number of cycles, number of starts or demands. The characteristics of dependability, depending on specific applications, include availability, reliability, maintainability and supportability, as well as related characteristics such as recoverability and durability.

Figure 1 illustrates the relationship of dependability to the needs of stakeholders and the requirements of an item. Depending on context, stakeholders can include users, owners, customers, government agencies, businesses and organisations responsible for ensuring dependability requirements are met.

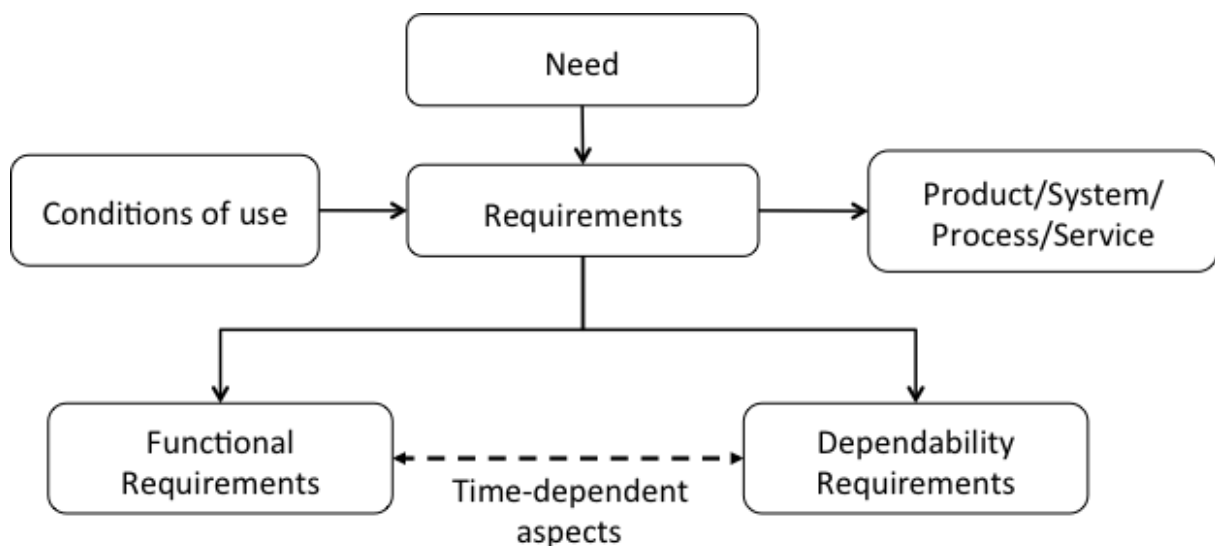


Figure 1 – Relationship of dependability to the needs and requirements of a product, system, process or service

Requirements are determined from the needs of stakeholders, the conditions of use, , and other constraints such as prescribed maintenance. They include functional requirements, which define what the item is required to do, and dependability requirements, which define the time dependent ability to achieve dependability performance in these functional requirements. Examples of functional requirements are capacity, performance, safety and environmental sustainability. Examples of dependability requirements are reliability, availability, maintainability and supportability.

Functional requirements and dependability requirements are inter-related. A dependability requirement can only exist if there is a functional requirement that has to be satisfied. There can be competing objectives between desirable functional requirements such as safety or production capacity and dependability and therefore trade-offs may be needed. There can also be constraints related to cost, availability of item components or resources, or fixed timelines that could cause a compromise between functionality and dependability.

The perception of the ability to perform as and when required can vary for different stakeholders. Users, providers, operators, maintainers and others who interact with an item can have overlapping dependability requirements but with different application objectives and usage expectations. This can result in differing perceptions of dependability which may need to be considered in defining requirements.

5 Managing dependability

5.1 Management of dependability

The purpose of dependability management systems is to direct and control an organisation with regard to dependability, coordinating with other disciplines to achieve an integrated effort that results in global optimization of organisational effort.

The management of dependability requires control and vision, accountability and commitment, knowledge and prudent judgment to address dependability issues and the consequences of the applied measures. This involves planning and control, resource allocation, coordination, execution and review of dependability.

To meet dependability expectations, managers are responsible for

- leadership through management commitment, policy direction and establishment of roles, responsibilities and authority,
- planning to consider risks and opportunities and determining objectives and plans to achieve them,
- support by providing resources, competence, awareness, communication and documentation,
- operational planning and control,
- performance evaluation through monitoring, measuring analysis and evaluation, audit and assurance and management review, and
- improvement.

Management of dependability results in benefits such as

- meeting dependability requirements and objectives,
- achieving expected service levels,
- improving functionality,
- maintaining production or manufacturing capacity through increased availability,
- improving safety when potential detrimental side effects are identified and dealt with appropriately,
- reducing environmental impact when detrimental side effects are identified and dealt with appropriately,
- reducing life cycle costs, and
- improving quality.

Dependability management needs to be aligned with organisational objectives and those of stakeholders comprising both technical and business perspectives. Dependability management activities are normally integrated within existing management systems to achieve a clearly defined common objective. However, technical expertise and resources are needed to ensure dependability aspects are properly addressed on a timely basis.

How dependability is managed in conjunction with dependability-related activities needs to be tailored to the particular situation and in conjunction with other related activities, such as safety tasks.

Dependability needs to be considered and addressed during the entire life cycle of an item. Early consideration and implementation of relevant dependability activities will better ensure that dependability requirements are achieved. These can be complicated when multiple organisations are involved, dependability management is introduced or changed mid-life cycle, or the item's contribution is influenced by interconnected and external systems.

One of the challenges with managing dependability over the life cycle is that often more than one organisation is involved. Over the life cycle, certain responsibilities may need to be passed from one organisation to another. Since organisational styles and procedures vary, the management of dependability needs to adapt to different situations. Where functions such as maintenance and logistic support are outsourced, the responsibility for dependability aspects of outsourcing should be specified, monitored and controlled.

Items are often integrated to operate with legacy items that are in different stages of the life cycle with, older generation technologies and methods of design. Dependability management is involved in the assurance of interoperability and dependability of the integrated items. This necessitates addressing specific legacy-related dependability issues to adapt them by available processes through interface specifications to ensure dependable performance.

A further complexity arises when services are provided by interconnected systems under autonomous management and responsibilities and at different stages of the life cycle. Each system may have an incomplete understanding of the whole complex that may change unexpectedly. These are sometimes referred to as open systems. Sustainability of services becomes the key to dependability of open systems. For that reason, it is crucial for stakeholders to understand and agree on the boundaries of their responsibilities. Planning for service continuity needs to take into account major failures and changes outside respective boundaries as well as inside, to mitigate their effects to the whole system, restore services, and adapt to changes. The perception of dependability is obtained through accountable implementation of agreements between stakeholders.

The use of a dependability case provides a means of recording and presenting an argument that dependability objectives will be or have been achieved (see clause 6.4).

5.2 Dependability management systems

Dependability management systems do not require a complex organisational infrastructure and reporting hierarchy. Dependability activities can be managed by a separate organisational unit with close coordination, be fully integrated into other relevant areas, or be a mixture of the two approaches.

The alignment of organisational structure, responsibilities, procedures, processes, resources and information is critical to efficient and effective direction and control of dependability.

Key considerations that form the basis for establishing a viable dependability management system include:

- *governance*: the structure, process, and procedure to control operations and changes to meet performance objectives including dependability;
- *planning and resource allocation*: coordination and control of functional and technical activities with appropriate resource allocations, including outsourcing, to meet planned dependability objectives and delivery targets;
- *policy alignment*: the dependability activities necessary to support the policies of the organisation such as continuous dependability improvement, quality of service and safety;
- *technology*: different technology applications requiring different methods to achieve dependability objectives. Hardware, software, and human aspects of dependability will require coordination by management;

- *application environment*: different application environments requiring management consideration of design and implementation strategies on technology selection, item deployment, and regulatory compliance;
- *communications and information management*: implementing effective communications with customers and suppliers and the organisation's staff members at all levels to establish market or other needs and user expectations;
- *assurance*: ensuring adherence to standards and procedures for management accountability by means of regular reviews, assessments, verification and validation, preventive and corrective actions for continuous improvement, and dependability knowledge-base enhancement;
- *risk management*: a proactive approach that seeks to recognise and understand the effects of uncertainty on the objectives of the organisation and stakeholders so that opportunities are realised and undesired effects prevented;
- *stakeholder management*: identification and engagement of stakeholders on dependability issues, communication of dependability programme status, conflicts resolution and trade-offs, and securing and maintaining agreements and accountability.

A means to manage and control dependability data and information should be established as a part of the organisation's management information systems. This is to provide management insights on historical data and dependability-related performance records, enabling measurement of dependability status and improvements.

Annex A presents the framework structure for dependability standards to support dependability management and guide the application of methods and tools. Information on specific and current dependability standards is provided on the IEC/TC56 Website [1] to facilitate dependability applications.

