IEEE SA
STANDARDS ASSOCIATION

IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems

STANDARDS

IEEE Reliability Society
and the
IEEE Computer Society

Developed by the
Reliability Society Standards Committee
and the
Systems and Software Engineering Standards Committee

IEEE Std 7009™-2024

IEEE

IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems

Developed by the

Reliability Society Standards Committee
of the
IEEE Reliability Society

and the

Systems and Software Engineering Standards Committee
of the
IEEE Computer Society

Approved 20 May 2024

IEEE SA Standards Board

Abstract: A practical, technical baseline of specific methodologies and tools for the development, implementation, and use of effective fail-safe mechanisms in autonomous and semi-autonomous systems is established in this standard. The standard serves as the basis for developers, as well as users and regulators, to design fail-safe mechanisms in a robust, transparent, and accountable manner.

Keywords: autonomy, fail-safe, failure, harm, IEEE 7009™, regulation, safety, system design

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 979-8-8557-0838-7 STD27016
Print: ISBN 979-8-8557-0839-4 STDPD27016

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all IEEE standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers involved in technical working groups are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. "Artificial intelligence" refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and shall not be considered or inferred to be, the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE or IEEE SA. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments or questions, except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory

[1]Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2]Available at: https://standards.ieee.org/about/contact/.

requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

[3]Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4]Available at: https://standards.ieee.org/standard/index.html.

Patents

IEEE standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, data privacy, and interference protection practices and all applicable laws and regulations.

[5]Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

Participants

At the time this draft standard was completed, the P7009 Working Group had the following membership:

Ken Wallace, *Chair*
Danit Gal, *Vice Chair*
Marie Farrell, *Secretary*

Raja Chatlia
Michael Fisher
Simos Gerasimou
Lou Gullo
Ali Hessami
Xiao Liang
Matt Luckcuck
Zvikomborero Murahwi
Rod Muttram
Davy Pissoort
M. S. Prasad
Laura Pullum
Steven Ross
Cedric Sabbah
Alan Winfield

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Boon Chong Ang
Butch Anton
Mauro Bennici
Pieter Botman
Kevin Cameron
Zhiman Chen
Scott Crawford
Kurniawan Diharja
Marie Farrell
Andrew Fieldsend
David Fuschi
Danit Gal
Lou Gullo
Jon Hagar
Sheri Harshberger
Marco Hernandez
Ali Hessami
Werner Hoelzl
Piotr Karocki
Edmund Kienast
Stanislav Kovalenko
Madhav Krishna
Thomas Kurihara
Xiao Liang
Roberto Moreno
Zvikomborero Murahwi
Rajesh Murthy
Rod Muttram
Andrew Nack
Paul Nikolich
Joanna Olszewska
Bansi Patel
Howard Penrose
George Percivall
Davy Pissoort
R. K. Rannow
Annette Reilly
Steven Ross
Cedric Sabbah
Peter Saunderson
Robert Schaaf
Stephen Schwarm
Jhony Sembiring
Carl Singer
Thomas Starai
David Tepen
Ken Wallace
Alan Winfield
Oren Yuen
Janusz Zalewski

When the IEEE SA Standards Board approved this standard on 20 May 2024, it had the following membership:

David J. Law, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Gary Hoffman, *Past Chair*
Alpesh Shah, *Secretary*

Sara R. Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W Hotchkiss
Hao Hu
Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano
Paul Nikolich
Robby Robson
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 7009-2024, IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems.

This standard establishes a requirement-based framework for the design of fail-safe autonomous and semi-autonomous systems. A baseline set of system requirements and verification criteria, associated design capabilities, constraints, prerequisites, and characteristics for the design, implementation, and use of fail-safe capabilities in autonomous and semi-autonomous systems is provided.

Acknowledgments

Portions of this standard reprinted with permission from ISO/IEC Guide 51:2014 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved, ©ISO.

Portions of this standard reprinted with permission from IEC 60050-192 ed.1.0, Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch.

The IEEE P7009 Working Group thanks the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

Contents

IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems

1. Overview

1.1 Scope

This standard establishes a practical, technical baseline of specific methodologies and tools for the development, implementation, and use of effective fail-safe mechanisms in autonomous and semi-autonomous systems. The standard serves as the basis for developers, as well as users and regulators, to design fail-safe mechanisms in a robust, transparent, and accountable manner.

1.2 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[6,7]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

1.3 Field of application

This standard treats autonomous and semi-autonomous systems as engineered aggregations of products, processes, services, or any combination thereof that are capable, to a degree, of making and acting upon decisions without human intervention.

[6]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
[7]The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

1.3.1 Distinguishing characteristics of autonomous and semi-autonomous systems

For the purposes of this standard, *Distinguishing Characteristics* of autonomous and semi-autonomous systems include, but are not necessarily limited to, the following intrinsic capabilities:

a) To make decisions without prior human validation of the consequences of these decisions.

b) To act upon such decisions through interactions with the environment in which such a system operates.

c) To adapt and modify both the decision-making processes and the consequential interactions with the environment within which such a system operates through a process of learning.

