BS EN 60300-1:2014

BSI Standards Publication

Dependability management

Part 1: Guidance for management and application

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 60300-1:2014. It is identical to IEC 60300-1:2014. It supersedes BS EN 60300-1:2003 and BS EN 60300-2:2004, which are withdrawn.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 78089 9
ICS 03.100.40; 03.120.01; 21.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2014.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60300-1

September 2014

ICS 03.100.40; 03.120.01; 21.020

Supersedes EN 60300-1:2003, EN 60300-2:2004

English Version

Dependability management - Part 1: Guidance for management and application (IEC 60300-1:2014)

Gestion de la sûreté de fonctionnement - Partie 1: Lignes directrices pour la gestion et l'application (CEI 60300-1:2014)

Zuverlässigkeitsmanagement - Teil 1: Leitfaden für Management und Anwendung (IEC 60300-1:2014)

This European Standard was approved by CENELEC on 2014-06-27. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 60300-1:2014 E

Foreword

The text of document 56/1550/FDIS, future edition 3 of IEC 60300-1, prepared by IEC TC 56, “Dependability”; was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 60300-1:2014.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2014-09-27
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2017-06-27

This document supersedes EN 60300-1:2003 and EN 60300-2:2004.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 60300-1:2014 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION

This part of IEC 60300 describes the processes involved in managing dependability within an organization 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. 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 describes the extent to which something can be trusted to behave as expected.

Dependability creates trust and confidence and affects the ability of an organization to meet its objectives. It is achieved by effective planning and implementation of dependability activities throughout the life cycle of items.

Dependability has a strong impact on the user's perception of the value of an item developed or provided by an organization. Poor dependability will affect an organization's capability to deliver its objectives and reduce its reputation.

Dependability management provides a systematic approach for addressing dependability and related issues from an organizational and business perspective. Dependability is often driven by technology and requires the integration of innovation with legacy products. Achieving dependability throughout 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 organizational objectives and return-on-investments.

This standard 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 side effects on safety, environment and other factors should be identified, analysed and managed when optimizing dependability.

The intended audience for this standard ranges from users, owners and customers to organizations involved in and responsible for ensuring dependability requirements are being met. Organizations include all types and sizes of corporations, public and private institutions such as in government agencies, 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 integrated combinations of these elements. It presents guidance on planning and implementation of dependability activities and technical processes throughout the life cycle taking into account other requirements such as those relating to safety and the environment.

This standard gives guidelines for management and their technical personnel to assist them to optimize dependability.

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.

None.

3 Terms, definitions and abbreviations

For the purposes of this document, the following terms and definitions apply.

3.1 Terms and definitions

3.1.1
availability < of an item>
ability to be in a state to perform as required

Note 1 to entry: 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 to entry: Availability may be quantified using appropriate performance measures.

[SOURCE: IEC 60050-191:2014 [1][1], 191-41-23]

3.1.2
dependability <of an item>
ability to perform as and when required

Note 1 to entry: Dependability includes availability, reliability, recoverability, maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security.

_____

1 Numbers in brackets refer to the bibliography.

Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.

[SOURCE: IEC 60050-191:2014, 191-41-22]

3.1.3
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system will satisfy the dependability requirements

3.1.4
dependability management
coordinated activities to direct and control an organization with regard to dependability

Note 1 to entry: Dependability management is part of an organization's overall management.

3.1.5
dependability management system
set of interrelated or interacting elements of an organization to establish dependability-related policies and objectives and the processes to achieve those dependability objectives

Note 1 to entry: Systems for managing dependability are part of the overall management system and not usually a separate management system.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, procedures and processes.

3.1.6
dependability plan
set of scheduled activities to achieve dependability objectives and targets for an item

3.1.7
dependability programme
coordinated set of plans that describe the activities that lead to cost-effective achievement of dependability objectives and targets and the way they are resourced

3.1.8
item
subject being considered

Note 1 to entry: The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

Note 2 to entry: The item may consist of hardware, software, people or any combination thereof.

Note 3 to entry: The item is often comprised of elements that may each be individually considered.

[SOURCE: IEC 60050-191:2014, 191-41-01]

3.1.9
life cycle
series of identifiable stages through which an item goes, from its conception to disposal

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

Note1 to entry: The stages identified will vary with application.

[SOURCE: IEC 60050-191:2014, 191-41-09]

3.1.10
maintainability <of an item>
ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance

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

Note 2 to entry: Maintainability may be quantified using appropriate measures.

[SOURCE: IEC 60050-191:2014, 191-41-27]

3.1.11
maintenance support
provision of resources to maintain an item

Note 1 to entry: Resources include human resources, support equipment, materials and spare parts, maintenance facilities, documentation and information, and maintenance information systems.

[SOURCE: IEC 60050-191:2014, 191-41-28]

3.1.12
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization 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 to entry: For organizations with more than one operating unit, a single unit may be defined as an organization.

3.1.13
reliability <of an item>
ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration may be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions and maintenance.

Note 3 to entry: Reliability may be quantified using appropriate measures.

[SOURCE: IEC 60050-191:2014, 191-41-24]

3.1.14
requirement
need or expectation that is stated, generally implied or obligatory

[SOURCE: ISO 9000:2005, 3.1.2]

3.1.15
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

3.1.16
supportability <of an item>
ability to be supported to sustain the required availability with a defined operational profile and logistic and maintenance resources

Note 1 to entry: Supportability complements the inherent reliability and maintainability of the item, combined with factors external to the item that affect the relative ease of providing the required maintenance and logistic support.

[SOURCE: IEC 60050-191:2014, 191-41-31, note 1 has been modified]

3.1.17
system <in dependability>
set of interrelated items that collectively fulfil a requirement

Note 1 to entry: A system is considered to have a defined real or abstract boundary.

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

Note 3 to entry: A system structure may be hierarchical, e.g. system, subsystem, component, etc.

Note 4 to entry: Conditions of use and maintenance should be expressed or implied within the requirement.

[SOURCE: IEC 60050-191:2014, 191-41-03]

3.1.18
tailoring <process>
process to adapt, adjust or alter an organization'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
FMEA	Failure modes and effects analysis
FRACAS	Failure recording, analysis and corrective action system
FTA	Fault tree analysis
HSE	Health, safety and environment
MTBF	Mean time between failure
HAZOP	Hazard and operability studies
RCM	Reliability centred maintenance

4 Dependability management

4.1 Understanding dependability

Dependability is the ability of an item to perform as and when required. Dependability is thus the ability to fulfil the requirements and expectations of an item consistently over time. Dependability creates value in that the item retains its performance characteristics, operates as desired, and satisfies customer needs and expectations.

Management of dependability is a key element of an organization's wider management systems in particular those for assets, finance and quality. Dependability management encompasses the planning and application of organizational arrangements, processes and associated methods and techniques to achieve the organization's performance and product objectives.

