

Australian/New Zealand Standard™

Dependability management

Part 1: Guidance for management and application



AS/NZS IEC 60300.1:2015

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 12 December 2014 and on behalf of the Council of Standards New Zealand on 12 December 2014.

This Standard was published on 23 January 2015.

The following are represented on Committee QR-005:

Asset Management Council
Australian Industry Group
Australian Organisation for Quality
Department of Defence (Australian Government)
Engineers Australia
Independent Transport Safety and Reliability Regulator
Institution of Professional Engineers New Zealand
New Zealand Institute of Safety Management
New Zealand Society for Risk Management
Risk Management Institution of Australasia
The Institute of Chemical Engineers
University of New South Wales
University of Wollongong

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.saiglobal.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR AS/NZS IEC 60300.1:2014.

Australian/New Zealand Standard™

Dependability management

Part 1: Guidance for management and application

Originated in Australia as AS 3900.4—1994.
Previous edition AS IEC 60300.1—2004.
Jointly revised and designated as AS/NZS IEC 60300.1:2015.

COPYRIGHT

© Standards Australia Limited/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Australia) or the Copyright Act 1994 (New Zealand).

Jointly published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001 and by Standards New Zealand, Private Bag 2439, Wellington 6140.

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee QR-005, Dependability to supersede AS IEC 60300.1—2004, *Dependability management, Part 1: Dependability management systems*.

The objective of this Standard is to provide guidance on dependability management of products, systems, processes or services involving hardware, software and human aspects or any integrated combinations of these elements.

This Standard is identical with, and has been reproduced from, IEC 60300-1 Ed.3.0 (2014), *Dependability management, Part 1: Guidance for management and application*.

As this Standard is reproduced from an International Standard, the following applies:

- (a) In the source text ‘this part of IEC 60300’ should read ‘this Australian/New Zealand Standard’.
- (b) A full point substitutes for a comma when referring to a decimal marker.

The term ‘informative’ has been used in this Standard to define the application of the annex to which it applies. An ‘informative’ annex is only for information and guidance.

CONTENTS

1	Scope	7
2	Normative references	7
3	Terms, definitions and abbreviations	7
3.1	Terms and definitions	7
3.2	Abbreviations	10
4	Dependability management	10
4.1	Understanding dependability	10
4.2	Benefits of dependability management	12
4.3	Challenges of managing dependability	12
5	System for managing dependability	12
5.1	Overview	12
5.2	Organizational arrangements	13
5.3	Management actions	14
5.4	Performance evaluation	14
6	Application of dependability management	15
6.1	Tailoring a dependability programme	15
6.2	Analysis of objectives and requirements	16
6.3	Risk management	17
6.4	Implementation of dependability activities through the life cycle	17
6.5	Selection of dependability tools and technical activities	17
6.6	Resources	18
6.7	Measurement and assessment	18
6.8	Assurance of dependability	19
6.9	Reviewing dependability outcomes and activities	20
	Annex A (informative) Organizational arrangements of a dependability management system	22
A.1	Organizational structures	22
A.2	Organization of dependability activities	22
	Annex B (informative) Activities of a dependability management system	24
B.1	Dependability activities within the life cycle	24
B.2	Dependability life cycle activities	27
	Annex C (informative) Defining requirements of an item	32
C.1	Requirements from an application perspective	32
C.2	Examples of performance requirements that include dependability	33
C.2.1	Requirements determined by both provider and user	33
C.2.2	Requirements determined by provider only	34
	Annex D (informative) Structure of dependability standards	37
D.1	Structure	37
D.2	Core standards	37
D.3	Process standards	37
D.4	Support standards	38
D.5	Associated standards	38

Annex E (informative) Checklist for review of dependability	39
E.1 Introductory remark.....	39
E.2 Concept	39
E.2.1 Requirements definition	39
E.2.2 Requirements analysis.....	39
E.2.3 High-level architectural design.....	39
E.3 Development.....	40
E.3.1 Item design.....	40
E.3.2 Full-scale system development	40
E.4 Realization.....	41
E.4.1 Item realization	41
E.4.2 Item implementation	41
E.5 Utilization.....	41
E.6 Enhancement.....	41
E.7 Retirement	42
Bibliography.....	43

Figure 1 – Relationship of dependability to the needs and requirements of an item (product, system, process or service).....	11
Figure 2 – Dependability management systems	13
Figure B.1 – Dependability activities and the life cycle	26
Figure C.1 – Example showing the relationship between the functional, non-functional and dependability requirements for a motor-driven pipeline pump	34
Figure C.2 – Example showing the relationship between the functional, non-functional and dependability requirements for a family car	36
Figure D.1 – Framework for dependability standards	37
Table B.1 – Activities during the concept stage	27
Table B.2 – Activities during development stage	29
Table B.3 – Activities during the realization stage	30
Table B.4 – Activities during the utilization stage	31
Table B.5 – Activities during the enhancement stage	31
Table B.6 – Activities during the retirement stage	31

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.

