AS IEC 60300.3.15—2011
IEC 60300-3-15, Ed.1.0 (2009)

AS IEC 60300.3.15—2011

Australian Standard®

Dependability management

Part 3.15: Application guide—Engineering of system dependability

This Australian Standard® was prepared by Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 19 October 2011.
This Standard was published on 14 November 2011.

The following are represented on Committee QR-005:

- Asset Management Council
- Australian Industry Group
- Australian Organisation for Quality
- CSIRO Information and Communication Technologies Centre
- Department of Defence (Australia)
- Energy Networks Association
- Engineers Australia
- Independent Transport Safety & Reliability Regulator
- Risk Management Association of Australia
- Risk Management Institution of Australasia
- The University of New South Wales
- University of Wollongong

This Standard was issued in draft form for comment as DR AS IEC 60300.3.15.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that 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Standards may also be withdrawn.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 that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Dependability management

Part 3.15: Application guide—Engineering of system dependability

First published as AS IEC 60300.3.15—2011.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9957 0

PREFACE

This Standard was prepared by the Standards Australia Committee QR-005, Dependability.

The objective of this Standard is to provide guidance on processes to achieve dependability of an engineering system throughout its lifecycle, and on methods to assess and measure dependability attributes.

This Standard is identical with, and has been reproduced from IEC 60300-3-15, Ed.1.0 (2009), *Dependability management*—Part 3-15: *Application guide—Engineering of system dependability*.

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

(a) Its number appears on the cover and title page while the International Standard number appears only on the cover.

(b) In the source text 'this part of IEC 60300' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian Standard*	
IEC		AS IEC	
60300	Dependability management	60300	Dependability management
60300-1	Part 1: Dependability management systems	60300.1	Part 1: Dependability management systems
60300-2	Part 2: Guidance for dependability programme management	60300.2	Part 2: Guidance for dependability programme management

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

INTRODUCTION

Systems are growing in complexity in today's application environments. System dependability has become an important performance attribute that affects the business strategies in system acquisition and the cost-effectiveness in system ownership and operations. The overall dependability of a system is the combined result of complex interactions of system elements, application environments, human-machine interfaces, deployment of support services and other influencing factors.

This part of IEC 60300 gives guidance on the engineering of the overall system to achieve its dependability objectives. The engineering approach in this standard represents the application of appropriate scientific knowledge and relevant technical disciplines for realizing the required dependability for the system of interest.

The four main aspects for engineering dependability concerning systems are addressed in terms of

– process,
– achievement,
– assessment, and
– measurement.

The engineering disciplines consist of technical processes that are applicable to the various stages of the system life cycle. Specific technical processes described in this part of IEC 60300 are supported by a sequence of relevant process activities to achieve the objectives of each system life cycle stage.

This part of IEC 60300 is applicable to generic systems with interacting system functions consisting of hardware, software and human elements to achieve system performance objectives. In many cases a function can be realized by commercial off-the-shelf products. A system can link to other systems to form a network. The boundaries separating a product from a system, and a system from a network, can be distinguished by defining the application of the entity. For example, a digital timer as a product can be used to synchronize the operation of a computer; the computer as a system can be linked with other computers in a business office for communications as a local area network. The application environment is applicable to all kinds of systems. Examples of applicable systems include control systems for power generation, fault-tolerant computing systems and systems for provision of maintenance support services.

Guidance on dependability engineering is provided for generic systems. It does not classify systems for special applications. The majority of systems in use are generally repairable throughout their life cycle operation for economic reasons and practical applications. Non-repairable systems such as communication satellites, remote sensing/monitoring equipment, and one-shot devices are considered as application-specific systems. They require further identification of specific application environment, operational conditions and additional information on unique performance characteristics to achieve their mission success objectives. Non-repairable subsystems and components are considered as throwaway items. The selection of applicable processes for engineering dependability into a specific system is carried out through the project tailoring and dependability management process.

This part of IEC 60300 forms part of the framework standards on system aspects of dependability to support IEC 60300-1 and IEC 60300-2 on dependability management. References are made to project management activities applicable to systems. They include identification of dependability elements and tasks relevant to the system and guidelines for dependability management reviews and tailoring of dependability projects.

AUSTRALIAN STANDARD

Dependability management

Part 3.15:
Application guide—Engineering of system dependability

1 Scope

This part of IEC 60300 provides guidance for an engineering system's dependability and describes a process for realization of system dependability through the system life cycle.

This standard is applicable to new system development and for enhancement of existing systems involving interactions of system functions consisting of hardware, software and human elements.

This standard also applies to providers of subsystems and suppliers of products that seek system information and criteria for system integration. Methods and tools are provided for system dependability assessment and verification of results for achievement of dependability objectives.

2 Normative references

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

IEC 60300-1, *Dependability management – Part 1: Dependability management systems*

IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

3 Terms and definitions

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

3.1
system
set of interrelated items considered as a whole for a defined purpose, separated from other items

NOTE 1 A system is generally defined with the view of performing a definite function.

NOTE 2 The system is considered to be bound by an imaginary surface that intersects the links between the system and the environment and the other external systems.

NOTE 3 External resources (i.e. outside the system boundary) may be required for the system to operate.

NOTE 4 A system structure may be hierarchical, e.g. system, subsystem, component, etc.

3.2
subsystem
system that is part of a more complex system

3.3
operating profile
complete set of tasks to achieve a specific system objective

