IEC 62853

Edition 1.0 2018-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Open systems dependability

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Sûreté de fonctionnement des systèmes ouverts

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

IEC 62853:2018-06(en-fr)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2018 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IECNORM.COM : Click to view the full PDF of IEC 62853:2018
Withdrawn
(standards.iteh.ai)
IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b706c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC 62853

Edition 1.0 2018-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Open systems dependability

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Sûreté de fonctionnement des systèmes ouverts

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.40; 03.120.01; 21.020

ISBN 978-2-8322-5789-0

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418db13de80/iec-62853-2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-241b5b8a180f/iec-62853-2018

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2 Normative references

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418db15d680/iec-62853-2018

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-[illegible]da20/iec-62853-2018

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/29-8536-411c-be52-2418dbf3de80/iec-62853-2018

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.

3.13
open systems dependability
ability to accommodate changes in purpose, objectives, environment and actual performance and to achieve accountability continually, so as to provide expected services as and when required

3.14
process
set of interrelated or interacting activities that use inputs to deliver an intended result

Note 1 to entry: Whether the “intended result” of a process is called output, product or service depends on the context of the reference.

Note 2 to entry: Inputs to a process are generally the outputs of other processes and outputs of a process are generally the inputs to other processes.

Note 3 to entry: Two or more interrelated and interacting processes in series can also be referred to as a process.

Note 4 to entry: Processes in an organization are generally planned and carried out under controlled conditions to add value.

Note 5 to entry: A process where the conformity of the resulting output cannot be readily or economically validated is frequently referred to as a “special process”.

Note 6 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified to prevent circularity between process and output, and Notes 1 to 5 to entry have been added.

iTeh STANDARD PREVIEW

[SOURCE: ISO 9000:2015 [8], 3.4.1]

(standards.iteh.ai)

3.15
process view
collection of processes, activities and tasks that provides a focus for a stakeholder’s particular concern about a system in a manner that cuts across all or parts of the life cycle

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296629-8556-411e-be52-2418db15de80/iec-62853-2018

3.16
resilience
adaptive capacity in a complex and changing environment

Note 1 to entry: The definition of resilience in UNISDR Terminology on Disaster Risk Reduction [9]: the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions.

Note 2 to entry: The definition in [10]: the persistence of service delivery that can justifiably be trusted, when facing changes.

[SOURCE: ISO Guide 73:2009, 3.8.1.7, modified – The definition has been made applicable to items other than organizations and Notes to entry have been added.]

3.17
stakeholder
individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations

EXAMPLE End users, end user organizations, supporters, developers, producers, trainers, maintainers, disposers, acquirers, supplier organizations and regulatory bodies.

Note 1 to entry: Some stakeholders can have interests that oppose each other or oppose the system.

Note 2 to entry: The term ‘interested party’ constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. This document uses the admitted term ‘stakeholder’, following ISO/IEC/IEEE 15288:2015.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.44, modified – Note 2 to entry has been added.]

4 Open systems dependability

4.1 Open systems

Open systems have the following characteristics [11].

– They are large, complex and interconnected.

– They can include black box components.

NOTE 1 A black box component is a component whose users do not know its implementation details and cannot control its functionality and interface.

– Their purpose, objectives, environment and actual performance are not determined and change through their lives. Unpredictable changes of user requirements, service objectives, services received via network, black box components, technological basis, etc., are commonplace.

– Their boundaries, functions and structure are ever-evolving and perceived differently by different stakeholders. Preventing them from becoming vague requires particular effort.

– Accountability is vital in their system life cycle and for risk control, but it needs particular effort to establish because of lack of effective central control.

– Understanding of the systems and their risks by their stakeholders is neither complete nor certain at any given time.

– The possibility of failures due to an incomplete understanding of the systems, unanticipated events and changes cannot be eliminated or predicted. Systems need to be resilient, need to have risk controls including error proofing, need to be able to recover from failures and need to be able to adapt to prevent recurrence.

– Achievement of dependability requires an iterative approach and depends on integration of the system operation and development. Performing dependability activities throughout the system life cycle and iterating them as often as needed is particularly important for open systems.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

NOTE 2 Some of these features are shared with so-called “system of systems” [12], [13] and “unbounded or weakly bounded systems”.

NOTE 3 Depending on a particular point of view, most systems have these features to some, possibly negligible, degree. A system is an open system when these features of the system are significant for the discussion at hand regardless of its being a system of systems.

A system necessarily exchanges services with a wide variety of other interconnected, independently managed systems. These surrounding systems are managed according to their own principles and stakeholders, and their interfaces are subject to change for various reasons. The system must serve diverse stakeholders. Each stakeholder has different objectives and there might be no single authority over the system; moreover, the objectives of the system and the surrounding systems change with time. The conditions for the system, such as requirements and constraints, change frequently and unpredictably. Thus, there are uncertainty and incompleteness about these conditions and they cannot be understood completely at any given time.

Since an open system changes continuously through its life, the design process, as modelled by the spiral product development model, will to some extent continue during the whole lifetime of the system.

Moreover, uncertainty and incompleteness are also present within the system itself, such as with respect to its functions, internal structure, and the boundary. Its subsystems are often managed by different parties and those involved in integration and coordination of the system boundaries might not have complete knowledge and control of them. Services and components might be added to or removed from the system during its operation by/for various stakeholders. This dynamic nature makes the system boundary, functions and structure ambiguous in practice, even if there is no ambiguity in theory at any specific time from a specific point of view.