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, eliminating root causes of failure, simplifying complex processes, mitigating anomalies, promoting fault tolerance in design and fitness for use, advocating fault avoidance and error prevention, managing maintenance activities and making commitments to build 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, time consuming and costly at a later time.

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 organizations responsible for ensuring dependability requirements are met.

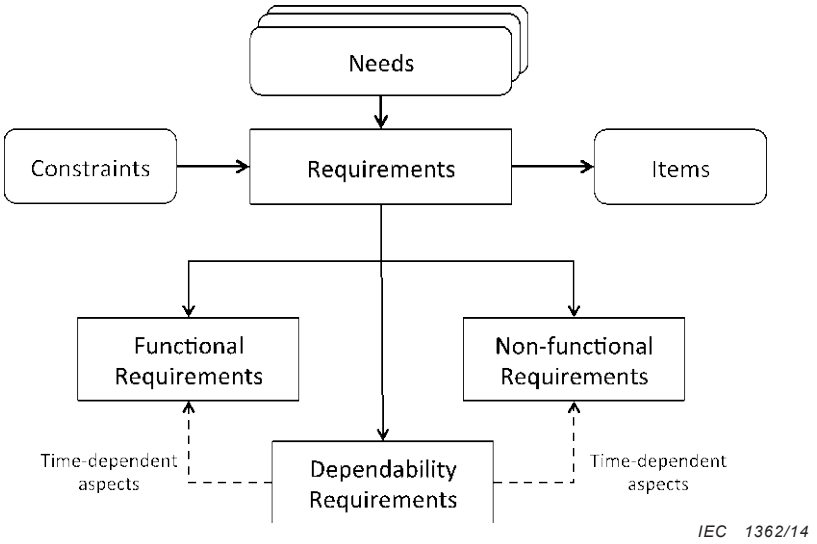


Figure 1 – Relationship of dependability to the needs and requirements of an item (product, system, process or service)

Requirements are determined from the needs of stakeholders and from constraints such as the conditions of use, resources and legislation. They include functional requirements, which define what the item is required to do, and non-functional requirements, which specify additional attributes. Examples of functional requirements are capacity and power output and examples of non-functional requirements are safety, environmental sustainability and efficiency. Dependability requirements, which define the time-dependent ability to achieve dependability performance in these requirements consist of characteristics such as reliability, availability, maintainability and supportability.

Functional and non-functional requirements and dependability requirements are inter-related. A dependability requirement can only exist if there is a functional or non-functional requirement that has to be satisfied. There can be competing objectives between desirable requirements, such as safety or oil/gas production and dependability, and therefore trade-offs may be necessary. 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 might need to be considered while defining requirements.

Dependability includes objectively measureable characteristics, such as reliability, availability and maintainability, and more subjective judgements of trustworthiness relating to the functions required by particular stakeholders. The ability to measure the attainment of performance objectives is a fundamental consideration in setting the requirements.

Dependability includes both the ability to meet functional and non-functional requirements under normal and expected conditions, and the ability to adapt to unexpected changes in requirements, assumptions and circumstances to recover from external system failures.

4.2 Benefits of dependability management

Managing dependability results in benefits such as

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

4.3 Challenges of managing dependability

Dependability needs to be 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.

There can be complications when multiple organizations are involved, mid-life upgrading occurs, or the item’s dependability is influenced by interconnected and external systems.

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 needs to ensure interoperability and dependability of the integrated items through interface specifications to ensure dependable performance.

Systems are becoming more complex and can exhibit the characteristics of "open systems”, “systems of systems” or “unbounded or weakly bounded systems”. The systems can be managed by different parties that have different objectives and can be at different stages of the life cycle. This, together with the scale and complexity of the system makes it difficult for any stakeholder to comprehend the system as a whole and changes are thus less predictable and controllable. For that reason, it is crucial for stakeholders to understand and agree on the boundaries of their responsibilities and to assign accountability for implementation. Planning for dependability needs to take into account the potential for major failures and changes outside respective boundaries as well as inside.

5 System for managing dependability

5.1 Overview

The purpose of a system for managing dependability is to direct and control an organization with regard to dependability, coordinating with other disciplines to provide an efficient and integrated effort to achieve objectives. Organizational policies and objectives may include dependability policies and objectives, which then lead to a dependability management system that can effectively implement them.

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

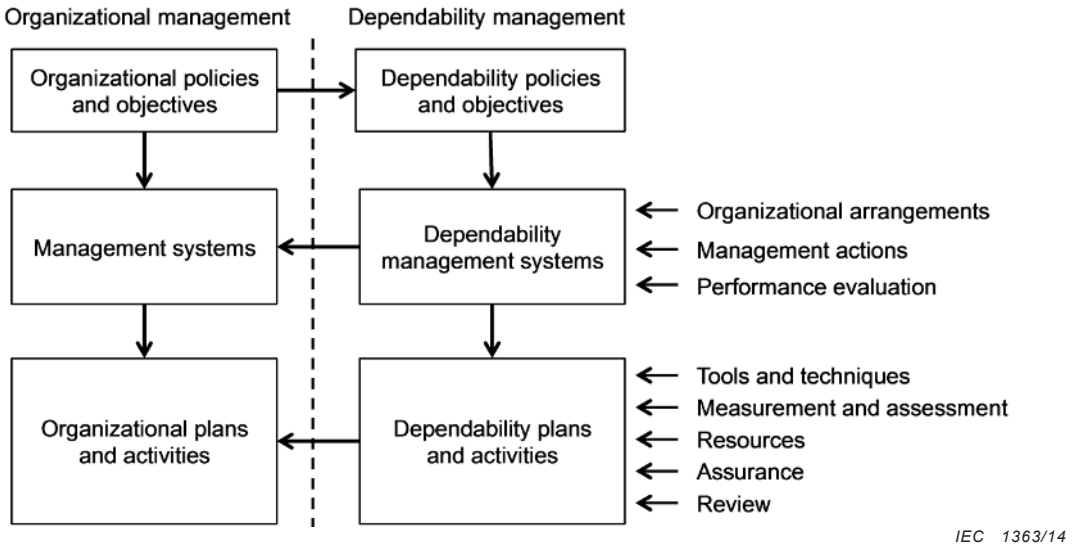


Figure 2 – Dependability management systems

A dependability management system consists of three elements:

- organizational arrangements to implement dependability policies and objectives;
- dependability activities that are implemented in the dependability programme;
- performance evaluation arrangements.

5.2 Organizational arrangements

Establishing organizational arrangements focuses on the management structure needed to facilitate effective implementation of the dependability policies. Dependability management should be integrated by the management systems of an organization in order to enable effective decision-making and influence technical direction. In particular, dependability engineering should be closely integrated into engineering projects for design and process improvements. Annex A describes the incorporation of dependability activities in the organizational operations, strategies and processes to achieve long-term goals and on-going project objectives.

Dependability policies and objectives need to be aligned with organizational policies and objectives and those of stakeholders comprising both technical and business perspectives. Organizational arrangements for managing dependability should take into consideration the organization's context, its objectives and the strategies to achieve them, and its risks and opportunities.