5.3 Elements of a dependability programme

A dependability programme helps management ensure that dependability requirements are met in conjunction with functional requirements. The basic elements of a dependability programme are a dependability plan, defined activities, required resources, dependability analysis techniques and assurance that dependability objectives are being met.

A dependability programme should address performance of the following:

- *coordination* of different organisational functions requiring integration of dependability activities, usually by a project lead with assigned dependability responsibility for the coordination of management and technical effort;
- *resource management* requiring planning, acquisition of capital equipment, staff training and deployment, outsourcing and sub-contracting of dependability technical work;
- *development management* requiring dependability management authority for assignment of specific expertise to assist design, development, realization, implementation and review of dependability needs;
- *process management* requiring planning, development, evaluation, and application of management and technical processes involved in the execution of dependability disciplines;
- *configuration management* requiring dependability management inputs and confirmation to effect design changes of configured items;
- *operation and maintenance management* requiring dependability technical involvement to resolve dependability related problems and assess impact consequences;
- *performance management* requiring assessment of dependability-related performance trends during utilisation of items and for the provision of support services;
- *support management* requiring dependability inputs on planning and implementation on item upgrades, modification and service enhancement;

- *information management* requiring dependability contributions to establish and update dependability-related performance database for use by cognizant personnel;
- *knowledge management* requiring dependability involvement for dependability knowledge capture, patent applications, and dissemination of relevant dependability data and knowledge to cognizant personnel;
- *assurance management* requiring dependability management involved in planning, review, audit, verification and validation of on-going project activities;
- *risk management* requiring a proactive approach that seeks to recognise and understand the effects of uncertainty on an item's dependability and functional objectives.

Dependability related issues and technical concerns should be brought to management attention at review meetings for resolution, decisions and priority setting of task assignments.

6 Application of dependability management

6.1 Implementation of dependability management

Figure 2 shows the dependability management system as a part of a generic management system. The dependability management system results in a dependability programme which feeds into organisational plans and activities.

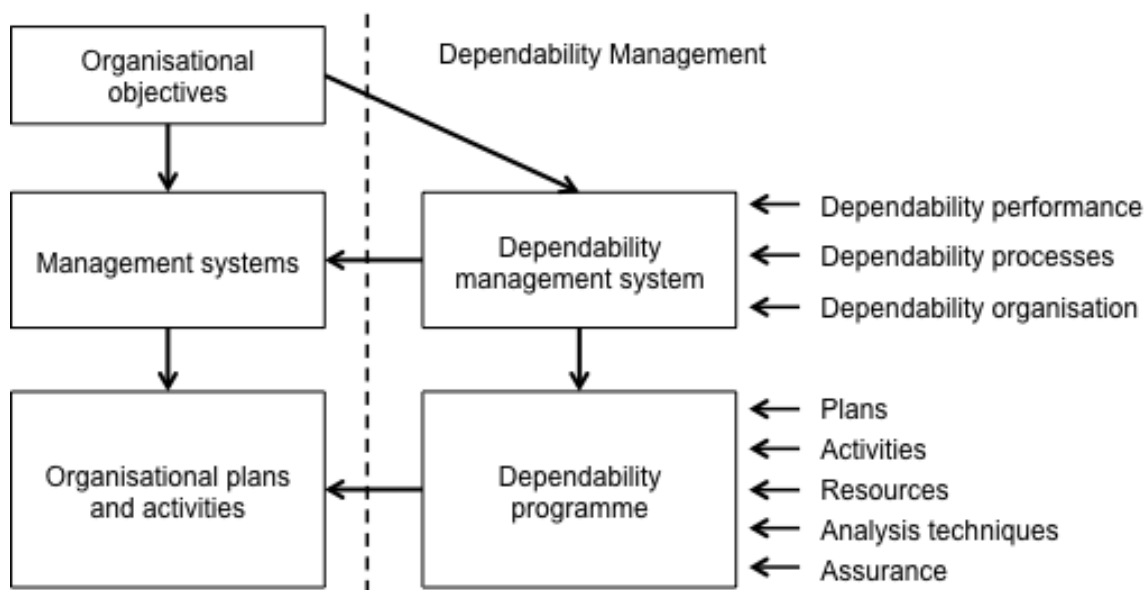


Figure 2 – Implementation of dependability management

Implementation of a dependability management system consists of three elements:

- defining dependability performance against performance requirements;
- implementing dependability processes;
- establishing organisational arrangements.

Performance requirements are defined to satisfy the needs of stakeholders and can be divided into two interrelated groups, functional requirements and dependability requirements (see Figure 1). Dependability is a time-dependent quality characteristic that describes how the functional requirements are achievable. It consists of characteristics such as availability, reliability, maintainability and supportability. Reliability is an intrinsic characteristic of an item while maintainability is a characteristic of the design of the item and its installation. Supportability is a characteristic of the item's support concept, systems, and in-practice resourcing. The combination of these characteristics determines the resultant availability.

Annex B describes the establishment of dependability requirements and relevant dependability characteristics identified to achieve the performance requirements.

Since perceptions of dependability may vary depending on the stakeholder it is important to ensure there is good communication between all relevant stakeholders when defining performance requirements and how they will be assessed.

Dependability performance and functional performance should be assessed against the performance requirements to check that requirements have been achieved and to provide information for improvement of the process. Dependability assessment and measurement are discussed in clause 6.3.

The dependability process is implemented through a series of activities that lead to coordinated efforts for cost-effective management of dependability activities. The process may consist of these steps:

- defining dependability objectives in consultation with stakeholders;
- describing the project and organisational context to enable tailoring;
- assessing risks to dependability objectives in the relevant context;
- planning a tailored strategy and activities for achieving objectives and treating risks;
- implementing the dependability programme and plan;
- guiding technical activities and dependability analyses
- assessing and measuring dependability outcomes;
- reviewing dependability outcomes and processes.

Annex C presents a process view for the alignment of dependability management activities with the life cycle of an item.

Dependability management occurs throughout the life cycle. The planned dependability activities are normally incorporated as part of engineering processes at every life cycle stage even when the different stages of the life cycle overlap. The transitions of life cycle stages often entail different technical resources, diverse enabling systems and support criteria. Dependability management can utilize technology acquisition and business collaboration such as supply-chain management, outsourcing and partnerships to achieve project objectives.

Establishing organisational arrangements focuses on the management infrastructure needed to facilitate effective implementation of dependability policy within an organisation. Dependability objectives must be integrated by management into the framework of an organisation's infrastructure in order to enable decision-making and influence technical direction. Dependability engineering as a technical discipline should be closely integrated into on-going engineering projects for design and process improvements. Annex D describes the incorporation of dependability activities in the organisational operations, strategies and processes to achieve long-term goals and on-going project objectives.

The management activities required for each stage of the life cycle can be different. Dependability activities should be organized and managed as part of engineering or other programs or projects for maximum effectiveness. A project has a definite duration with specific start and end dates and a project plan. A program is usually longer term and on-going, and can consist of several related projects to achieve common organisational objectives such as technology platform studies, dependability process improvement and supportability systems optimization.

6.2 Tailoring of a dependability programme

Establishing a dependability programme entails the elements shown in Figure 2: plans, activities, resources, analysis techniques and assurance. Management accountable for the

resulting dependability of an item should tailor these elements to fulfill the dependability objectives for that specific situation or project. Tailoring applies to any stage of the life cycle but the most important tailoring occurs during the initial design-related parts of the life cycle. It may not be necessary to tailor activities in all cases, for example, for manufacturers who develop and produce similar products.

The general tailoring of the dependability programme consists of the following:

- identification of the organisational policy and infrastructure;
- analysis of requirements and contract stipulations, characteristics and objectives which can be difficult to realize and to deliver;
- capability and resources needed and actually available for implementation;
- determination of the specific life cycle stages or phases that are applicable;
- identification of item related characteristics such as its features and functions, past history of similar items, their intended end use and anticipated application environments;
- selection of applicable dependability actions relevant to the specific life cycle stages or phases identified;
- prioritisation and allocation of resources;
- consideration of regulatory requirements or standards;
- documentation of the rationale in formalizing the tailoring decisions as part of the organisational or project plan.

The outcome of tailoring activities, once compiled and documented, form the basis of a dependability plan of activities and resources for that particular project. As directed by management, the depth of detail of this planning activity should be to a level that is easily measurable for management tracking and for costing purposes. In concert with other functional plans, this dependability list of activities contributes to the overall programme management plan. Tailored dependability activities should, along with other functional areas such as safety, scheduling, integration, production, operations and maintenance, build the backbone of the overall project plan. Integration into this overall project plan can require further tailoring to accommodate project time and cost limitations. This will inevitably incur a trade-off of predicted product dependability and risks against project timing and cost.

If the magnitude of the programme dictates the need for each functional area to have its own plan, these dependability activities can be documented in their own separate plans.