These characteristics are intentional outcomes of design and production processes when applied to the manufacture of a *system-of-interest*. Such processes are integral to the engineering life cycle of any system-of-interest, regardless of whether capable of operating autonomously or not.

1.3.2 Key characteristics of a system-of-interest

A system-of-interest can be characterized as identified in ISO/IEC/IEEE 15288:2023 [B7] and ISO/IEC/IEEE 12207:2017 [B3].[8] These standards adopt a harmonized set of characteristics for such systems as identified below:

a) Defined boundaries encapsulate meaningful needs and practical solutions.

b) There is a hierarchical or other relationship between system elements.

c) An entity at any level in the system-of-interest can be viewed as a system.

d) A system comprises an integrated, defined set of subordinate system elements.

e) Humans can be viewed as both users external to a system and as system elements (i.e., operators) within a system.

f) A system can be viewed in isolation as an entity, i.e., a product; or as a collection of functions capable of interacting with its surrounding environment, i.e., a set of services.

Characteristics a) through f) are referred to as the *Key Characteristics* in the remainder of this standard.

1.3.3 Autonomous-System-Of-Interest

This standard refers to any system-of-interest or systems-of-interest capable of exhibiting both the Key and Distinguishing Characteristics as an *Autonomous-System-Of-Interest,* abbreviated hereinafter to ASOI, regardless of whether there is one or more such system-of-interest.

The environment within which an ASOI operates can include both tangible (e.g., physical entities) and intangible elements (e.g., natural human cognitive processes). While the combination of the Distinguishing and Key Characteristics can be used as an aid to determine whether application of this standard is appropriate, these characteristics are not, for the purposes of this standard, normative. The extent to which ASOI can exhibit the Distinguishing Characteristics reflects the degree of autonomy engineered into the ASOI.

NOTE 1—Reference to ASOI in this standard includes both autonomous and semi-autonomous systems.[9]

NOTE 2—This standard recognises and delineates manufactured systems as being distinct from naturally occurring (biological) systems that exhibit autonomous capabilities.

[8]The numbers in brackets correspond to those of the bibliography in Annex C.
[9]Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

NOTE 3—Manufactured systems that operate autonomously but do not exhibit the Distinguishing Characteristics are not addressed in this standard. There is, however, nothing in this document that intentionally excludes or prevents application of this standard to such systems.

NOTE 4—Both ISO/IEC 15288 [B7] and ISO/IEC 12207 [B3] address the wider context that a system-of-interest can be incorporated within by reference to System-of-Systems (SoS). SoS are systems-of-interest the elements of which are themselves systems. While an ASOI can be an element (a system) within a SoS, consideration of ASOI as such elements is not addressed in this standard.

1.4 Audience

This standard is intended to be used by stakeholders throughout the engineering life cycle of an ASOI. Such stakeholders typically include, but are not limited to, the following:

a) *Acquirer:* the stakeholder that acquires or procures the ASOI.

b) *Independent Safety Assessor:* the stakeholder that holds responsibility for the independent assessment of the safety of the ASOI.

c) *Certification Authority:* the stakeholder that holds responsibility for the certification of the ASOI.

d) *Competent Authority:* the stakeholder that holds authority in respect of safety for the domain of application within which the ASOI operates.

e) *Maintainer:* the stakeholder that performs maintenance activities (including, but not limited to, inspection, maintenance, repair, and upgrade of the ASOI) during operation of the ASOI.

f) *Manufacturer:* the stakeholder that performs manufacturing activities (including, but not limited to, requirements analysis, design, implementation, and verification through to acceptance) during the engineering life cycle of the ASOI. This stakeholder is typically referred to as the Original Equipment Manufacturer (OEM).

g) *Operator:* the stakeholder that operates the ASOI to provide a service to End Users.

h) *Safety Supervisor:* the stakeholder that holds responsibility for supervision of the ASOI in respect of safety during operation.

i) *End Users:* the group of stakeholders that utilize the ASOI directly or indirectly through a service provided by the ASOI.

j) *Supplier:* the stakeholder that supplies the ASOI to an Acquirer.

k) *Regulator:* the stakeholder that regulates the domain of application within which the ASOI operates.

This list of stakeholders, and the individual entries within, are not definitive, nor exhaustive. The exact concerns and interests of individual stakeholders can vary relative to the foregoing list for a domain of application or specific application in a particular domain.

The term *stakeholder* is used in this standard without necessarily identifying the specific concerns or interests of the stakeholder in respect of the ASOI.

When applying this standard early identification and agreement of accountabilities and responsibilities of stakeholders should be a priority during the engineering life cycle.

NOTE—Responsibilities of competent stakeholders are identified throughout this standard, however, consideration of the accountability that can result from such responsibilities is not addressed in this standard.

1.5 Competency considerations

This standard applies the phrase *competent stakeholder* to an individual or an organized group of individuals performing an identified role, activities, or tasks. All instances of the phrase *competent stakeholder* in this standard are in reference to a person (or persons) *who through education, training, and experience possesses the knowledge, skills, cognitive abilities, and the attitudes necessary to perform a specified scope of work* (IEC/IEEE 82079-1:2019 [B2], ISO/IEC/IEEE 24765:2017 [B10]).