Dependability management systems do not always require a complex organizational infrastructure and reporting hierarchy to be effective. Dependability activities either can be managed by a separate organizational unit with close coordination, be fully integrated into other relevant areas, or be a mixture of the two approaches. The alignment of organizational structure, responsibilities, procedures, activities, resources and information is critical to efficient and effective direction and control of dependability. There should be dependability management involvement in planning, review, auditing, verification and validation of on-going project activities.

Where functions such as design, maintenance and logistic support are outsourced, the responsibility for dependability aspects of outsourcing should be specified, monitored and controlled.

One of the challenges with managing dependability over the life cycle is that often more than one organization is involved. Over the life cycle, certain responsibilities may need to be

passed from one organization to another. Since organizational styles and procedures vary, the management of dependability needs to adapt to different situations.

A means to manage and control dependability data and information should be established as a part of the organization'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.

5.3 Management actions

Effective dependability management helps to ensure that dependability requirements are met in conjunction with functional and non-functional requirements.

Management actions should address the following:

- provide leadership through management commitment, policy direction and establishment of roles, responsibilities and authority;
- provide operational planning and control to achieve dependability objectives and manage risks;
- involve stakeholders by identifying dependability requirements and issues, communication of dependability programme status, conflict resolution and trade-offs, and securing and maintaining agreements and accountability;
- coordinate different organizational functions that are involved in dependability activities with assigned dependability responsibility for the coordination of management and technical effort;
- manage risks to dependability objectives and targets;
- provide and manage resources including acquisition of capital equipment, staff training and deployment, outsourcing and sub-contracting of dependability technical work;
- manage the technical activities needed during an item's life cycle to achieve dependability;
- manage knowledge and information through the capture and dissemination of relevant dependability data and knowledge, including maintenance of a dependability performance data base;
- undertake performance evaluations through monitoring, measuring analysis and evaluation, audit and assurance and management review;
- ensure sustained improvement via the planning and control of enhancement activities and appropriate reviews of progress.

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

5.4 Performance evaluation

Performance of organizational arrangements and processes is evaluated to assure relevant stakeholders that dependability management activities are being carried out well and will achieve the required dependability performance.

The organization should define performance indicators and targets for the dependability management system and monitor measure, analyse and improve performance against these indicators and targets.

This could involve

- evaluating the operation and effectiveness of dependability processes, activities and procedures,
- evaluating whether the organization's dependability policies and objectives are being met,

- reviewing the suitability of the dependability policies objectives and programme,
- assessing the dependability performance of items, and
- monitoring agreements and responsibilities.

6 Application of dependability management

6.1 Tailoring a dependability programme

The basic elements of a dependability programme are as follows:

- dependability plans, which define the activities, techniques and resources required to achieve dependability of items;
- methods for measurement and assessment;
- assurance and review (see Figure 2).

Management accountable for the resulting dependability of an item should tailor these elements to fulfil the dependability objectives for that specific situation or project. Tailoring applies to any stage of the life cycle but important tailoring occurs during the initial design-related parts of the life cycle. It might 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 involves the following:

- identification of the organizational context, including policy and infrastructure;
- consideration of regulatory requirements or standards;
- identification of item related characteristics such as its features and functions, past history of similar items, their intended end use and anticipated application environments;
- analysis of objectives and requirements;
- determination of the specific life cycle stages or phases that are applicable;
- assessing risks;
- selection of dependability activities relevant to the specific life cycle stages or phases identified;
- selection of tools and technical activities needed to achieve dependability;
- selection of techniques for measurement and assessment;
- definition of the capability and resources needed and actually available for implementation;
- prioritization and allocation of resources;
- planning reviews and assurance;
- documentation of the rationale in formalizing the tailoring decisions as part of the organizational or project plan.

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 organization’s dependability activities are used within project processes,
- which mandatory and legal requirements need to be satisfied,
- which options may be exercised as well as the criteria for selecting from these options, and
- how to make decisions about which dependability procedures should be performed.

Tailoring needs to take into account the nature of the organization and the dependability tasks that need to be managed. The organization could vary from a technical consultancy to a multinational conglomerate requiring appropriate dependability management of diverse disciplines, organization and specialization. Management approaches often seek technology transfer, knowledge infusion, or expert consultancy to deal with critical short-term technical gaps.

The tailoring of dependability activities includes consideration of the organization's technical and administrative processes with their constraints and influencing factors, which include, but are not limited to the following:

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

The outcome of tailoring activities form the basis of a dependability plan of activities and resources for that particular project. The depth and detail of the plan should enable measurement for management tracking and costing purposes. Tailored plans should, along with other plans such as those relating to 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 can incur a trade-off of predicted product dependability against project timing and cost.

The provision of flexibility through tailoring should be balanced with the need to ensure appropriate consistency in the dependability activities across the organization. Flexibility is needed to address contextual variables such as the nature of the customer, cost, schedule, quality trade-offs, and technical difficulty of the work as well as the depth of experience of the people implementing the process. Tailoring criteria can allow for use of a standard process with no tailoring or an approach where only exceptions are noted from a standard process.

6.2 Analysis of objectives and requirements

Requirements are defined to satisfy the needs and objectives of stakeholders. Requirements can be divided into two interrelated groups, functional and non-functional requirements, both of which could include dependability requirements (see Figure 1). Annex C describes how dependability requirements can be defined.

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

When there is a contract between a customer and a provider, they need to agree on the way dependability is to be measured and how it will be decided that dependability targets have been achieved.

6.3 Risk management

Risks should be identified considering both potential failures to achieve requirements and opportunities for enhanced performance. Risks to dependability and to functional and non-functional objectives such as those concerning safety or the environment need to be considered and trade-offs could be required.

Failure to meet requirements and objectives can arise as a result of

- failures of or within an item, which can be identified by reference to past data and methods including root cause analysis of failures or by procedures such as FTA or FMEA,
- failure in support for the item such as in maintenance or maintenance support, and
- changes in requirements, assumptions and circumstances from outside the dependability system and sometimes outside the organization.

Where practicable and cost beneficial, adverse consequences should be prevented or reduced. Arrangements should be made to monitor external circumstances critical to dependability to obtain early warning of changes. The need for an item to be able to recover from and adapt to risks should be taken into account in defining requirements and the activities and plans to achieve them.

6.4 Implementation of dependability activities through the life cycle

Dependability activities occur throughout the life cycle of an item and 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 between life cycle stages often entail different technical resources, diverse enabling systems and support criteria.

The 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 programmes or projects for maximum effectiveness.

Annex B maps dependability activities to a generic life cycle; it should be recognized that life cycle stages can be simpler or more complex, depending on specific circumstances.

6.5 Selection of dependability tools and technical activities

There is a broad range of technical activities and tools to facilitate achievement of dependability management objectives such as reliability analysis and testing, maintenance and logistic support management, customer care services, failure analysis and corrective action systems. Dependability tools vary with the stage of the life cycle.