Tailoring criteria and guidelines describe

- how the organisation's dependability standard processes are used to create the defined project processes,
- which mandatory and legal requirements must be satisfied,
- which options can be exercised as well as the criteria for down-selecting these options, and
- which dependability procedures must be performed in the process tailoring.

Tailoring of dependability management activities needs to take into account the nature of the organisation and the dependability tasks that need to be managed. The organisation could vary from a technical consultancy to a multi-national conglomerate requiring appropriate dependability management of diverse disciplines, organisation and specialization. Management approaches often seek technology transfer, knowledge infusion, or expert consultancy to deal with critical short-term technical gaps. There is also a broad range of supporting disciplines and enabling systems to facilitate achievement of dependability management objectives such as maintenance and logistic support management, customer care services, failure reporting, analysis and corrective action systems, and a dependability knowledge base. Project management reviews should be enhanced to include dependability aspects.

The tailoring of dependability activities includes considering the organisation's technical and administrative processes with their constraints and influencing factors. These constraints and influencing factors include, but are not limited to the following:

- customer requirements;
- regulatory requirements;
- safety requirements;
- delivery targets;
- allowable budgets;
- available resources;
- technical capability;
- environmental impact and risk exposures;
- novelty of technology involvement;
- provision of sustainable services.

They affect the outcome of successful dependability application to achieve the trustworthiness in item performance from a user perspective.

However, flexibility in the tailoring and defining processes is balanced with ensuring appropriate consistency in the dependability processes across the organisation. Flexibility is needed to address contextual variables such as the nature of the customer, cost, schedule, and quality trade-offs, technical difficulty of the work as well as the experience depth of the people implementing the process. Tailoring criteria can allow for using a standard process "as is" with no tailoring or the "same as except for" approach.

6.3 Assessment and measurement

Dependability assessment is an appraisal process to determine the status of an item's dependability performance. Dependability is assessed in two different ways according to the stage in the life cycle:

- forecasted at the design stage by using probabilistic assessment and modelling methods;
- measured and analysed at the operation stage using statistical and other methods.

The dependability characteristic that is measured depends on whether an user or organisational perspective taken and on the applicable performance requirements. For example, for a transportation service, the user (hence the passenger) will be concerned with accessibility of the service (availability of space and conformance to the posted schedule), dependability of service (on-time arrival) and integrity (properly maintained seating and facilities). Dependability can also be assessed by means of an overall effectiveness measure that integrates availability, production rate and product quality.

The characteristics that constitute dependability can be measured either qualitatively or quantitatively. Qualitative assessment can be done descriptively or by using ranking methods.

A quantitative value of dependability performance is derived from observed or estimated data such as time duration and the number of incident occurrences. Dependability characteristics can be quantified in different ways such as instantaneous and operational measures of availability or reliability derived from direct and indirect measures of items in test, operation or maintenance. For example, they can be measured by times of failures, operating time to first failure, duration of intervals of up-time and down-time, and effort expended on maintenance activities.

Since high reliability or availability is difficult and time-consuming to verify by testing, even when using accelerated testing, the reliability of the item can be verified by analysis methods. If it is not possible to test the entire item, tests could be made on the component and module

level. However, the final measure of the performance of the item is not normally feasible until it is in operation.

The measurement process involves

- identifying the type and objectives of the measurements of dependability attributes that are needed under contractual and operational requirements or for specific conditions such as product evaluation
- determining the relevant data and the nature of the data sources for measurements,
- utilizing effective enabling systems to facilitate the measurement process such as deployment of data collection systems, failure reporting, analysis and corrective action systems, survey questionnaires, or other support schemes,
- interpreting the measurement results to establish performance trends, identify critical issues, and recommend management actions with rationales and justifications, and
- documenting the measurement findings for record retention, quality audits, and objective evidence.

6.4 Assurance of dependability performance

The purpose of assurance is to ensure continual improvement during design and implementation and sustain dependability-related performance in operation to assure relevant stakeholders that dependability management activities are being carried out well and will achieve required dependability performance.

Assurance is the process to ensure item conformance to established requirements, standards, and procedures. Assurance establishes the grounds for justified confidence that dependability-related performance achievement claims have been or will be achieved. The assurance objective is to gain the trust of stakeholders that item dependability can be achieved. There are three generic approaches to determining item dependability. They serve different purposes and have varying degrees of engineering rigour. In practice, a combination of these approaches would likely be used.

Demonstration of dependability assurance is achieved by means of actual utilization in an application environment over a scheduled time period to demonstrate dependability-related performance. This may involve formal demonstration or actual performance during warranty or operation.

Inference is achieved by means of statistical methods using observed data of constituent item functions based on established criteria and assumptions to arrive at a numerical value representing dependability characteristics or specific performance characteristics. This may be achieved by prediction, testing, simulation, a capability maturity model or a test case verification.

Progressive evidence is achieved by progressive accomplishment of project milestones with auditable arguments to support objective evidence such as a dependability case, reliability growth programme, environmental impact assessment or root cause analysis.

The dependability case study provides a means of achieving progressive assurance that dependability requirements are being met or will be satisfied throughout the life cycle of the item. The framework for establishing a dependability case for assurance includes

- a reasoned auditable argument to support the contention that a defined item satisfies the dependability requirements,
- a summary of evidence and arguments to support the claims for dependability achievement, and
- progressive assurance throughout the life cycle of the item as target of evaluation.

The dependability case provides a focal point for determining uncertainties and managing related risks. Thereby assurance has become a key factor in risk assessment and risk management, and for the life cycle activities that plan, design, achieve, demonstrate, sustain, and monitor the dependability-related performance during operation.

A reliability growth program is a technique to measure the progress of design with respect to reliability goals as set out in the Dependability Plan. Reliability growth is related to factors such as the management strategy toward taking corrective actions, effectiveness of the improvements, reliability requirements, the initial reliability level, reliability funding and competitive factors. A planned growth curve sets realistic interim reliability goals to be attained during the testing indicating that sufficient progress is being made in order to reach the final goal or requirement. Assessments of the progress should correctly indicate if the program will be successful, or if the interim goals are set too low. Problems and issues can be uncovered in a timely manner.

An environmental impact assessment deals with the process of identifying, predicting, evaluating and mitigating the biophysical, social, and other relevant effects of development proposals prior to major decisions being taken and commitments made. It is an assessment of the item's environmental load to predict or forecast dependability parameters in its defined stressing conditions as the result of exposure to various environmental conditions during utilization. Some typical natural environment stressing conditions are storage and operating temperatures, humidity, and solar loading. Cultural, organisational or political rules can lead to the conclusion that human involvement has dependability impacts.

Root cause analysis is another technique for providing progressive evidence that dependability requirement issues are noted, analyzed and resolved throughout the life cycle of the item. Root cause failure analysis is used to address a problem or non-conformance, in order to get to the primary cause of the problem. It is used so that action can be taken to correct or eliminate the cause, and to prevent the problem from recurring. Typical application is in response to a major failure or the development of corrective action plans to address failures found through internal or customer audits.

Management of dependability assurance activities should engage the use of existing performance monitoring systems to generate the needed information for process and service improvement. Typical examples include

- a failure reporting, analysis and corrective action system,
- a customer care and feedback system,
- a maintenance and logistic support system,
- an incident reporting and fault management system,
- a health monitoring system, and
- a quality management system.

6.5 Dependability management review

The purpose of management review of dependability is to ensure that specific objectives from both technical and business perspectives are being met. The review should set a course of action from a technical perspective to achieve objectives and manage risks.

Management review is different from a management briefing where the information is moving only in one direction to alert senior management. The review process should present a positive element of feedback of deliverables and on checks and balances. The object for each management review should clearly indicate what needs to be accomplished from the review session. An action register is usually maintained to track progress and document closures for open items. Management review should provide an environment to promote meaningful dialogue for participants in the review process. Otherwise, it could easily turn into a debate without gaining any sensible results on value.

Dependability managers should participate in various capacities at management review meetings and contribute accordingly to issues of dependability interest and impact requiring management attention and follow-up actions. A typical dependability management review checklist is shown in Annex E. The checklist is provided to assist dependability management review at major decision points during the life cycle.

The checklist reflects the processes for transfer of responsibilities, resource allocation and transition of ownership during the entire life cycle. The checklist could be used by the supplier and the customer for tailoring purposes to meet their specific application needs.

The checklist is aligned with the life cycle as identified in the process view in Annex C. The information provided herein is based on the recommended dependability actions to meet management objectives.