NOTES

AUSTRALIAN/NEW ZEALAND STANDARD

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.

Note 1 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.

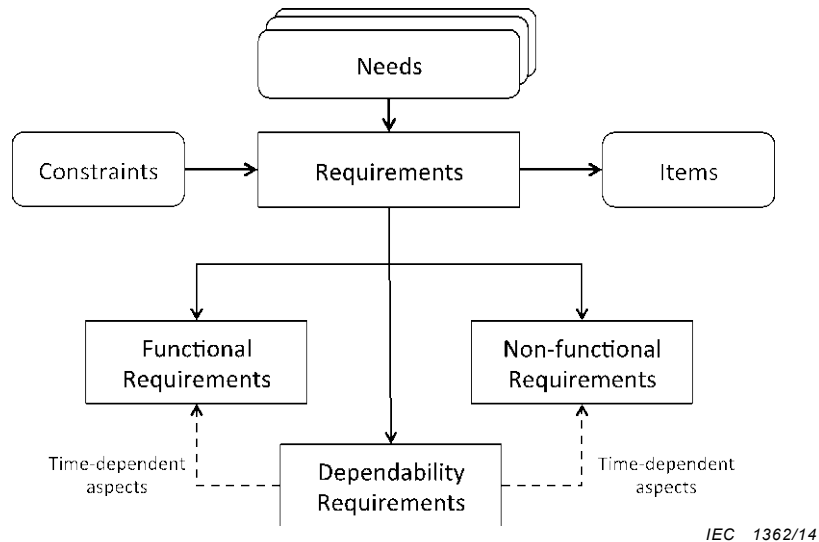


Figure 1 – Relationship of dependability to the needs and requirements of an item (product, system, process or service)

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.

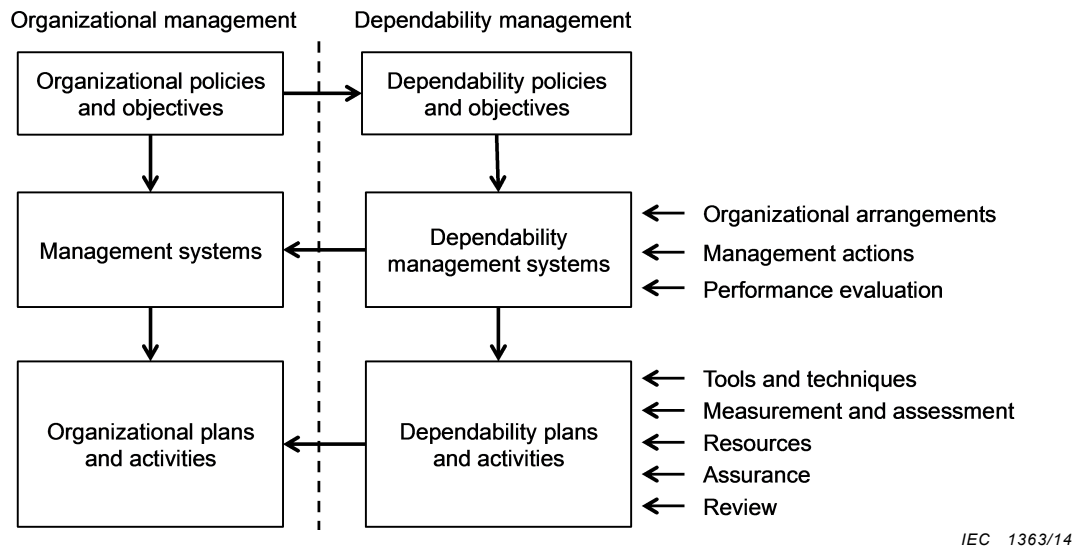


Figure 2 – Dependability management systems

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