For example, at the design and development stage, techniques such as HAZOP, FMEA or FTA can be applied. Those techniques aim to identify and prevent faults, failures or undesired events before they have been observed in real operation.

During implementation and utilization, reliability improvement by a growth programme should be part of an overall reliability activity in the development of an item, particularly for a design that uses novel or unproven techniques, components or a substantial content of software. In such a case, the programme can expose, over a period of time, many types of weaknesses having design-related causes. Reliability growth is achieved by learning about the deficiencies of the design through testing and taking action to eliminate or minimize the effect of these deficiencies. Various statistical models can be used to develop a planned growth curve that sets realistic interim reliability goals to be attained during the testing and indicates that sufficient progress is being made in order to reach the final goal or requirement.

Root cause analysis is another dependability tool that consists of any systematic process to identify the causes of a fault, failure or undesired event that have been observed in operation or during testing with the aim of preventing similar or related failures from occurring. It is

performed with the understanding that failures are best resolved by eliminating the primary or root causes rather than addressing the immediately obvious symptom. It is typically applied in response to a repeated failure or a failure with significant consequences.

Annex D presents the 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 [2] to facilitate dependability applications.

6.6 Resources

The resources to achieve dependability of an item include

- someone to take responsibility for the dependability of an item either as a prime responsibility or possibly as part of another role,
- expertise to carry out the appropriate technical activities and analyses,
- an information management system such as a dependability knowledge database (either stand-alone or part of a logistic support system), and
- appropriate dependability analysis software.

The resources necessary can vary with the stage of the life cycle. For example, the design and development stage requires dependability design expertise and the use of dependability analysis techniques, which often require software programs and dependability data. The realization stage can involve resources for detailed testing. During utilization of the item, resources might be needed for data gathering and assessment and performance of maintenance and support activities.

6.7 Measurement and assessment

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;
- documenting the measurement findings for record retention, quality audits and objective evidence.

Dependability is assessed in different ways according to the stage in the life cycle:

- forecasted at the design stage by using probabilistic assessment and modelling methods;
- estimated at the realization stage by, for example, accelerated reliability and durability testing;
- measured and analysed at the utilization stage using statistical and other methods.

The dependability characteristic that is measured depends on whether a user or organizational perspective is taken and on the applicable performance requirements. For example, for a transportation service, the user (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). From an organizational perspective, dependability can also be assessed by means

of an effectiveness measure such as customer satisfaction, reliability of the service and maintenance cost.

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

Examples of qualitative methods are as follows:

- An assessment by an expert providing explanations on the item and providing a score (such as 5 ‘stars’). In certain cases, the attributes are weighted to incorporate levels of importance before an overall score is established. By comparing various scores from different experts, an objective assessment can be achieved. Making judgments based on the scores of a single expert should be treated with caution.
- An assessment derived from the general public providing an individual score and associated justifications for a particular item. These scores are accumulated within a database to establish an overall ranking for the item compared with other similar items.
- In these cases, the method of ranking needs to be understood as well as the potential biases of the individuals providing the score before the accuracy of the ranking can be acknowledged.

A quantitative value of dependability performance is derived from observed or estimated data. 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 during testing, 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 might need to 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.

Dependability parameters of an item should be predicted, forecast or measured under defined stressing conditions such as the exposure to various environmental conditions that will occur during utilization. Some typical natural environment stressing conditions are storage and operating temperatures, humidity and solar loading. Cultural, organizational or political rules and human involvement can also have dependability impacts.

6.8 Assurance of dependability

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

a) Dependability assurance is demonstrated by actual utilization in an application environment over a scheduled time period. This could involve a formal demonstration or actual performance during the warranty or operating period.
b) Dependability is inferred by applying statistical methods to data of the dependability of constituent items.
c) Evidence of correct implementation of required dependability activities and tools is provided.

A means of achieving progressive assurance that dependability requirements are being met, or will be satisfied throughout the life cycle of the item, is by use of a dependability case. 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 part of the evaluation.

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

Where possible, existing performance monitoring systems should be used to generate the information needed for improving dependability activities and outcomes.

Typical examples include

- a failure recording, analysis and corrective action system (FRACAS),
- 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.

6.9 Reviewing dependability outcomes and activities

Dependability outcomes and activities should be reviewed throughout the life cycle. The purpose of dependability reviews is to ensure that specific objectives from both technical and business perspectives are being met throughout the life cycle. The reviews provide feedback on dependability deficiencies and deviations at one life cycle stage for correction and mitigation at other stages, as well as improving the way dependability is managed. The reviews should consider both activities and outcomes and should set a course of action from a technical perspective to achieve objectives and manage risks, for example, at critical design points to prevent the propagation of errors and inadequate design decisions.

Dependability reviews are conducted in conjunction with other management reviews with broader scope to address dependability management issues such as those associated with the organization’s policies, administration, operation or customer services. For example, project management reviews should be enhanced to include dependability aspects.

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

Reviews cover a broad range of review activities over the life cycle of an item. Typical reviews conducted at various levels of management which should incorporate dependability components could include:

- operations review to determine the health and operational status of an organization, 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 application of new technology, 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 the environment of application and service support needs, and final design approval prior to design release to production;
- component application review to check operating conditions of components and COTS items against data sheets and test results and for special requirements of use, handling and assembly processes;
- production review to determine resource requirements and delivery schedules, production capacity and throughput, outsourcing and subcontracting of production work, tooling, assembly fabrication, material control and testing activities;
- risk review to determine whether risks have changed and whether the risk management process is effective;
- service review to determine customers' 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;
- verification and validation review to ensure proper verification and validation processes have been carried out;
- product release review releasing the product for delivery and/or customer acceptance;
- regulation review to determine if applicable health, safety and environmental rules have been identified and are properly implemented.

Dependability components in those reviews have to work together as a whole. Each of those reviews typically involves several life cycle stages and activities and feedback from one review can trigger activities affecting other reviews.

All reviews are part of the assurance process. The reviews of dependability ensure that all critical issues have been assessed and resolved. The review records could be used as objective evidence to support the dependability assurance process in a wider review of assurance processes.

Annex A
(informative)

Organizational arrangements of a dependability management system

A.1 Organizational structures

In order to achieve their objectives effectively, organizations 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 organizations, dependability is a very important requirement that needs to be met and the organizational structure should accommodate these specific requirements.

Some organizations 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. In other cases, an organization can exist for a longer time period. In both situations, dependability requirements will need to be accommodated in the organizational structure.

In organizations where business or technology is fast-moving, new organizational 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 organizations 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 organizations have also engaged in matrix management and participative organizational structures to retain expertise for strategic deployment. Organizations can then expand beyond standard corporate management and can include collaborations of government, industry and academic institutions or complex systems where no one stakeholder fully understands the system.

