SLOVENSKI STANDARD
SIST EN IEC 62853:2018

01-december-2018

Odprti sistemi zanesljivosti (IEC 62853:2018)

Open systems dependability (IEC 62853:2018)

Ta slovenski standard je istoveten z: **EN IEC 62853:2018**

ICS:

03.100.40	Raziskave in razvoj	Research and development
03.120.01	Kakovost na splošno	Quality in general
21.020	Značilnosti in načrtovanje strojev, aparatov, opreme	Characteristics and design of machines, apparatus, equipment

SIST EN IEC 62853:2018 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62853

October 2018

ICS 03.100.40; 03.120.01; 21.020

English Version

Open systems dependability
(IEC 62853:2018)

Sûreté de fonctionnement des systèmes ouverts
(IEC 62853:2018)

Zuverlässigkeit offener Systeme
(IEC 62853:2018)

This European Standard was approved by CENELEC on 2018-07-18. 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, Serbia, 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: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 56/1772/FDIS, future edition 1 of IEC 62853, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62853:2018.

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) 2019-04-18
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2021-07-18

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

Endorsement notice

The text of the International Standard IEC 62853:2018 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

ISO 22301:2012	NOTE Harmonized as EN ISO 22301:2014 (not modified)
ISO 9000:2015	NOTE Harmonized as EN ISO 9000:2015 (not modified)
IEC 62741	NOTE Harmonized as EN 62741

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 60050-192	-	International electrotechnical vocabulary Part 192: Dependability	--	-
IEC 60300-1	-	Dependability management - Part 1: Guidance for management and application	EN 60300-1	-
ISO/IEC/IEEE 15288	2015	Systems and software engineering System life cycle processes	--	-

IEC 62853

Edition 1.0 2018-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Open systems dependability

Sûreté de fonctionnement des systèmes ouverts

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.40; 03.120.01; 21.020

ISBN 978-2-8322-5789-0

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 7
4 Open systems dependability 11
4.1 Open systems 11
4.2 Dependability issues specific to open systems 12
4.3 Objective 12
4.4 Achieving open systems dependability 13
4.5 Relationship to resilience and fault tolerance 13
5 Conformance 14
6 Process views for achieving open systems dependability 14
6.1 General 14
6.2 Consensus Building process view 15
6.2.1 Purpose 15
6.2.2 Outcomes 16
6.2.3 Processes, activities and tasks 17
6.3 Accountability Achievement process view 20
6.3.1 Purpose 20
6.3.2 Outcomes 21
6.3.3 Processes, activities and tasks 22
6.4 Failure Response process view 30
6.4.1 Purpose 30
6.4.2 Outcomes 31
6.4.3 Processes, activities and tasks 33
6.5 Change Accommodation process view 38
6.5.1 Purpose 38
6.5.2 Outcomes 39
6.5.3 Processes, activities and tasks 40
Annex A (informative) Example life cycle models with open systems dependability 49
A.1 General 49
A.2 Dependable Engineering for Open Systems (DEOS) life cycle model 49
A.3 Warranty Chain Management (WCM) life cycle model 51
Annex B (informative) An example template for dependability cases 53
B.1 Overview 53
B.2 Consensus Building argument 54
B.3 Accountability Achievement argument 56
B.4 Failure Response argument 58
B.5 Change Accommodation argument 61
Annex C (informative) Smart Grid 64
C.1 General 64
C.2 Background 64

C.3 Construction of a smart grid dependability case 64
C.3.1 General 64
C.3.2 Steps for construction of a smart grid dependability case 65
C.4 The Change Accommodation cycle 68
C.5 The Failure Response Cycle 69
Bibliography 70