Reviews related to life cycle management cover a broad range of review activities. Typical reviews conducted at various levels of management which might incorporate dependability components, can include:

- *operations review* to determine the health and operational status of an organisation, a subsidiary division, a manufacturing plant, or a service facility;
- *project review* to determine work progress status, project schedules and milestones commitments, resource availability, outsourcing needs, supplier coordination, and identify problems requiring management actions;
- *technical review* to evaluate new technology platform applications, product line diversification, make-buy decisions, and timeline for new product introduction;
- *design review* to evaluate technical development achievements, dependability assessments, design weaknesses for improvement, product qualification, manufacturability, functional design operability in application environment and service support needs, and final design approval prior to design release to production;
- *production review* to determine resource requirements and delivery schedules, production capacity and throughput, outsourcing and subcontracting of production work, tooling, assembly fabrication, materiel control and testing activities;
- *risk review* to determine whether risks have changed and whether the risk management process is effective;
- *service review* to determine clients' service needs, scheduled and unscheduled maintenance activities, third-party service provisions, logistic support, inventory holdings and depot locations;
- *customer satisfaction review* to address user concerns and improvement strategies;
- *supplier review* to ascertain supplies quality, delivery schedule commitments, ordering process efficiency, multiple sourcing and supply-chain management;
- *quality review* to determine non-conformance status, assurance effectiveness and quality performance trends, identify areas for improvements and recommend management actions;
- *product release review* releasing the product for delivery and/or customer acceptance.

The objective of the review is to determine the progress status and adequacy, and to identify an appropriate course of action on the organisation's on-going management of dependability programs and projects. Dependability management reviews could be conducted as needs arise or in conjunction with other management reviews with broader scope to address dependability management issues associated with the organisation's policy, administration, operation or customer services.

The dependability management review ensures that all critical issues have been assessed and resolved. The review records can be used as objective evidence to support the dependability assurance process.

Annex A (informative) Structure of dependability standards

A.1 Structure

The structure of IEC/TC56 standards is shown in Figure A.1.

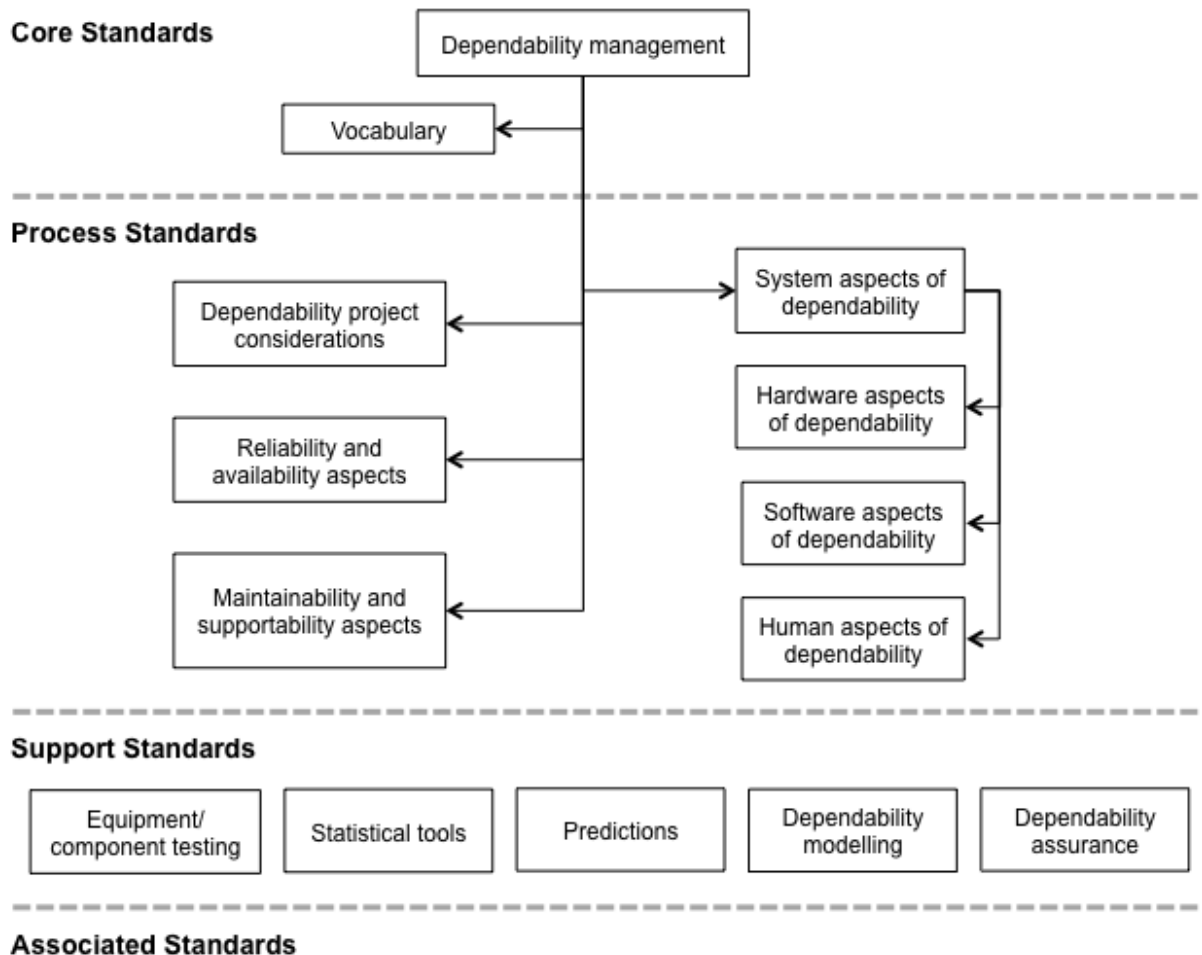


Figure A.1 – Framework for dependability standards

The dependability standards are structured into four levels to facilitate dependability project implementation.

A.2 Core standards

The core standards provide guidance on overall management of dependability and present the standard framework for dependability application. In support of dependability management, the vocabulary contains the basic definitions relevant to dependability. Individual dependability standards can contain specific definitions applicable primarily to that standard.

A.3 Process standards

The process standards focus on the application processes of the major aspects of dependability to facilitate implementation of dependability for projects and achievement of other organisational objectives. The process standards are presented in these major technical focus groupings:

- dependability project consideration: guidance on standards selection for dependability project application;
- reliability and availability aspects: guidance on these characteristics of dependability;
- maintainability and supportability aspects: guidance on these characteristics of dependability;
- system aspects: guidance on standards selection for engineering of system dependability;
- hardware aspects: guidance on standards selection for hardware reliability/availability/maintainability design and supportability implementation;
- software aspects: guidance on standards selection for software dependability design and implementation;
- human aspects: guidance on standards selection for human factors engineering and ergonomic design and application, for human reliability and its assessment.

If a standard deals explicitly with a system and also addresses dependability as a whole (reliability, availability, maintainability and supportability), then it is included within the title 'System aspects of dependability'. Similarly, if the standard only addresses hardware, software or human aspects, then it is included within the respective sub-titles provided it addresses all related aspects of dependability.

Where a document addresses a particular element of dependability for an item, then it is included within the respective titles of 'Reliability & availability aspects' or 'Maintainability & supportability aspects'.

A.4 Support standards

Support standards deal with particular aspects of dependability and describe specific dependability methods and tools to assist dependability implementation. Support standards are focused primarily on the specific methods and techniques for the process groupings and are divided into the following:

- equipment/component testing: testing methods for ensuring equipment/component dependability;
- statistical tools: techniques for statistical evaluation of dependability performance including mathematical symbols and equations;
- predictions: methods for predicting dependability performance;
- dependability modelling: tools for determining dependability for different scenarios;
- dependability assurance: standards to ensure and sustain performance achievement in dependability of items.

A.5 Associated standards

Associated standards include those standards which are not generated by IEC/TC56, but are currently included within the list of standards on the TC56 website for reference purposes.

The standard framework which presents the list of dependability standards and guidance on selection of standards for dependability project implementation can be found on the IEC/TC56 website [1].

Annex B (Informative) Performance element of a dependability management system

B.1 Performance requirements from an application perspective

There is a wide variance in how performance requirements are established and implemented for different applications. The dependability requirements together with the functional requirements define the performance requirements of the item.

The functional requirements can be determined by identifying the needs of stakeholders taking into account aspects such as

- knowledge of similar items and performance data,
- relevant technology and application limitations,
- information on operating environment and usage scenario,
- established standards and relevant specifications, and
- users' experiences and complaints.

The functional requirements can be derived from this set of inputs and translated into technical specifications that will include quantitative requirements of expected performance.

The dependability requirements are an integral part of the overall requirements and relate to how the functional requirements can be achieved from a time-related performance perspective, where time is a general term for a variety of measures such as calendar time, operating time, number of demands, and number of operating cycles.

The dependability requirements can be determined by identifying the needs of stakeholders taking into account aspects such as

- expected length of uninterrupted operation,
- maximum allowable failure rate during operation,
- time to first failure or time to wearout,
- minimum expected availability of the item,
- required maintainability,
- the capability and availability of maintenance and support needs,
- expected total life of the item,
- safety requirements, and
- cost constraints.

Functional and dependability requirements are very closely linked and should not be seen as separate characteristics of performance. Trade-offs can occur between them to achieve a combined solution. For example, a specified level of performance could require decreased maintenance intervals that might be unacceptable from an operational point of view. Cost constraints will impact both functional and dependability requirements.