A.2 Organization of dependability activities

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

- Dependability activities are fully integrated into the organizational structure with dependability resources embedded into an organizational entity, for example, where every employee is responsible for the dependability aspects of his or her activities. Often one or more persons are assigned as facilitators for such activities.
- Dependability activities are sufficiently time-consuming and important that one or more organizational entities will be needed to complete dependability activities as would be appropriate for the design, construction and commissioning of a major facility. These entities will still function in close coordination with other entities.
- For a large organization with multiple product lines or many large facilities to operate, it can be worthwhile to set up a major organizational entity to serve the overall needs of the organization in an efficient manner. This can eliminate duplication of effort and ensure consistency of dependability activities while at the same time enabling the highest level of expertise to be applied. In some cases, a separate dependability organization is required

by regulatory authorities, e.g. type approval within the fields of telecommunication, medical equipment and aerospace.

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

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

- defining a single overall responsibility for meeting dependability requirements and coordinating shared responsibilities among the various organizational entities that are 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, and
- 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 B
(informative)

Activities of a dependability management system

B.1 Dependability activities within the life cycle

A variety of dependability activities 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 activities.

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, human aspects the regulatory requirements (such as traceability, safety, environment, sustainability, retirement and waste disposal) and other constraints. From this, functional and non-functional requirements and the preliminary dependability requirements can be defined and analysed and feasible design or purchasing solutions identified from broad technical specifications. Potential needs for trade-off such as between safety and dependability should be identified at this stage. Modelling 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. Selection of design options is based on the best practical engineering approaches to achieve requirements and manage risks within the constraints imposed.

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 the realization of item functions. This is transcribed into an appropriate design and development effort including designing system architecture, engineering modelling and prototype construction and testing. Interfaces between system and subsystem elements are identified and a systematic evaluation of the integrated item functions and its interactions with external environments is conducted to validate the final configuration. Risks associated with the selected design are assessed in more detail and treatments specified. Planning for supportability 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 implements 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 development, tooling, manufacturing, packaging and supply 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 for 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 a 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 can 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 might 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 upgrades or additions, maintenance improvements, simplifying procedures to improve operational efficiency or obsolescence management. At this stage relevant modeling and probabilistic approaches can be used to assess the impact of the possible enhancements and select the best solutions. Risk assessment during the enhancement stage often looks at cost versus 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 from the conceptual stage. For complex items, a strategy for decommissioning could be established to formalize planning and implementation of the decommissioning process to meet regulatory requirements. For other items, there could be regulatory rules concerning their return and reuse or disposal.

Dependability activities are often considered in the context of the life cycle as shown in Figure B.1.

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

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

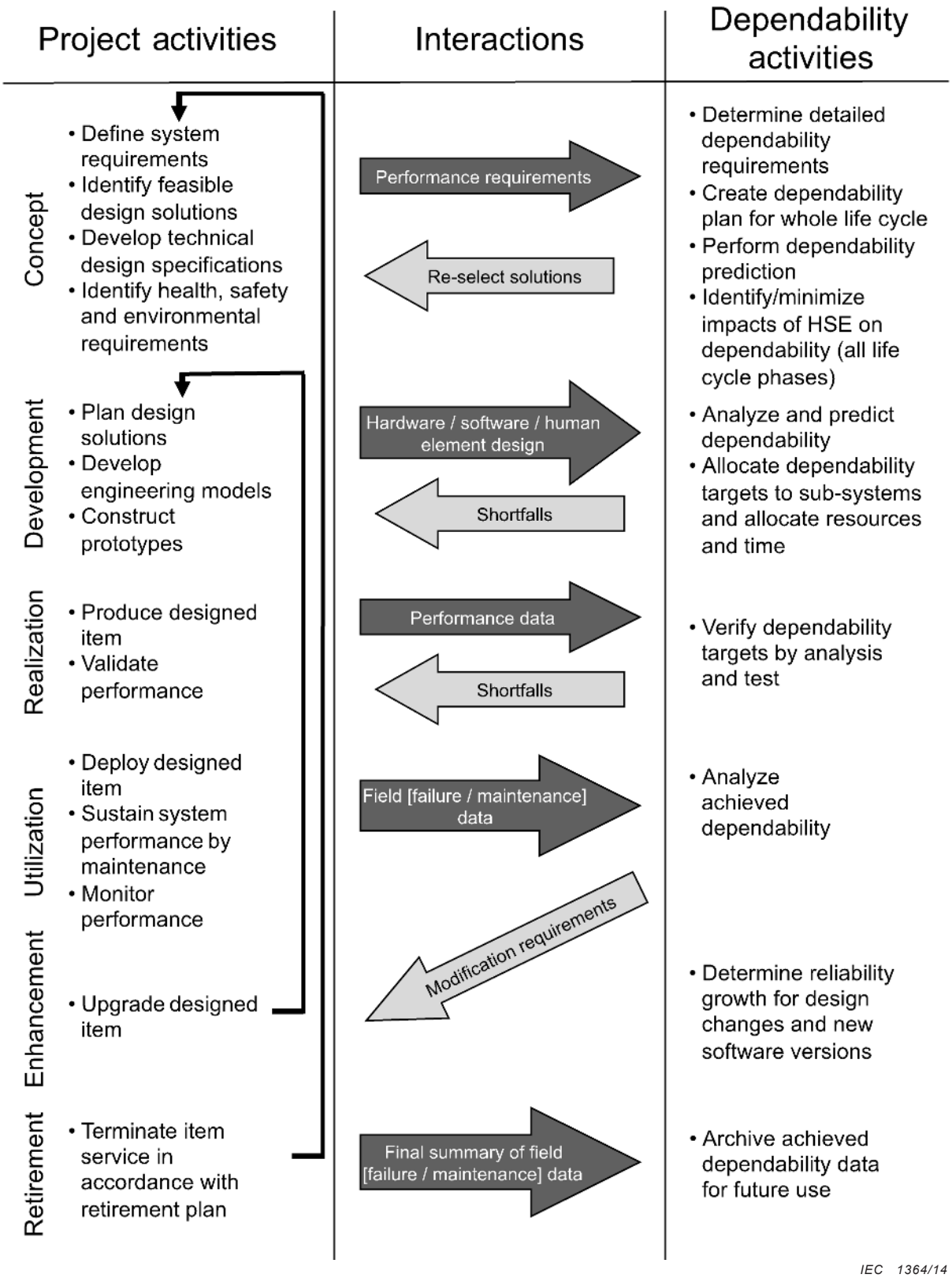


Figure B.1 – Dependability activities and the life cycle

B.2 Dependability life cycle activities

The following tables provide typical examples of activities with an impact on dependability objectives that could be part of a life cycle. This list is not exhaustive and should be modified or tailored to meet specific requirements.

