AS IEC 62347—2008
IEC 62347 Ed. 1.0 (2006)
Reconfirmed 2018

AS IEC 62347—2008

Australian Standard®

Guidance on system dependability specifications

This Australian Standard® was prepared by Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 16 June 2008.
This Standard was published on 28 July 2008.

The following are represented on Committee QR-005:

- AirServices Australia
- Australian Chamber of Commerce and Industry
- Australian Electrical and Electronic Manufacturers Association
- Australian Industry Group
- Australian Nuclear Science & Technology Organisation
- Australian Organisation for Quality
- Certification Interests (Australia)
- Department of Defence (Australia)
- Energy Networks Association
- Engineers Australia
- The University of New South Wales

This Standard was issued in draft form for comment as DR 08035.

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Standards may also be withdrawn.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.

STANDARDS AUSTRALIA

RECONFIRMATION

OF

AS IEC 62347–2008

Guidance on system dependability specifications

RECONFIRMATION NOTICE

Technical Committee QR-005 has reviewed the content of this publication and in accordance with Standards Australia procedures for reconfirmation, it has been determined that the publication is still valid and does not require change.

Certain documents referenced in the publication may have been amended since the original date of publication. Users are advised to ensure that they are using the latest versions of such documents as appropriate, unless advised otherwise in this Reconfirmation Notice.

Approved for reconfirmation in accordance with Standards Australia procedures for reconfirmation on 23 July 2018.

The following are represented on Technical Committee QR-005:

Asset Management Council
Australian Industry Group
Department of Defence (Australian Government)
Engineering New Zealand
Independent Transport Safety & Reliability Regulator
Institution of Occupational Safety and Health
National Road Carriers Association (NZ)
New Zealand Institute of Safety Management
Professionals Australia
Risk Engineering Society
Risk Management Institute of Australasia
RiskNZ
The University of New South Wales
University of Wollongong

Australian Standard®

Guidance on system dependability specifications

First published as AS IEC 62347—2008.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 8834 3

PREFACE

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

The objective of this Standard is to present a procedure for determining the dependability requirements for a system, and the rationale on the importance of dependability in determining and specifying the functions needed to meet a system's purpose, operating profile and performance objectives. It is suitable for use in conjunction with the AS IEC 60300 series of dependability management Standards.

This Standard is identical with, and has been reproduced from IEC 62347 Ed. 1.0 (2006), *Guidance on system dependability specifications*, which is part of a suite of Standards developed by the IEC Technical Committee IEC/TC 56, Dependability.

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

(a) Its number does not appear on each page of text and its identity is shown only on the cover and title page.

(b) In the source text 'this International Standard' should read 'this Australian Standard'.

(c) A full point should be substituted for a comma when referring to a decimal marker.

References to international Standards that are struck through in the bibliography are replaced by references to Australian or Australian/New Zealand Standards that are listed immediately thereafter and identified by shading.

The terms 'normative' and 'informative' are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

CONTENTS

Page

INTRODUCTION

A system is a physical and/or virtual entity. It is necessary sometimes to define a system's boundary so that it can be distinguished or separated from other systems. A system interacts with its surroundings or environment to fulfil a specific need or purpose, or to achieve a defined objective. This is accomplished through the interaction of the system's elements representing the necessary functions designed to meet the intended objective. Determining the functions needed to meet a specific objective represents the process of developing a system specification. Detailed system design begins only after the functions have been identified.

Systems may vary in their complexity structurally and functionally. A system can consist of hardware, software, and human elements, or a combination of any of these elements to perform the necessary functions. A system consisting of a single function can be a product, such as a television set or a software program for lighting controls. A system performing multiple functions can be a home theatre system or an aircraft. Individual systems with defined boundaries can be joined together to form a complex set of interacting systems such as a power distribution network or an internet protocol service.

System specification establishes the envelope and boundary for the system. System structure is often hierarchical linking subsystems and interacting systems. System specification is applicable to all systems under the generic definition of system irrespective of its hierarchy. It does not replace or substitute for use a product specification, which provides specific details of the product requirements.

The dependability of a system infers that the system is perceived to be trustworthy and has the ability to provide service upon demand as desirable performance attributes. Such performance attributes can be achieved through the incorporation of dependability into the functions. Dependability implies the awareness of user confidence acquired through prior experience of the system with reliable performance results in meeting user expectations.

This International Standard provides the rationale on the importance of dependability in system specification by functions. It presents a procedure for determining system dependability requirements. For generic system operation, the process of determining the functions needed to meet system dependability objective is described. For specific system operation, the concept of an operating profile is introduced to establish the requirements of functions in an environment relevant to the specific system operation. This International Standard is based on the system model and categorization of functions established in the IEC 61069 series. Relevant technical processes for the definition and analysis of system requirements are adopted from ISO/IEC 15288. The procedural steps and processes for determining system dependability requirements are presented with applicable examples. IEC 60300-1 and IEC 60300-2 are used to guide dependability management. This International Standard extends the dependability specification process to address functions as a prerequisite for system design. It complements IEC 60300-3-4 in specification of dependability requirements for products and equipment. The technical process for engineering dependability into systems is described in IEC 60300-3-15.

STANDARDS AUSTRALIA

Australian Standard

Guidance on system dependability specifications

1 Scope

This International Standard gives guidance on the preparation of system dependability specifications. It provides a process for system evaluation and presents a procedure for determining system dependability requirements.

This International Standard is not intended for certification or to perform conformity assessment for contractual purposes. It is not intended to change any rights or obligations provided by applicable statutory or regulatory requirements.

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 60050(191), *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

ISO/IEC 15288, *Systems engineering – System life cycle processes*

3 Terms and definitions

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

3.1
system
set of interrelated or interacting elements

[ISO 9000:2005, 3.2.1]

NOTE 1 In the context of dependability, a system will have:

- a defined purpose expressed in terms of intended functions;
- stated conditions of operation/use; and
- defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

[IEC 60300-1, 3.6]

NOTE 3 For some systems, such as Information Technology products, data is an important part of the system elements.

3.2
operating profile
complete set of tasks to achieve a specific system objective

NOTE An operating profile is the sequence of tasks to be performed by the system to achieve its operational objective. The operating profile represents a specific operating scenario for the system in operation.