The following two examples serve to illustrate how functional and dependability requirements can be defined for the two scenarios and the methods that may be used as part of the dependability programme for this item, in the first case where requirements are defined by both provider and user and, for the second case where requirements are defined mainly by the provider based on their understanding of user expectations but without specific user input.

B.2 Examples of performance requirements that include dependability

B.2.1 Requirements determined by both provider and user

In many industrial and other applications, performance requirements are determined by both provider and user. The example given here is that of a motor-driven oil pump in pipeline service, transporting crude oil which has been processed to remove entrained gas and lighter liquids but which still contains some contaminants. The overall function of the pump is to provide dependable pumping capacity and that it does so safely and with minimum environmental impact. The conditions of use or operational environment are tropical with ambient temperatures not to exceed 40°C but with high humidity. Required maintenance will be determined by a risk-based approach such as Reliability Centred Maintenance that will include both normal preventive maintenance tasks and condition monitoring.

The primary functional requirement for the pump is to provide a flow capacity that is defined by a specified head (pressure increase) at a certain flow with an associated efficiency. The expected operating range is between 80% and 120% of the rated design flow. These fundamental performance requirements are derived from the process requirements of the pumping facility and its location in the pipeline system.

The pump unit has a software-based control system supported by instrumentation and remote control from a centralized facility. To minimize environmental impact, the mechanical seals use a nitrogen buffer fluid. Safety protection is built into the control system with fire monitoring and protection devices. A number of available design standards are followed including ones for petroleum pumps, sealing systems and machinery protection systems. Safety concerns are addressed by local and national safety standards.

In this case, all of the main dependability characteristics are applicable. A target of 99% for operational reliability between yearly maintenance activities is established. In order to predict that this level of reliability is achievable, a Reliability Block Diagram, consisting of the major blocks of the pump-motor system, is produced. Data on the reliability of individual equipment or blocks using MTBF is obtained from both industry reliability databases and estimates from the vendor. It is compared to practical results from actual maintenance history for similar equipment already in operation for verification and validation.

High availability is required due to the nature of the pipeline system and downtime is to be minimized with an operational availability of 98% considered to be achievable over a time period associated with a major maintenance cycle. The final availability over a 5-year time period is estimated from the reliability data and the maintenance records including a major overhaul.

Additional dependability characteristics are maintainability and durability. To recover quickly from a failure requires high maintainability and careful supportability planning. Down time due to a major failure usually takes 3 days requiring the pump to be dismantled. For durability, a minimum life of 20 years is necessary with a low life cycle cost compared to similar equipment. A life cycle cost analysis is carried out based on the initial purchase and installation cost and also the anticipated operating and maintenance costs.

The relationship between the functional and dependability requirements is illustrated in Figure B.1.

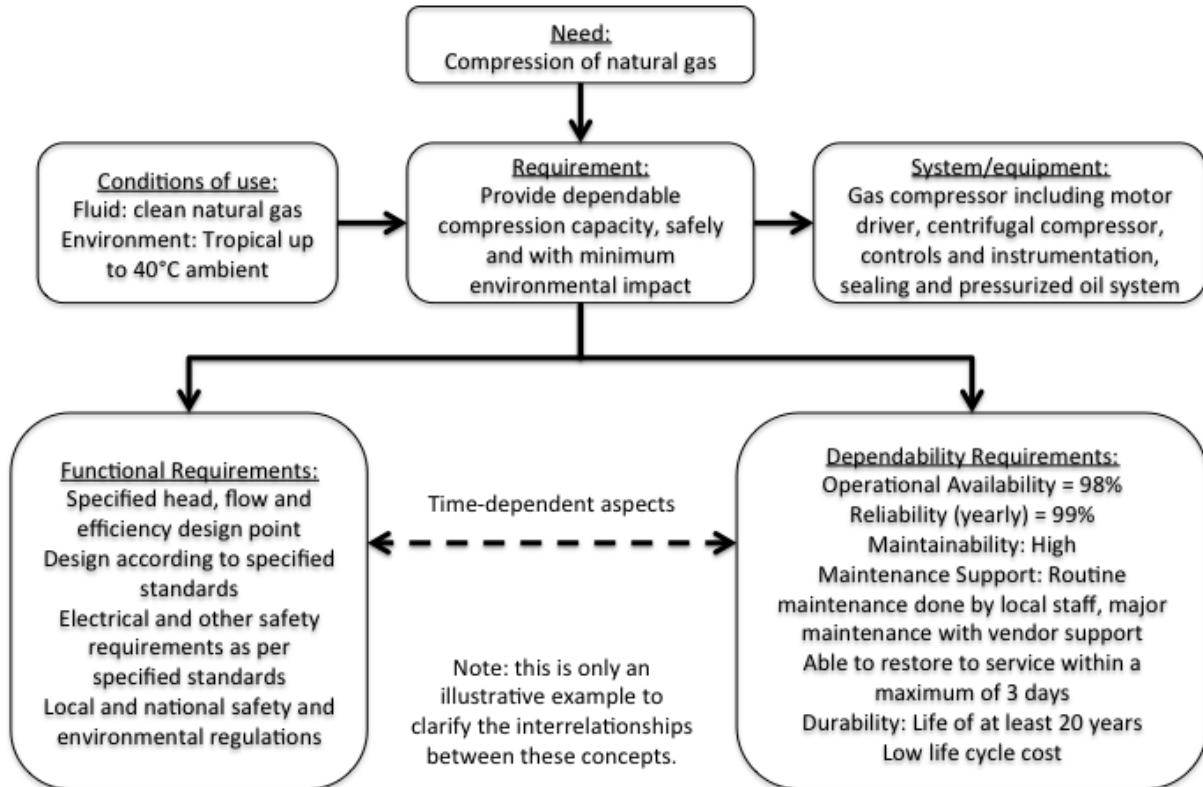


Figure B.1 - Example showing the relationship between functional and dependability requirements for a pipeline motor-driven pump

The decision-making process for functional requirements is largely standardized for this type of product and application. Reliability and availability prediction techniques for the components of the pump-motor system can be used by individual vendors but this is not as common for the final packaged system. Life cycle costing is attempted but sometimes does not include all life cycle costs. The specific reliability costs can be estimated using Weibull estimates but the cost of lost production of an unscheduled outage usually is much larger than the cost of equipment failure. Users that acquire a complete understanding of dependability requirements are normally better able to manage the operation and maintenance phase of the life cycle.

B.2.2 Requirements determined by provider only

Acquiring a family car is a common decision process. The cost of ownership is a major target objective but other functional requirements will influence the final cost and selection of a vehicle. There are quite a few options available to a buyer within a certain price range and the final selection cannot always be based on a rational evaluation of functional and dependability requirements. However, with the exception of some flexibility provided by options available to the customer, the fundamental performance requirements are fixed for each vehicle.

There are certain features of the car representing potential requirements that are essential to the customer. The selection criteria are based on the value of these features from the customer's budget viewpoint. The conditions of use are defined by the driving environment such as type of roads, ambient temperature and possible rain or snow conditions.

The desirable functional features for selection include

- size and capacity, both number and type of passengers and other carrying requirements,
- fuel economy,
- ease of driving and parking,

- safety protection such as crash-worthiness,
- build quality,
- initial purchase cost,
- operating and maintenance costs, and
- optional features.

The desirable dependability characteristics are mainly reliability, maintainability and supportability. Availability is not usually a major concern as long as maintenance support services are located close to the user but durability can be very important if the objective is to own the vehicle for a long time. The resultant dependability requirements for selection include

- reliability,
- maintainability,
- location and accessibility of maintenance support services, and
- durability.

These features represent a set of performance requirements for the car under consideration by the user. There are interrelationships between the functional and dependability requirements, for example, maintainability will clearly influence maintenance costs and build quality will be related to durability. There are also requirements which compete and where trade-offs will need to be made. For example, while quality of build, reliability and safety are probably related these are likely to conflict with a requirement for a low initial purchase cost.

The objective is to set a priority of importance pertaining to the relevant requirements identified which can be done by means of a decision matrix.

In this example the customer is faced with a set of options that fulfill the performance requirements to various degrees but none completely fulfill all requirements. One method by which a decision can be made is for the customer to weight the relative importance of their requirements, then to scoring each option according to how it achieves each requirement. The choice is the option that achieves the highest total weighted score.

Although the individual user has no direct input to the performance requirements, manufacturers of personal vehicles will use various means such as customer surveys to guide their selection of performance requirements and expectations for the target user market they are aiming at.

A graphical representation of this example is shown in Figure B.2.