Table B.1 – Activities during the concept stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Define item requirements	a. Identify market needs or other opportunities	• 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 policies and incentives for implementation	• 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 programme portfolios • Plan achievement targets • Establish project tailoring criteria • Document policies and mission statement • Determine development tools and procedures
2. Analyse item performance requirements	a. Identify technical approaches and feasibility for item realization	• 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 organization's capability to undertake the work • Identify risks • Evaluate trade-offs which can be required between desired functionality 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	• Determine feasibility of supply-chain and joint venture collaboration • Determine outsourcing requirements

Dependability objectives	Dependability strategies	Activities with impact on dependability
3. Establish high level design criteria	a. Identify appropriate logical architectural design options	• 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	• Formalize the design process and how trade-offs will be handled • Identify design composition of hardware/software elements for each function • 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 • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability
	c. Document item specifications	• Incorporate dependability requirements in item specifications

Table B.2 – Activities during development stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Design and develop the item	a. Initiate item design	• Establish item dependability programme • Establish quality assurance programme • 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 programmes • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability
	b. Initiate full scale item development	• 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 programme • Establish dependability acceptance criteria and reliability growth programmes • Establish item maintenance and logistics support programme • Conduct risk assessments • Monitor and collaborate with material outsourcing and contracting external development efforts • Develop spares provisioning programme • Define warranty conditions • Establish training programmes

Table B.3 – Activities during the realization stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item or module realization	a. Initiate production or acquisition of hardware assemblies and functions	• Implement item dependability programme • Implement quality assurance programme • 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 programmes
	b. Initiate software module functions and item development	• Implement software reliability assurance programme • Implement software test and diagnostic programme • Implement software module qualification and evaluation plan for acceptance
2. Item implementation	a. Item integration	• Execute integration plan • Coordinate outsourcing and support programmes • 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	• Implement verification/validation plan • Document verification/validation test results • Conduct failure analysis and recommend preventive/corrective actions for improvement
	c. Item installation and acceptance	• 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 • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability • For consumer products, release to mass production, distribution and sale

Table B.4 – Activities during the utilization stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item operation and maintenance	a. Implement operation strategy	• Monitor item performance • Implement reliability growth programme • Implement field data collection system for information about in-service dependability • Conduct customer satisfaction survey • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability
	b. Implement supportability strategy	• Provide customer care service • Monitor item maintenance efforts • Analyse failure trends and maintenance service records • Recommend design or procedural changes for continual improvement • Determine quality of service and provide customer value

Table B.5 – Activities during the enhancement stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item enhancement	a. Implement item enhancement strategy	• Identify new feature and enhancement requirements • Evaluate the need for change and resulting benefits • Conduct risk and value assessments • Analyse the impact on health, safety and environmental requirements • Implement enhancement efforts • Evaluate impact on dependability-related performance like stability and robustness due to changes with added new features • Conduct customer satisfaction survey resulting from change reactions

Table B.6 – Activities during the retirement stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item retirement	a. Implement item retirement strategy	• Execute item retirement/decommissioning plan • Implement reuse of components, data and materials from disposed items • Ensure that health, safety and environmental requirements are met • 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 C
(informative)

Defining requirements of an item

C.1 Requirements from an application perspective

The dependability requirements together with the functional and non-functional requirements define the performance requirements of the item.

The dependability requirements are an integral part of the overall requirements and relate to how the functional and non-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.

There is a wide variance in how performance requirements are established and implemented for different applications.

The 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 dependability requirements take 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/effectiveness 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.

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

Performance 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 power output could require shorter maintenance intervals that might be unacceptable from an operational point of view. Cost constraints will impact both performance and dependability requirements.

The following two examples serve to illustrate how performance and dependability requirements can be defined for two scenarios and the methods that can be used as part of

the dependability programme for this item: in the first case, requirements are defined by both provider and user and, in the second case requirements are defined mainly by the provider based on their understanding of user expectations but without specific user input.

C.2 Examples of performance requirements that include dependability

C.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, safely and with minimum environmental impact. The constraints in terms of conditions of use and operational environment are tropical climate with ambient temperatures normally below 40 °C, but with high humidity. Required maintenance will be determined by a risk-based approach such as RCM 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. Non-functional requirements consist of extensive safety and environmental features to minimize potential impact to employees and the public.

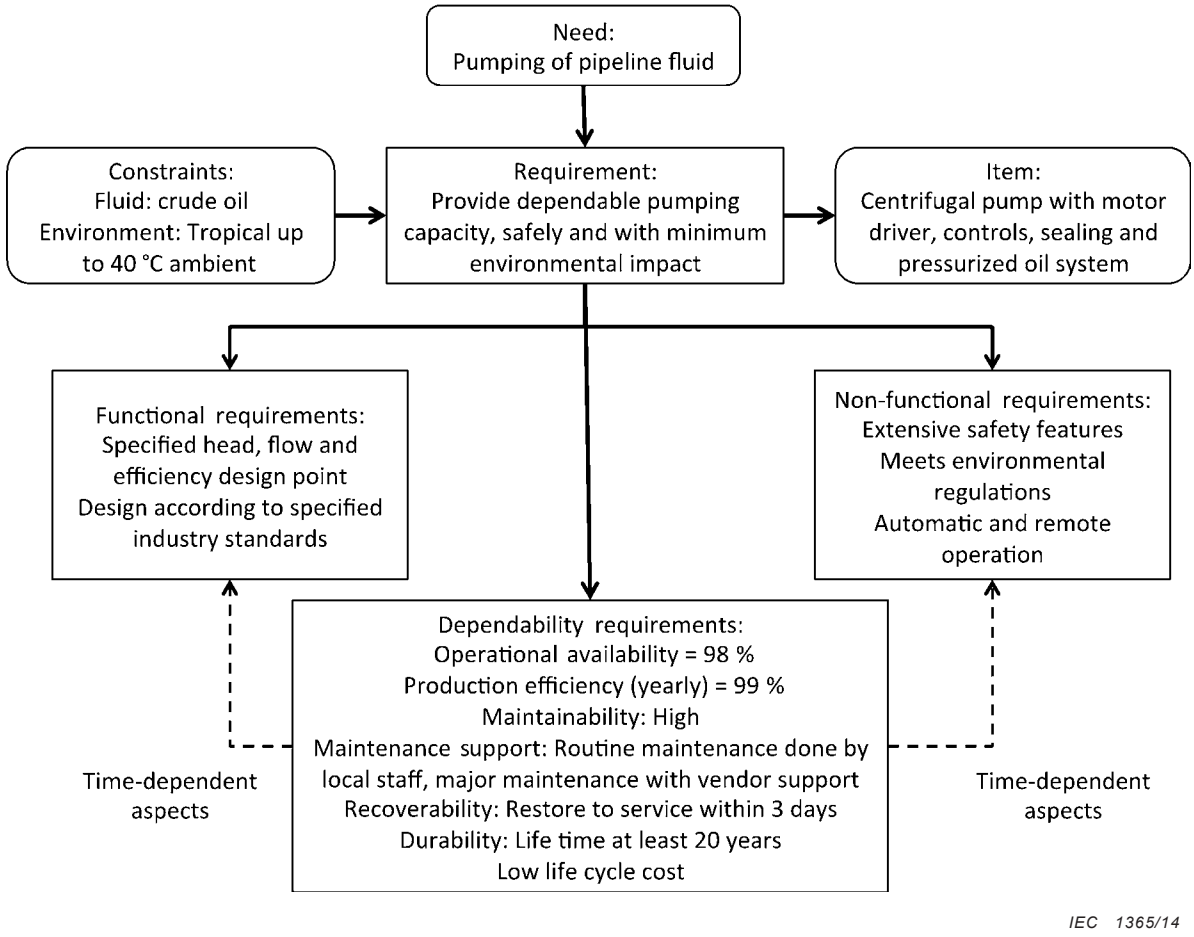
The pump unit has a software-based control system supported by instrumentation and remote control from a centralized facility. To minimize environmental impact, the mechanical seals use a nitrogen buffer fluid. Safety protection is built into the control system with fire monitoring and protection devices. 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 production efficiency (i.e. the expected production of the system is an average over 1 year of the rated design flow) 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 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, which will depend on the selection of an acceptable support solution.

