AS IEC 62628:2014
IEC 62628 Ed 1.0 (2012)

AS IEC 62628:2014

Australian STANDARD

Guidance on software aspects of dependability

STANDARDS Australia

This Australian Standard® was prepared by Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 13 March 2014.
This Standard was published on 4 April 2014.

The following are represented on Committee QR-005:

- Asset Management Council
- Australian Organisation for Quality
- Department of Defence (Australia)
- Engineers Australia
- Independent Transport Safety and Reliability Regulator
- Institution of Professional Engineers New Zealand
- New Zealand Society for Risk Management
- 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/NZS IEC 62628.

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Standards may also be withdrawn.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®

Guidance on software aspects of dependability

First published as AS IEC 62628:2014.

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

ISBN 978 1 74342 687 6

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee QR-005, Dependability. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian Standard rather than an Australian/New Zealand Standard.

The objective of this Standard is to provide Australian and New Zealand organizations who may be new to the areas of software development and assurance, with relevant guidance and methodology to facilitate the achievement of software dependability. It identifies the influence of management practices on dependability of software, and provides relevant technical processes to engineer software dependability into systems.

This Standard is identical with, and has been reproduced from IEC 62628 Ed 1.0 (2012), *Guidance on software aspects of dependability*.

Organizations should apply this Standard within the overall context of an AS/NZS ISO 31000 *Risk management—Principles and guidelines*, where aspects of software dependability (e.g. reliability, availability, and maintainability) have been clearly linked to the reduction of uncertainty with respect to business objectives.

This Standard is an entry-level Standard for those industries where a system lifecycle approach may not have previously been applied to software development and assurance. This Standard is not intended to revoke, supersede or be applied in preference to more sophisticated, industry-based or well-tried Standards for software dependability that are already used by some industries (e.g. rail, aerospace, automotive, and safety-related systems). Indeed, some aspects of this Standard may be seen to conflict with practices advocated by those other Standards..

For entry-level users, particular attention is drawn to Clauses 5.1, 5.2, 5.3 and Annex B where the overall system lifecycle framework for software dependability is described. Furthermore, Clauses 5.8, 6.1 and 7.4 suggest some fundamental strategies and practices for achieving software dependability.

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

(a) In the source text ‘this International Standard’ should read ‘this Australian Standard’.

(b) 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
60300-3-15	Part 3-15: Application guide—Engineering of system dependability	60300.3.15	Part 3.15: Application guide—Engineering of system dependability

Only normative references that have been adopted as Australian or Australian/New Zealand Standard have been listed.

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

Page

INTRODUCTION

Software has widespread applications in today's products and systems. Examples include software applications in programmable control equipment, computer systems and communication networks. Over the years, many standards have been developed for software engineering, software process management, software quality and reliability assurance, but only a few standards have addressed the software issues from a dependability perspective.

Dependability is the ability of a system to perform as and when required to meet specific objectives under given conditions of use. The dependability of a system infers that the system is trustworthy and capable of performing the desired service upon demand to satisfy user needs. The increasing trends in software applications in the service industry have permeated in the rapid growth of Internet services and Web development. Standardized interfaces and protocols have enabled the use of third-party software functionality over the Internet to permit cross-platform, cross-provider, and cross-domain applications. Software has become a driving mechanism to realize complex system operations and enable the achievement of viable e-businesses for seamless integration and enterprise process management. Software design has assumed the primary function in data processing, safety monitoring, security protection and communication links in network services. This paradigm shift has put the global business communities in trust of a situation relying heavily on the software systems to sustain business operations. Software dependability plays a dominant role to influence the success in system performance and data integrity.

This International Standard provides current industry best practices and presents relevant methodology to facilitate the achievement of software dependability. It identifies the influence of management on software aspects of dependability and provides relevant technical processes to engineer software dependability into systems. The evolution of software technology and rapid adaptation of software applications in industry practices have created the need for practical software dependability standard for the global business environment. A structured approach is provided for guidance on the use of this standard.

The generic software dependability requirements and processes are presented in this standard. They form the basis for dependability applications for most software product development and software system implementation. Additional requirements are needed for mission critical, safety and security applications. Industry specific software qualification issues for reliability and quality conformance are not addressed in this standard.

This standard can also serve as guidance for dependability design of firmware. It does not however, address the implementation aspects of firmware with software contained or embedded in the hardware chips to realize their dedicated functions. Examples include application specific integrated circuit (ASIC) chips and microprocessor driven controller devices. These products are often designed and integrated as part of the physical hardware features to minimize their size and weight and facilitate real time applications such as those used in cell phones. Although the general dependability principles and practices described in this standard can be used to guide design and application of firmware, specific requirements are needed for their physical construction, device fabrication and embedded software product implementation. The physics of failure of application specific devices behaves differently as compared to software system failures.

This International Standard is not intended for conformity assessment or certification purposes.

AUSTRALIAN STANDARD

Guidance on software aspects of dependability

1 Scope

This International Standard addresses the issues concerning software aspects of dependability and gives guidance on achievement of dependability in software performance influenced by management disciplines, design processes and application environments. It establishes a generic framework on software dependability requirements, provides a software dependability process for system life cycle applications, presents assurance criteria and methodology for software dependability design and implementation and provides practical approaches for performance evaluation and measurement of dependability characteristics in software systems.

This standard is applicable for guidance to software system developers and suppliers, system integrators, operators and maintainers and users of software systems who are concerned with practical approaches and application engineering to achieve dependability of software products and systems.

2 Normative references

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

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

IEC 60300-3-15, *Dependability management – Part 3-15: Application guide – Engineering of system dependability*

3 Terms, definitions and abbreviations

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

3.1 Terms and definitions

3.1.1
software
programs, procedures, rules, documentation and data of an information processing system

Note 1 to entry: Software is an intellectual creation that is independent of the medium upon which it is recorded.

Note 2 to entry: Software requires hardware devices to execute programs and to store and transmit data.

Note 3 to entry: Types of software include firmware, system software and application software.

Note 4 to entry: Documentation includes: requirements specifications, design specifications, source code listings, comments in source code, “help” text and messages for display at the computer/human interface, installation instructions, operating instructions, user manuals and support guides used in software maintenance.

3.1.2
firmware
software contained in a read-only memory device, and not intended for modification