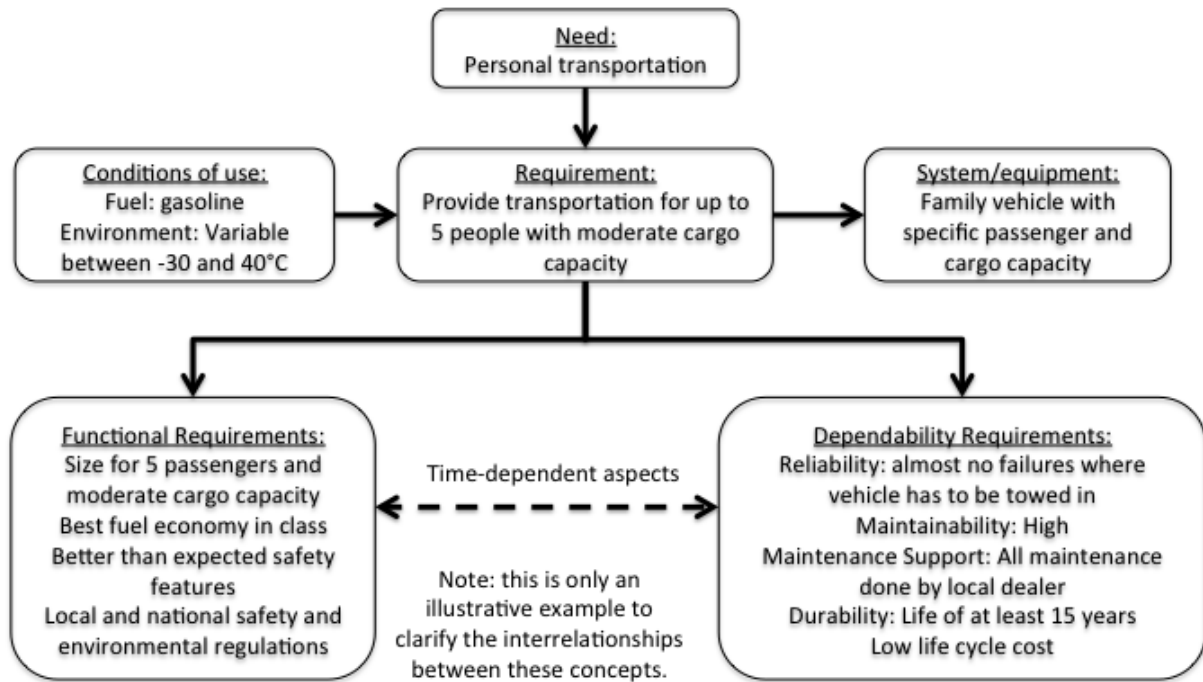


Figure B.2 - Example showing the relationship between functional and dependability requirements for a family car

Annex C (Informative) Process element of a dependability management system

C.1 Dependability processes within the life cycle

The process view is concerned with the interrelated and interacting activities that are needed to achieve required dependability performance. A variety of processes are needed as items are created or acquired, used or operated, enhanced and finally retired or disposed. This series of identifiable stages is known as the life cycle and forms the basis for dependability processes.

For the purpose of this annex, a generic life cycle has been used that should be generally applicable to all items. Note that these stages often overlap in their timing.

a) Concept

The *concept* stage is the initial visioning stage for an item. It can entail activities to identify market or other needs, define/identify the general operational use environment and timeline, define/identify the regulatory requirements (such as traceability, safety, environment, sustainability, retirement and waste disposal), the preliminary dependability requirements and confirm feasible design solutions by producing broad technical specifications for the design. Selection of design options is based on risk analysis, impact evaluation, and practical engineering approaches. The process activities involve requirements definition, requirements analysis, architectural design, and functional design/evaluation to provide high-level specifications. Potential needs for trade-off between safety and dependability should be identified at this stage. Relevant modeling and probabilistic approaches can be used to achieve high-level dependability predictions in order to select the preliminary architecture and the maintenance and supportability policies which are likely to meet the regulatory and dependability requirements. Risk assessment during the concept stage should focus on the feasibility of concept design and technology selection for project implementation.

b) Development

The *development* stage follows the initial concept once its feasibility has been verified. The focus is to plan and execute selected engineering design solutions for realization of item functions. This is transcribed into an appropriate design and development effort including system architecture, engineering modelling, prototype construction, risk assessment, and interface identification of system and subsystem elements. Systematic evaluation of the integrated item functions is conducted to verify interoperability of item performance and interactions with external environments to validate the final configuration. Supportability planning, maintenance access, operational procedures and assurance as well as support processes should be well established prior to item realization. Relevant modeling and probabilistic approaches can be used at this stage to achieve detailed dependability predictions in order to consolidate the architecture and the maintenance and supportability policies selected at the conceptual stage and to verify that the regulatory and dependability requirements are likely to be met.

c) Realization

The *realization* stage entails executing make-buy decisions for the acquisition, and/or manufacturing of the final item and its components. The realization efforts deal with activities such as technology application, tooling, manufacturing, packaging and supplies sourcing to ensure the complete transformation from the design to the specified item or its subsystem components. The realized items or components can comprise a combination of hardware and software functions. Realization includes component and module simulations, analyses and tests including integration tests as well as activities such as assembly of components, integration of item functions, verification of subsystems, and installation of the item. Acceptance procedures should be established with the customer with possible trials in the actual operating environment prior to commissioning. Validation

should be a part of the trial to provide objective evidence of conformance to specifications.

d) Utilization

The *utilization* stage is when the item is deployed for delivery of functionality or service with support of its operational capability by means of maintenance. The process activities include operating and maintaining the item in accordance with performance requirements, training for operators and maintainers to maintain skills competency, customer interface to establish service relationship, and record keeping on item performance status and reporting failure incidents to initiate timely corrective and preventive actions. The item performance should be monitored and checked on a regular basis to ensure that dependability, regulatory and quality of service objectives are met. Data collection and sampling could be used to estimate service dependability. Risk assessment during operation and maintenance can deal with issues that arise due to changing conditions.

e) Enhancement

The *enhancement* stage can be needed to improve item performance with added features to meet growing user demands, extend operating life or address obsolescence. The process activities can include hardware or software upgrade or addition, maintenance improvements, simplifying procedures to improve operational efficiency or obsolescence management. Relevant modeling and probabilistic approaches can be used at this stage to assess the impact of the possible enhancements and select the best solutions. Risk assessment during enhancement stage often looks at cost vs. benefits and return-on-investment.

f) Retirement

The *retirement* stage occurs at the end of the life of the item. Upon termination of the use of an item, it can be disassembled, redeployed for other uses, disposed for reuse of materials and components or, in some cases, abandoned in situ (such as a pipeline). This should be considered since the conceptual stage. For complex items, a strategy for decommissioning can be established to formalize planning and implementation of the decommissioning process to meet regulatory requirements. For other items, regulatory rules concerning return and reuse or disposal can be in existence.

Dependability processes are often considered in the context of the life cycle as shown in Figure C.1.

Variations of these generic life cycle stages can result in more specific life cycle stages such as:

- product: concept/definition, design/development; manufacturing/installation; operation and maintenance; mid-life upgrading, or life extension; and decommissioning/disposal;
- facility: concept/definition; design and development; construction and commissioning; operation and maintenance; mid-life upgrading, or life extension; and decommissioning and disposal;
- hardware: concept, design, fabrication/manufacturing and installation/commissioning, operation/maintenance, modification, disposal;
- software: concept, development, application, operation/maintenance, enhancement, retirement.