The relationship between the functional, non-functional and dependability requirements is illustrated in Figure C.1.



NOTE This is only an illustrative example to clarify the interrelationships between these concepts.

Figure C.1 – Example showing the relationship between the functional, non-functional and dependability requirements for a motor-driven pipeline pump

The decision-making process for performance 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 costs are estimated but sometimes do not include all life cycle costs. The lifetime of components can be estimated using Weibull analysis. Costs of preventive maintenance compared with maintenance on failure can be estimated. Often the cost of lost production due to an unscheduled outage is much larger than the cost of preventive maintenance. Users that acquire a complete understanding of dependability requirements are normally better able to manage the operation and maintenance phase of the life cycle.

C.2.2 Requirements determined by provider only

Acquiring a family car is a common decision process. The cost of owning and operating it is a major target objective but other performance 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 is not always based on a rational evaluation of performance 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 and non-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 crashworthiness,
- construction 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,
- supportability,
- location and accessibility of maintenance support services, and
- durability.

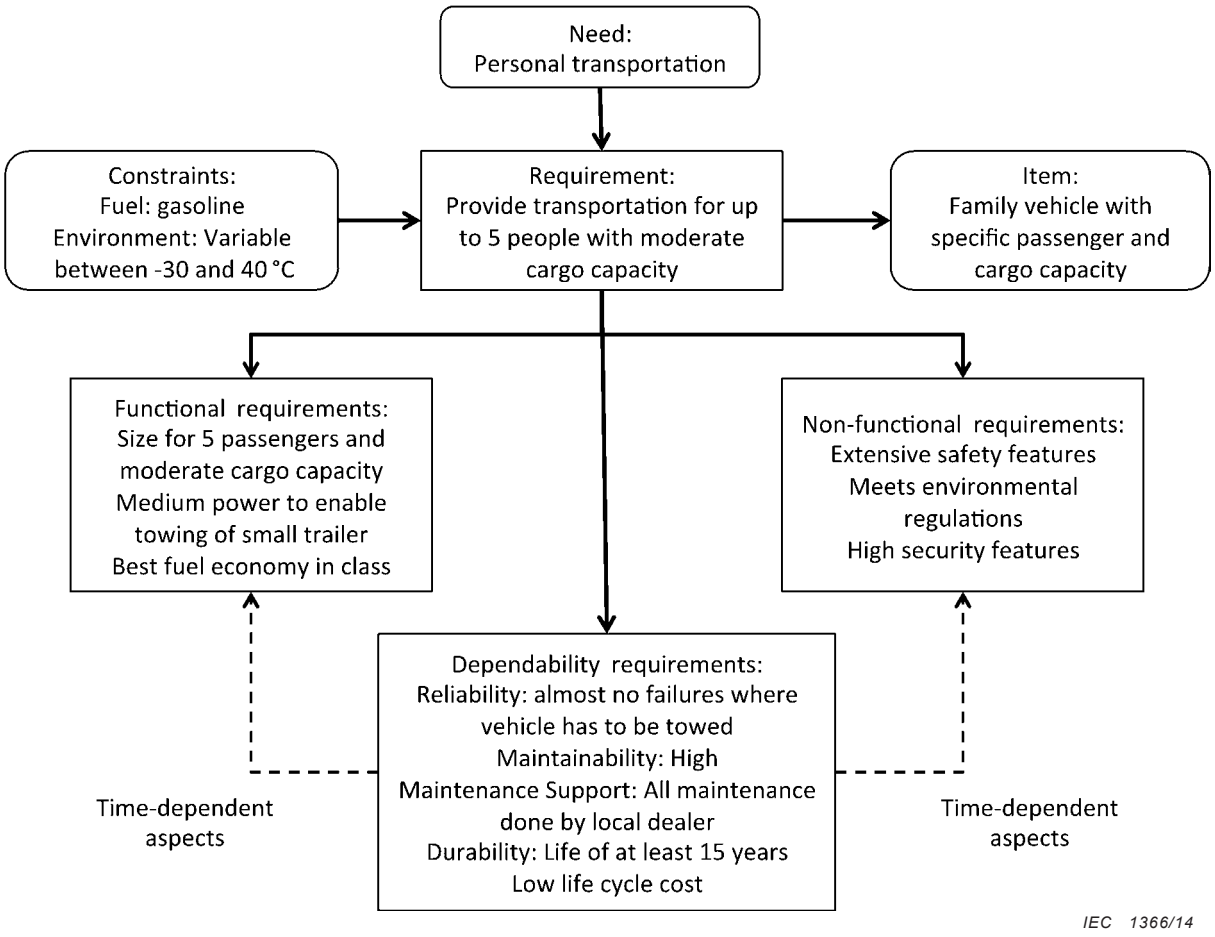
These features represent a set of performance requirements for the car under consideration by the user. There are interrelationships between the performance and dependability requirements, for example, maintainability will clearly influence maintenance costs and manufacturing quality will be related 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 fulfil the performance requirements to various degrees but none completely fulfil 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 score each option according to how it achieves each requirement. The final 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 and quality function deployment to guide their selection of performance requirements and expectations for the target user market at which they are aiming.

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



NOTE This is only an illustrative example to clarify the interrelationships between these concepts.