For these reasons, as well as the sheer complexity and scale of the system, it is very difficult for any stakeholder to specify, comprehend or control the system and its management to any sufficient completeness and certainty. Unanticipated changes and failures of various degrees are a part of the system's nature. The use of the term open systems emphasises this aspect of systems.

The true, implicit expectations for the system are always relative to the context of other surrounding systems and stakeholders. The objectives of the various levels of systems surrounding the target system should be taken into account. As the context changes, and as incompleteness and uncertainty are resolved in one way or the other, the system should adapt to the corresponding changes in the requirements and assumptions. These changes cannot be fully anticipated or specified in advance.

4.2 Dependability issues specific to open systems

Open systems dependability aims to achieve service continuity over extended periods of time notwithstanding changes and failures. Achieving service continuity places requirements on the entire life cycle of the system and iteration thereof aided by enhancement activities.

Dependability management provided by IEC 60300-1 generally applies to open systems and this document shall be used together with IEC 60300-1. IEC 60300-1 requires that sustained improvement be ensured via planning and control of enhancement activities and appropriate reviews of progress. Open systems dependability elaborates on this for open systems where dependability directly depends on improvement with respect to frequent unpredictable changes. An iterative approach to the life cycle can be applied to accommodate such changes; see Annex A.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The scope of dependability management of an open system is not trivial because of characteristics explained in 4.1. Merely conforming to explicit agreements is not sufficient because agreements cannot adequately cover all aspects of the system of interest, as no open systems can be completely defined. Stakeholders need to be prepared to act beyond the agreements based on a common understanding of the system and its environment. As a principle, open systems dependability strives for confidence and trust in the system even under broken assumptions, requirements invalidated by changes, and eventual system failures.

IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c79-8536-411c-be52-2418dbf3de80/iec-62853-2018

The argument above highlights the importance of processes that continually review and revise the scope of dependability management and that provide explicit documentation and an agreement on the scope. The agreement on the scope by stakeholders needs to be backed by agreements on accountability.

Unanticipated causes cannot be prevented. What can be done is to identify key functions, anticipate possible consequences of losing the key functions and protect the key functions so that they can be recovered quickly or covered by redundancy.

4.3 Objective

The objective of open systems dependability is to sustain a degree of service continuity of a system in the context of surrounding systems, stakeholders and the environment, so far as practicable under unanticipated events and changes due to incompleteness and uncertainty of knowledge by stakeholders.

Systems are no longer taken as definite, but as open systems of which our knowledge cannot be complete or certain. A system with open systems dependability should have the ability:

– to continuously remove factors which have the potential to cause failures and hence improve itself;

– to take quick and appropriate action when a failure occurs;

– to prevent, minimize and mitigate damage;

– to continuously provide the services anticipated by stakeholders as much as possible (graceful degradation);
– to maintain the activities and tasks to achieve accountability for the system operations and processes;
– to help understand and communicate the assumptions made when describing the system, documenting these assumptions explicitly, and determining the system's dependability through the documentation and the authority for accepting it.

These abilities are expected for any dependable system even though they have particular importance for an open system that has increased likelihood of being affected by changes in other systems connected to it. Specificity of open systems dependability arises from the incompleteness and uncertainty under which the stated abilities are to be attained. The characteristic of open systems dependability lies in the process of achieving the stated ability, and the open systems dependability is not different from conventional dependability.

4.4 Achieving open systems dependability

For an open system to be dependable, its life cycle should enable stakeholders to do the following.

a) Establish a frame of reference understood by all stakeholders for addressing the system, its purpose, its operation, its environment and changes thereof, and then establish a common understanding and explicit agreements on those matters in that frame of reference.
b) Make transparent the relationship between a failure to fulfil an item in the stakeholder agreement and its implications for stakeholders and society in general, including accountable stakeholders' obligations to provide remedies, so as to motivate best efforts to honour the agreement and to secure availability of remedies for potential damage.
c) Plan and execute immediate actions against failures to provide expected services as much as possible, with least possible disruption and damage, in the manner most expedient in the context.
d) Organize activities that arise when adapting the system to changes in its environment, purpose, agreement, etc., and to gain from experience with failures, so as to improve dependability continuously.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62853:2018
https://standards.iteh.ai/catalog/standards/sist/8b296c29-8536-411c-be52-2418dbf3de80/iec-62853-2018

These four practices work together and each depends on the others. Item a) provides the basis of b), c) and d). Item b) helps to enforce the agreement in a) and promotes public confidence and trust in the system by communicating the plans and activities executed according to c) and d). Item c) gives necessary information to b), and triggers item d) for prevention of failure recurrence. Item d) restarts a) to reflect time-dependent changes in the common understanding and explicit agreements of a), which is always a provisional snapshot in need of continuous updating.

The ways in which these four practices are combined and collaborate can be represented in life cycle models. Annex A provides examples. An example of applying open systems dependability to a concrete open system is given in Annex C.

4.5 Relationship to resilience and fault tolerance

The concept of resilience is very similar for open and conventional systems. Traditional resilience (3.16 and its Note 1 to entry) emphasizes the ability to get back to normal operation after disturbances, while open systems dependability embraces the fact that even the definition of "normal operation" varies from time to time or from one point of view to another. A more recent concept of resilience (Note 2 to entry in 3.16) considers a broader range of changes and adaptations and shares the goal with open systems dependability. The difference is that open systems dependability focuses on cases where changes and a need to adapt stem from openness of systems, and hence on consensus and accountability in a system life cycle approach.