Figure A.1 – DEOS life cycle model ([11], adjusted) 50
Figure A.2 – WCM life cycle model 52
Figure B.1 – Overall argument 53
Figure B.2 – Consensus Building 1 54
Figure B.3 – Consensus Building 2 55
Figure B.4 – Consensus Building 3 55
Figure B.5 – Accountability Achievement 1 56
Figure B.6 – Accountability Achievement 2 57
Figure B.7 – Accountability Achievement 3 57
Figure B.8 – Accountability Achievement 4 58
Figure B.9 – Failure Response 1 59
Figure B.10 – Failure Response 2 59
Figure B.11 – Failure Response 3 60
Figure B.12 – Failure Response 4 60
Figure B.13 – Failure Response 5 61
Figure B.14 – Failure Response 6 61
Figure B.15 – Change Accommodation 1 62
Figure B.16 – Change Accommodation 2 62
Figure B.17 – Change Accommodation 3 63
Figure B.18 – Change Accommodation 4 63

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPEN SYSTEMS DEPENDABILITY

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62853 has been prepared by IEC technical committee 56: Dependability.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
56/1772/FDIS	56/1776/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under “http://webstore.iec.ch” in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The ‘colour inside’ logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Open systems are systems whose boundaries, functions and structure change over time and which are recognized and described differently from various points of view. The dependability of open systems is a key attribute for the life cycle of a system that operates for an extended period of time in a real-world environment. Open systems dependability is the ability of open systems to accommodate changes in purpose, objectives, environment and actual performance and to continuously maintain accountability from stakeholders, in order to provide expected services as and when required. The attributes of dependability, including availability, reliability, maintainability and supportability, are the same for open systems as conventional systems but they have to be considered in the context that no single stakeholder has a full understanding of the system or its risks.

For open systems, security is especially important since the systems are much exposed to attack by malware. Since an open system changes continuously through its life, the design process, e.g. modelled by the spiral product development model, will to some extent continue during the whole lifetime of the system.

This document elaborates on IEC 60300-1 by providing additional guidance for dependability management of open systems.

This document provides guidance on open systems dependability by using the four process views, each of which selects and combines system life cycle processes, activities and tasks of ISO/IEC/IEEE 15288: 2015.

- Change Accommodation process view;
- Accountability Achievement process view;
- Failure Response process view;
- Consensus Building process view.

A dependability case that assures these process views is crucial for stakeholders to understand and agree on the boundaries of their responsibilities, to assign accountability for implementation and to duly manage changes in achieving open systems dependability.

The intended audience for this document ranges from users, owners and customers to organizations involved in and responsible for ensuring that open systems dependability requirements are being met. Organizations include all types and sizes of corporations, public and private institutions such as government agencies, business enterprises and non-profit associations.

OPEN SYSTEMS DEPENDABILITY

1 Scope

This document provides guidance in relation to a set of requirements placed upon system life cycles in order for an open system to achieve open systems dependability.

This document elaborates on IEC 60300-1 by providing details of the changes needed to accommodate the characteristics of open systems. It defines process views based on ISO/IEC/IEEE 15288:2015, which identifies the set of system life cycle processes.

This document is applicable to life cycles of products, systems, processes or services involving hardware, software and human aspects or any integrated combinations of these elements.

For open systems, security is especially important since the systems are particularly exposed to attack.

This document can be used to improve the dependability of open systems and to provide assurance that the process views specific to open systems achieve their expected outcomes. It helps an organization define the activities and tasks that need to be undertaken to achieve dependability objectives in an open system, including dependability related communication, dependability assessment and evaluation of dependability throughout system life cycles.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* (available at http://www.electropedia.org/)

IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-192 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
accountability
state of being answerable for decisions and activities to the organization's governing bodies, legal authorities and, more broadly, its stakeholders

Note 1 to entry: Accountability includes answerability to society in general.

Note 2 to entry: Description in ISO 26000:2010 [1]: Accountability involves an obligation on management to be answerable to the controlling interests of the organization and on the organization to be answerable to legal authorities with regard to laws and regulations. Accountability for the overall impact of its decisions and activities on society and the environment also implies that the organization's answerability to those affected by its decisions and activities, as well as to society in general, varies according to the nature of the impact and the circumstances.