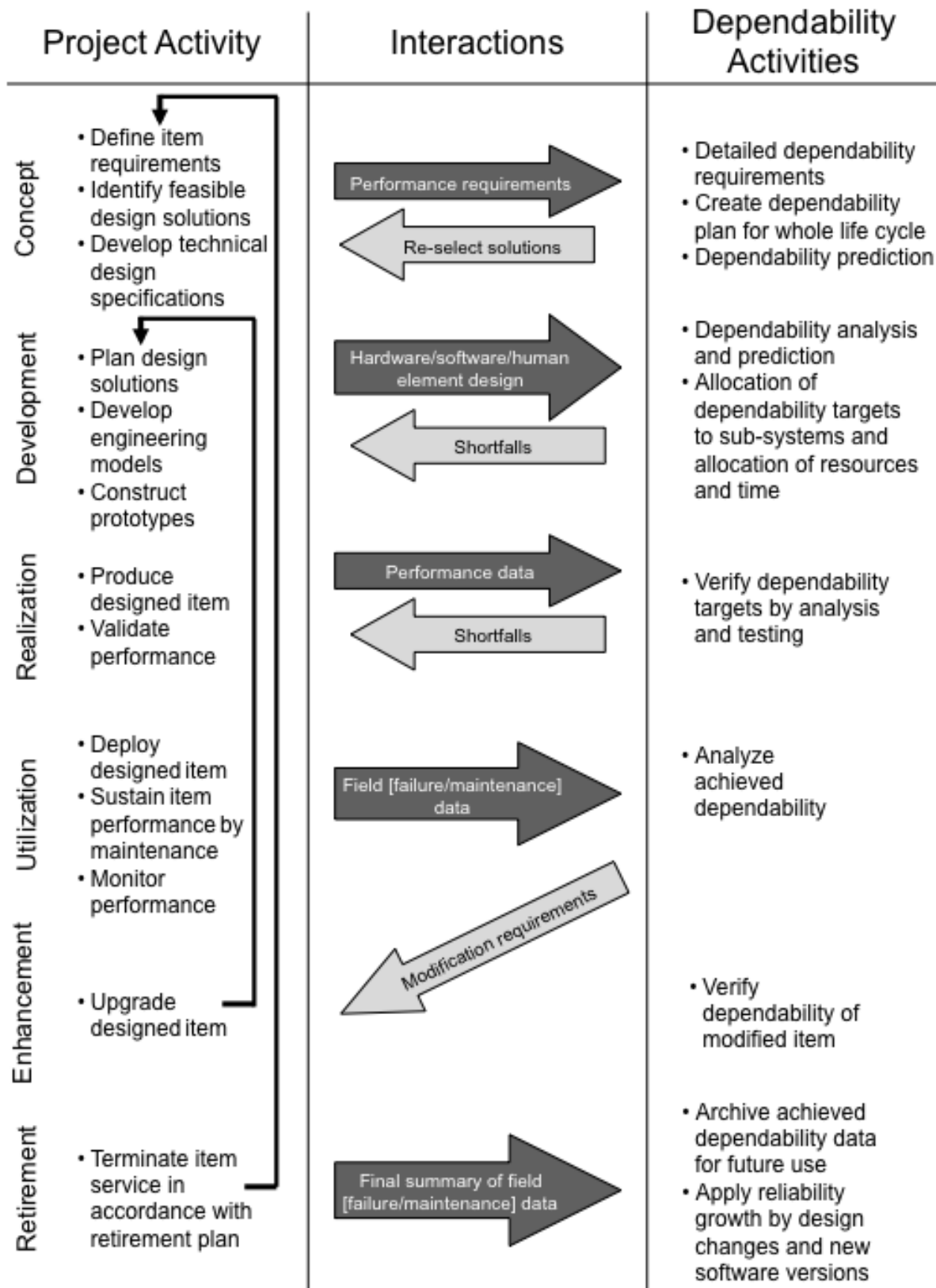


Figure C.1 – Dependability processes and the life cycle

C.2 Dependability life cycle processes

The following tables provide typical examples of dependability-related activities that can be part of a life cycle. This list is not exhaustive and should be modified or tailored to meet specific requirements.

Table C.1 – Processes during the concept stage

Dependability objectives	Dependability strategies	Activities with Impact on dependability
1. Define item requirements	a. Identify market or other relevance and dependability values of new initiatives	<ul style="list-style-type: none"> • Conduct market or other surveys and research studies to assess customer/user needs • Identify regulatory requirements related to new initiatives • Determine competitive leverage on dependability values • Identify scope of market or other needs and assess risk of new initiatives • Establish the context
	b. Establish dependability policy and incentives for implementation	<ul style="list-style-type: none"> • Determine timing for new venture initiation and define innovation objectives • Formulate strategic plans for new item development and acquisition tactics • Rationalize resource commitments to support new initiatives and on-going program portfolios • Plan achievement targets • Establish project tailoring criteria • Document policy and mission statement • Determine development tools and procedures
2. Analyze item performance requirements	a. Identify technical approaches and feasibility for item realization	<ul style="list-style-type: none"> • Conduct requirements analysis • Determine item boundaries, operating functions and performance characteristics from the set of defined performance requirements • Achieve probabilistic evaluations in order to establish feasible solutions and define the preliminary architectures • Identify the organisation's capability to undertake the work • Identify risks • Evaluate trade-offs which can be required between desirable functional and dependability requirements • Determine resource requirements and evaluate allocation plan for specific project tailoring. • Determine technical and quality measures for design guidance and to enable dependability assessments
	b. Identify potential partnership and supplier requirements	<ul style="list-style-type: none"> • Determine feasibility of supply-chain and joint venture collaboration • Determine outsourcing requirements
3. Establish high level design criteria	a. Identify appropriate logical architectural design options	<ul style="list-style-type: none"> • Establish item configuration • Partition item functions • Select technologies for design and choice of hardware/software for realization of functions • Formulate make/buy decisions of item functions • Formulate solution to meet item requirements • Establish means for verification and integration of item functions
	b. Establish design requirements for evaluation	<ul style="list-style-type: none"> • Formalize the design process and how trade-offs will be handled • Identify design composition of hardware/software elements for each function

	<ul style="list-style-type: none"> • Incorporate test functions for performance verification • Establish human factors design criteria • Establish dependability design criteria • Perform dependability prediction • Establish environmental design criteria • Establish ergonomics design and interface criteria • Establish electro-magnetic compatibility design criteria • Establish safety, security and reliability design criteria • Establish hardware design guidelines • Establish software design guidelines • Simulate item performance at functional level to determine fault coverage and item recovery strategy • Verify performance limits, robustness and interoperability of item functions to meet architectural design requirements
c. Document item specifications	<ul style="list-style-type: none"> • Incorporate dependability requirements in item specifications

Table C.2 – Processes during development stage

Dependability objectives	Dependability strategies	Activities with Impact on dependability
1. Design and develop the item	a. Initiate item design	<ul style="list-style-type: none"> • Establish item dependability program • Establish quality assurance program • Establish configuration management plan and design change procedures • Achieve probabilistic evaluations in order to assess the forecasted dependability values • Determine risk assessment requirements • Establish test plan and item acceptance criteria • Establish item monitoring, diagnostic schemes, incidents reporting and data management system • Establish suppliers' dependability programs
	b. Initiate full scale item development	<ul style="list-style-type: none"> • Formalize dependability requirements for system, subsystems and functions • Implement project tailoring plan • Achieve probabilistic evaluations in order to verify that the dependability targets are likely to be reached • Develop software test and diagnostic program • Establish dependability acceptance criteria and reliability growth programs • Establish item maintenance and logistics support program • Conduct risk assessments • Monitor and collaborate with material outsourcing and contracting external development efforts • Develop spares provisioning program • Define warranty conditions • Establish training programs

Table C.3 – Processes during the realization stage

Dependability objectives	Dependability strategies	Activities with Impact on dependability
1. Item realization	a. Initiate production or acquisition of hardware assemblies and functions	<ul style="list-style-type: none"> • Implement item dependability program • Implement quality assurance program • Implement failure reporting, analysis, data collection and feedback system • Establish configuration management plan and design change procedures • Establish test plan and item acceptance criteria • Establish item monitoring, diagnostic schemes, incidents reporting and data management system • Implement suppliers' dependability programs
	b. Initiate software module functions and item development	<ul style="list-style-type: none"> • Implement software reliability assurance program • Implement software test and diagnostic program • Implement software qualification and evaluation plan for acceptance
2. Item implementation	a. Item integration	<ul style="list-style-type: none"> • Execute integration plan • Coordinate outsourcing and support programs • Implement configuration management plan and design change procedures • Prepare and perform analysis and tests of components and modules • Prepare plans for and perform item acceptance analysis and testing • Perform required changes for reliability growth • Prepare item acceptance plan • Prepare verification and validation plans and procedures
	b. Item verification/validation	<ul style="list-style-type: none"> • Implement verification/validation plan • Document verification/validation test results • Conduct failure analysis and recommend preventive/corrective actions for improvement
	c. Item installation and acceptance	<ul style="list-style-type: none"> • Execute installation plan • Document installation records and procedures • Conduct item acceptance and generate acceptance report • Implement warranty schemes if applicable • Establish shared supportability and reporting schemes with customer maintainers on item installed on customer premises • Customer sign-off for item acceptance to initiate official item operation and full-scale deployment • Resolve warranty issues with customers

Table C.4 – Processes during the utilization stage

Dependability objectives	Dependability strategies	Activities with Impact on dependability
1. Item operation and maintenance	a. Implement operation strategy	<ul style="list-style-type: none"> • Monitor item performance • Implement reliability growth program • Implement field data collection system for information about in-service dependability • Conduct customer satisfaction survey
	b. Implement supportability strategy	<ul style="list-style-type: none"> • Provide customer care service • Monitor item maintenance efforts • Analyze failure trends and maintenance service records • Recommend design or procedural changes for

		continuous improvement <ul style="list-style-type: none"> • Determine quality of service and provide customer value
--	--	--

Table C.5 – Processes during the enhancement stage

Dependability objectives	Dependability strategies	Activities with Impact on dependability
1. Item enhancement	a. Implement item enhancement strategy	<ul style="list-style-type: none"> • Identify new feature and enhancement requirements • Evaluate the need for change and resulting benefits • Conduct risk and value assessments • Analyse the impact on safety requirements • Implement enhancement efforts • Evaluate impact on dependability-related performance due to changes with added new features • Conduct customer satisfaction survey resulting from change reactions

Table C.6 – Processes during the retirement stage

Dependability objectives	Dependability strategies	Activities with Impact on dependability
1. Item retirement	a. Implement item retirement strategy	<ul style="list-style-type: none"> • Execute item retirement/decommissioning plan • Implement reuse of components and materials from disposed items • Implement waste treatment on disposal items • Notify customers on service termination • Provide information on new or alternative service provision • Conduct customer satisfaction survey due to termination of service

Annex D (informative) Organisational element of a dependability management system

D.1 Organisational structures

In order to achieve their objectives effectively, organisations are usually structured into entities or business units with several levels of hierarchies. Each of these entities has responsibility for managing certain activities with assigned resources to accomplish their tasks. Unless objectives are very simple and easy to achieve, activities are normally divided into multiple groups for efficiency based on factors such as common skill sets or physical location requirements. Groups have leaders to manage activities, often with several layers of management. In many organisations, dependability is a very important requirement that needs to be met and the organisational structure should accommodate these specific requirements.