Figure C.2 – Example showing the relationship between the functional, non-functional and dependability requirements for a family car

Annex D
(informative)

Structure of dependability standards

D.1 Structure

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

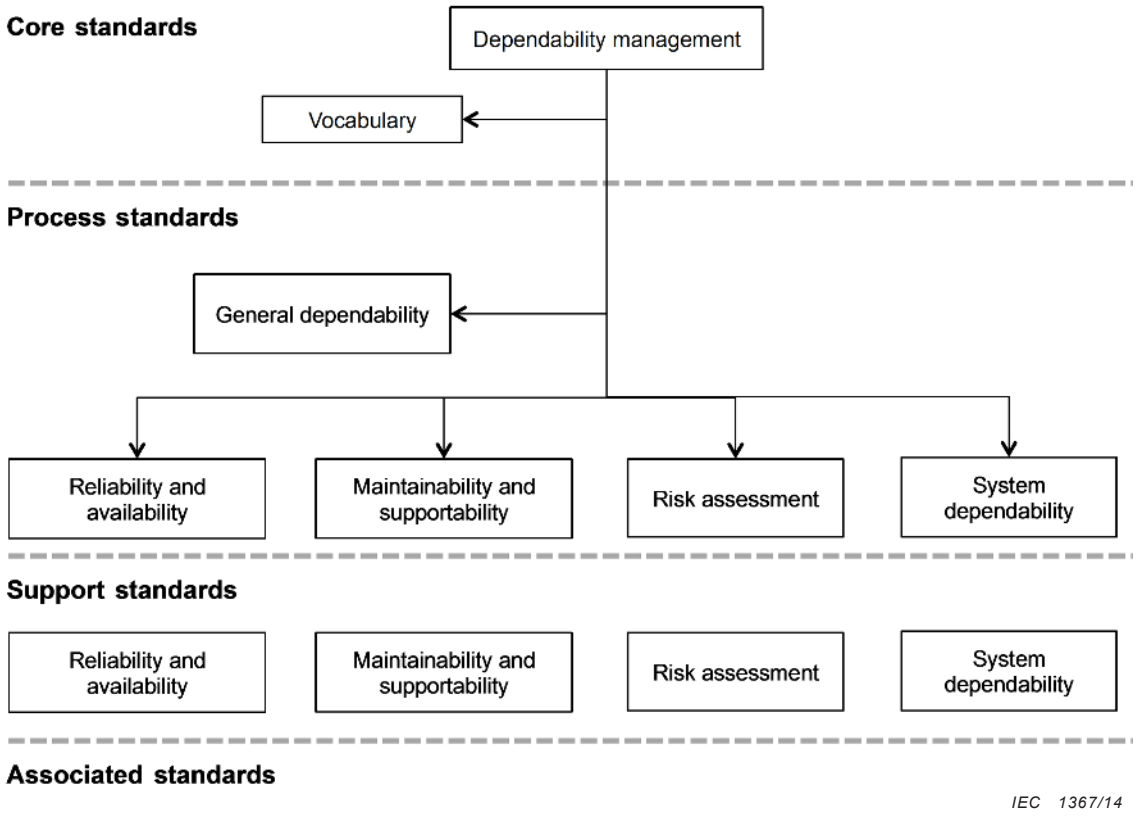


Figure D.1 – Framework for dependability standards

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

D.2 Core standards

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.

D.3 Process standards

Process standards focus on the application processes of the major aspects of dependability to facilitate implementation of dependability for projects and achievement of other organizational objectives.

Process standards can be of a general nature, be associated with the dependability characteristics or relate to risk assessment and system aspects of dependability. Their purpose is to assist with the processes associated with implementation of dependability methods and techniques.

General dependability covers subjects such as life cycle costing and dependability specifications.

D.4 Support standards

Support standards are focused primarily on the specific methods and techniques for the process groupings.

Standards on reliability and availability deal with modeling and analysis, statistical analysis methods, reliability testing and screening and reliability growth.

Maintainability standards cover maintainability studies, testability and verification while supportability is concerned with aspects related to maintenance and maintenance management, reliability centered maintenance, maintenance support agreements and integrated logistic support.

Risk assessment standards provide support for tools that analyse risk such as FMEA and HAZOP as well as project risk.

System aspects consist of guidance for engineering and specification of dependability related to systems and networks. It also includes human and software reliability.

D.5 Associated standards

Associated standards include those standards which are not generated by IEC/TC 56, but are currently included within the list of standards on the TC 56 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/TC 56 website [2].

Annex E
(informative)

Checklist for review of dependability

E.1 Introductory remark

The following checklists are examples of the dependability related issues that could be necessary for review by management to ensure that dependability objectives are being met. The lists should be tailored for individual circumstances with the agreement of 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 activities are identified.

f) The information on the proposed new system is adequate to initiate requirements analysis.

g) Stakeholder input into requirements and design to satisfy requirements has been obtained.

h) Risks that need to be taken into account in design have been identified.

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.

f) Risks of different options are assessed and taken into account in design selection.

g) Requirements for health, safety and the environment have been identified.

E.2.3 High-level architectural design

a) The architectural design criteria, possible item configuration and options are identified.

b) The technology selection for the 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.

l) Risks to performance associated with different designs are evaluated.

E.3 Development

E.3.1 Item design

a) The dependability plan for the 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) Component application has been reviewed with suppliers.

g) The suppliers' dependability programmes have been established.

h) The item design is verified and support programmes 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 part of the 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 programmes have been established.

e) Design has been modified and reliability estimated.

f) Revision control of development documentation has been implemented.

g) Risks to functional and non-functional objectives and to dependability requirements have been assessed and treatment plans specified.

h) The item maintenance and logistics support programmes are established.

i) The outsourcing programmes are established.

j) The spares provisioning programme is developed.

k) The training programmes are established.

l) The warranty criteria for system service support are established.

m) The item is fully developed and ready for production and construction.

n) Software specifications and flow charts have been finished and approved.

o) The development of software module functions and subsystems has been initiated.

p) Requirements for health, safety and the environment have been analysed and the impact on dependability has been minimised.

E.4 Realization

E.4.1 Item realization

a) The production of hardware assemblies and functions has been initiated.

b) The suppliers' dependability programmes 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 programmes 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) Actions specified to treat risks have been implemented.

c) The item verification and validation plans are implemented.

d) The item qualification and acceptance plans are implemented.

e) The item installation plan is implemented.

f) The warranty plan is implemented.

g) The training programmes for system operation and customer care services are initiated.

h) The required design changes for fulfilling the dependability requirements have been implemented and verified.

i) The item is ready for release to operation.

E.5 Utilization

a) Maintenance and support programmes are implemented.

b) Risks are reassessed in the light of actual conditions.

c) The item performance and service maintenance are monitored and controlled.

d) The training programmes for operators and maintainers are implemented.

e) The field data collection system is implemented.

f) The design change and configuration controls are implemented.

g) The customer satisfaction survey is implemented.

h) The item performance data are analysed for continual improvement.

i) 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 consequences, in particular with regards to health, safety and environmental requirements, and value of enhancement are analysed.

c) The enhancement programmes and improvement time frame are determined.

d) The decision for enhancement programmes is executed.

e) The customer satisfaction survey resulting from the enhancement programmes is monitored to determine enhancement value.

E.7 Retirement

a) The decommissioning and disposal strategy is planned and initiated.

b) The impact of service termination 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 the old service and the use of the new service is monitored.

e) Required data has been transferred.

Bibliography

[1] IEC 60050-191:2014, *International Electrotechnical Vocabulary – Part 191: Dependability*

[2] IEC/TC 56 website, http://tc56.iec.ch

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™