Note 3 to entry: The definition in ISO 15489-1:2001 [2]: principle that individuals, organizations and the community are responsible for their actions and may be required to explain them to others.

[SOURCE: ISO 26000:2010, 2.1, modified – Notes to entry have been added.]

3.2
assurance case
reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims) is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)

Note 1 to entry: An assurance case contains the following and their relationships:

– one or more claims about properties;
– arguments that logically link the evidence and any assumptions to the claim(s);
– a body of evidence and possibly assumptions supporting these arguments for the claim(s);
– justification of choice of top-level claim and the method of reasoning.

Note 2 to entry: An assurance case can be understood as a reasoned and compelling argument, supported by a body of evidence, that a system, service or organization will operate as intended for a defined application in a defined environment and defined lifetime.

[SOURCE: ISO/IEC 15026-1:2013 [3], 3.1.3, modified – Note 2 to entry has been added.]

3.3
change accommodation
set of activities which modify and adapt a system to changes in its purpose, objectives, environment or actual performance that require re-establishment of stakeholders' consensus on the system

3.4
consensus
general agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments

Note 1 to entry: Consensus need not imply unanimity.

[SOURCE: ISO/IEC Guide 2:2004 [4], 1.7]

3.5
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system does and/or will satisfy the dependability requirements

Note 1 to entry: A dependability case is an assurance case whose top-level claim is about dependability.

[SOURCE: IEC 62741:2015, 3.1.1, modified – Note 1 to entry has been added.]

3.6
dependability communication
continual and iterative process that a stakeholder conducts to provide, share or obtain information, and to engage in dialogue with other stakeholders regarding the management of dependability

Note 1 to entry: The role of dependability communication in the management of open systems dependability is not unlike that of risk communication in risk management.

Note 2 to entry: See the definition of the term “communication and consultation” in ISO Guide 73:2009 [5], 3.2.1.

3.7
environment
<system> context determining the setting and circumstances of all influences upon a system

[SOURCE: ISO/IEC/IEEE 42010:2011 [6], 3.8]

3.8
failure response
set of activities initiated immediately when a failure is predicted or detected in order to prevent the failure or minimize its effect, to analyse its causes and prevent its recurrence and to fulfil accountability

3.9
frame of reference
set of conventions for the construction, interpretation and use of documents describing a common understanding of and explicit agreements on a system, its purpose, objectives, environment, actual performance, life cycle and changes thereof

3.10
interaction error
error that occurs due to the interactions between items despite each item’s performance meeting the specification

3.11
monitoring
determining the status of a system, a process or an activity

Note 1 to entry: To determine the status there may be a need to check, supervise or critically observe.

[SOURCE: ISO 22301:2012 [7], 3.29]

3.12
open system
system whose boundaries, functions and structure change over time and is recognized and described differently from various points of view

Note 1 to entry: Changes include not only adaptation with specific purpose but also spontaneous evolution. For example, they include spontaneous and uncoordinated changes within a system that spans multiple domains with different authorities.

Note 2 to entry: An open system’s boundaries, functions and structure are not only changing with time but can be vague at any point in time and recognized differently by different stakeholders. This refines the definition of system in IEC 60050-192 for a given level of abstraction and a given viewpoint. A boundary can have a clear definition at one level of abstraction, but it could become more vague at a more detailed level. The level of details necessary for a purpose or for a stakeholder need not be predetermined nor guaranteed to be attainable.

Note 3 to entry: An open system exchanges resources over its boundary with other systems or the environment, possibly changing the boundary itself.

Note 4 to entry: Every substantial system has aspects of both an open system and of a conventional system. The term open system is not used for classification of systems. The term applies to a system when its open aspects are significant for the discussion at hand about the system.

Note 5 to entry: The fact that a software system can be “open source” is irrelevant to being an open system, except that being open source software necessarily brings in aspects of open systems such as lack of centralized authority.