Some organisations exist for a certain time period in order to achieve a specific objective as is common with situations such as product development and design and construction of facilities. With these project-oriented organisations, dependability is usually of paramount importance. During the subsequent utilization or operational phase, an organisation can exist for a longer time period and dependability will continue to be important for meeting organisational objectives. In both situations, dependability requirements will need to be accommodated in the organisational structure.

In organisations where business or technology is fast-moving, new organisational structures are appearing. Typical examples include new partnerships to promote communications networks, cross-regional and national jurisdictions in transportation and distribution, and specialized one-stop manufacturing services where different organisations collaborate by agreements to work together worldwide. Facilities can be established, transported and duplicated in almost any country where human resources, security and a level playing field can be established and sustained. Some vertically integrated organisations have also engaged in matrix management and participative organisational structures to retain expertise for strategic deployment. The organisational view then expands beyond standard corporate management and extends the collaboration of government, industry and academic institutions where different expertise and resources exist among them to facilitate sharing of responsibilities and achievement of cooperative results.

D.2 Organisation of dependability activities

There are different possible approaches to structuring an organisation to enable dependability objectives to be met successfully. Since overall performance requirements are a combination of functional and dependability requirements, they require close coordination of activities and should be seen as an integrated set of activities within an organisation. In general, dependability activities should be included within an organisational structure under one of the following general scenarios.

- Dependability activities are fully integrated into the organisational structure with dependability resources embedded into an organisational entity, for example, where every employee is responsible for the dependability aspects of his or her activities. But often one or more persons are assigned as facilitators for such activities.
- Dependability activities are sufficiently time-consuming and important that one or more organisational entities will be needed to complete dependability activities as would be appropriate for the design, construction and commissioning of a major facility. These entities would still function in coordination with other entities.
- For a large organisation with multiple product lines or many large facilities to operate, it can be worthwhile to set up a major organisational entity to serve the overall needs of the organisation in an efficient manner. This would eliminate duplication of effort and ensure

consistency of dependability activities while at the same time enabling the highest level of expertise to be applied.

- With any of these scenarios, specific activities can be outsourced, either because they are very specialized or their duration is short.

Dependability can be managed within different organisational structures as defined by business objectives. Dependability management does not require any specific separate structure but whatever the structure, dependability should be integrated into an organisation's decision-making and activities.

Key factors that contribute to successful achievement of dependability requirements from an organisational perspective include:

- defining a single overall responsibility for meeting dependability requirements and coordinating shared responsibilities among the various organisational entities that can be involved;
- supplying and enabling expertise and competence of dependability resources to carry out activities;
- managing information associated with dependability and related functional requirements;
- coordination between internal and external groups involved with dependability activities;
- incorporating dependability requirements in decision-making and fully understanding trade-offs that can be made between functional and dependability requirements and project-related factors such as schedule and cost.

Annex E
(informative)
Checklist for management review of dependability

E.1 Introduction

The following checklist is an example of the dependability-related issues that can be necessary for management review to ensure that dependability objectives are being met. The list needs to be tailored for individual circumstances with agreement by both management and staff responsible for carrying out dependability activities. The checklists in the example are somewhat general and can require additional specific criteria to enable proper review.

E.2 Concept

E.2.1 Requirements definition

- a) The dependability objectives established are suitable to meet market needs and user applications.
- b) The extent of market scope and strategy for new initiatives are identified including customer use conditions and market operating conditions e.g., climatic conditions.
- c) The dependability value, competitive leverage, incentives and application constraints are determined.
- d) The timing for new product introduction and achievement targets are identified.
- e) The tailoring criteria are established and applicable processes are identified.
- f) The information on the proposed new system is adequate to initiate requirements analysis.

E.2.2 Requirements analysis

- a) The requirements analysis of the system boundaries, operating functions and performance characteristics and technology limitations has been conducted and determined.
- b) The resource availability, technical capability, and new investment needs are identified.
- c) The technical approaches and feasibility for system realization are identified.
- d) The potential partnership and supplier requirements are identified.
- e) The requirements analysis results and rationale can be justified for resource investments to initiate high-level concept design of the new system.

E.2.3 High-level architectural design

- a) The architectural design criteria, possible item configuration and options are identified.
- b) The technology selection for design of item functions for realization is identified.
- c) The forecasted probabilistic evaluations are consistent with the dependability targets.
- d) The make/buy decision criteria are established.
- e) The means for verification and integration of item functions have been established.
- f) The criteria for hardware/software design functions have been established.
- g) The criteria for environmental and ergonomic designs have been established.
- h) The criteria for evaluation of item functions have been established.
- i) The interoperability of system functions and performance limits has been verified to meet item requirements.
- j) The dependability requirements in item specifications are incorporated as guidance for design and COTS acquisition.

- k) The new item concept and architectural design options are identified and verified with associated constraints to justify initiation of formal item design with documented specifications.

E.3 Development

E.3.1 Item design

- a) The dependability plan for design of the item and its components is established.
- b) The quality assurance plan and item configuration management process are established.
- c) The forecasted probabilistic evaluations are consistent with the dependability targets.
- d) Test plans and acceptance criteria are established and simulation and tests have been performed.
- e) The item monitoring and control, incidents reporting and data management systems have been established.
- f) The suppliers' dependability programs have been established.
- g) The item design is verified and support programs established for full-scale development.

E.3.2 Full-scale system development

- a) The tailoring process for various item and functional development projects is implemented and the responsibility to each project assigned, including dependability inputs to the design process.
- b) The verification that the forecasted probabilistic evaluations are consistent with the dependability targets has been performed.
- c) The item verification and validation plans have been developed.
- d) The dependability acceptance criteria and reliability growth programs have been established.
- e) Design has been modified and reliability growth has been verified.
- f) The item maintenance and logistics support programs are established.
- g) The outsourcing programs are established.
- h) The spares provisioning program is developed.
- i) The training programs are established.
- j) The warranty criteria for system service support are established.
- k) The item is fully developed and ready for production and construction.
- l) Software specifications and flow charts have been finished and approved.
- m) The development of software module functions and subsystems has been initiated.

E.4 Realization

E.4.1 Item realization

- a) The production of hardware assembles and functions has been initiated.
- b) The suppliers' dependability programs are implemented.
- c) The item functions and subsystem verification and validation plans are implemented.
- d) The failure reporting, analysis and data collection systems are implemented.
- e) The training programs are developed.
- f) The item is produced, constructed and realized and ready for implementation.

E.4.2 Item implementation

- a) The system integration plan is implemented.

- b) The item verification and validation plans are implemented.
- c) The item qualification and acceptance plans are implemented.
- d) The item installation plan is implemented.
- e) The warranty plan is implemented.
- f) The training programs for system operation and customer care services are initiated.
- g) The required design changes for fulfilling the dependability requirements have been implemented and verified.
- h) The item is ready for release to operation.

E.5 Utilization

- a) The item performance and service maintenance are monitored and controlled.
- b) The training programs for operators and maintainers are implemented.
- c) The field data collection system is implemented.
- d) The design change and configuration control are implemented.
- e) The customer satisfaction survey is implemented.
- f) The item performance data are analyzed for continuous improvement.
- g) The item continues to sustain operational dependability-related performance.

E.6 Enhancement

- a) The new item features and enhancement needs are identified.
- b) The risk impact, in particular with regards to safety requirements, and value of enhancement are analyzed.
- c) The enhancement programs and improvement time frame are determined.
- d) The decision for enhancement programs is executed.
- e) The customer satisfaction survey resulting from the enhancement programs are monitored to determine enhancement value.

E.7 Retirement

- a) The retirement and disposal strategy is planned and initiated.
- b) The service termination impact is determined.
- c) The schedule and timing for service termination and the new or alternative service provisions have been notified to customers.
- d) The customer satisfaction survey resulting from termination of old service and the use of new service is monitored.
- e) Required data has been transferred.

Bibliography

- [1] IEC/TC56 website, <http://tc56.iec.ch>