Existing frameworks regarding competence for safety engineering or similar frameworks, can be consulted for further information in respect of means for persons to achieve, demonstrate, and thereafter maintain competence within an organizational framework. Competent organizations can, by extension, demonstrate equivalent competencies at an organizational level.

The specification of necessary competencies required by persons involved in the application of this standard is the responsibility of competent stakeholders.

NOTE—Competency is typically considered a contributory element to a quality management system such as, for example, ISO 9001:2015 [B13].

1.6 Regulatory considerations

This standard does not assume, establish, nor require any jurisdictional, legal, or regulatory context, or equivalent, for the fail-safe design of an ASOI. The standard recognizes that domains and associated jurisdictions within which ASOI operate can address safety through established legal and regulatory frameworks. It is intended that this standard can be employed to augment and enhance the technical capabilities of such frameworks to address the specific challenges that autonomous systems present in respect of safety. In the absence of an established applicable framework this standard can be employed by stakeholders as a basis for identifying relevant technical considerations to be accounted for when developing such a framework. At minimum, such considerations shall include sufficient information to enable the design characteristics identified in 6.5 to be specified for an intended application in an identified regulatory context.

Clause 7 of this document addresses inclusion of capabilities required of an ASOI to enable fail-safe operations within a regulatory context. The extent of regulation considered in this standard is limited to the fail-safe capabilities of an ASOI. Consideration of wider regulatory aspects of ASOI is not within the scope of this standard.

Users of IEEE Standards documents should consult all applicable laws and regulations. Implementers of this standard are responsible for observing all applicable regulatory requirements.

NOTE—Regulatory mechanisms that manage complex systems range from those that occur naturally, in biological systems, to societal constructs such as governance, legal and other equivalent frameworks. All references in this standard to regulation are to societal constructs regardless of the actual mechanisms employed to achieve the required regulation.

1.7 Relationship to systems safety engineering life cycles

This standard addresses the fail-safe design of ASOI. To enable this outcome, it is intended that this standard augment and enhance, rather than act as a substitute or replacement for, established safety engineering practice—if such practice exists. Domains, within which ASOI operate, that utilize proven approaches to systems safety engineering can employ this standard to extend established practice to facilitate fail-safe design of ASOI. Extension beyond the incorporation of a fail-safe design for ASOI is, however, not within the scope of this standard. In particular, the development of a safety-critical system, as identified in 6.2, requires the application of appropriate engineering practices. Such practices are not addressed in this standard.

In the event of any discrepancies or inconsistencies between this standard and other applicable safety standards, responsibility for defining and communicating the precedence of standards that apply during the fail-safe design of an ASOI resides with competent stakeholders.

NOTE—Established systems safety engineering practice is typically conducted in accordance with an established approach and a supporting principle in respect of the management of risk. Examples of such principles include but are not limited to: As Low As Reasonably Achievable (ALARA), As Low As Reasonably Practicable (ALARP), So Far As Is Reasonably Practical (SFAIRP), Globalement Au Moins Aussi Bon (GAMAB), Minimum Endogenous Mortality (MEMS) or the Principle (PP). This standard does not require, rely upon, recommend, nor endorse any specific approach, or principle, to manage risk.

1.8 Relationship to systems and software engineering life cycles

This standard does not establish nor require a particular engineering life cycle for the development of ASOI. By agreement stakeholders can adopt any life cycle that is appropriate, taking account of the extent of existing engineering practice. This standard makes informative reference to ISO/IEC/IEEE 15288 [B7] and the software engineering equivalent ISO/IEC/IEEE 12207 [B3] and the harmonized set of processes therein as examples of the activities that are typically required during the development and operation of ASOI. When there is no established engineering practice, these standards can provide a basis for defining engineering processes capable of supporting the development of ASOI.

Significant use of software to implement ASOI functions is typical. Software cannot, however, operate in the absence of hardware and consideration of the system context of an ASOI shall always take precedence over consideration of any software that constitutes part of the system. When executed by hardware within a particular system context software can initiate or contribute to a hazardous situation.

NOTE—The foregoing precedence aligns with the fundamental premise identified in 5.2.1 of ISO/IEC/IEEE 12207:2017 [B3].

1.9 Limitations

Reasoning about safety requires specific knowledge and understanding of the context and the consequences of actions or inaction to determine what constitutes, or does not constitute, fail-safe. As a matter of practicality, it is not possible to address considerations of context or consequence directly in a general or universal manner. Application of this standard requires diligence by competent stakeholders to verify that all necessary considerations, in respect of fail-safe behavior, are accounted for when applying this standard.

The extent to which a realized design can fail safely, when in operation, is typically determined by multiple factors. Regardless of the nature and number of these factors, ultimately there is always a limit to the extent of failure beyond which a design is incapable of failing safely. Conformance to this standard cannot prevent there being such a limit for a design, nor does it confer immunity from such a limit adversely affecting safety if the design limit is exceeded. Conformance to this standard does not render a design invulnerable to failure, nor can conformance guarantee the preservation of safety.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices, and all applicable laws and regulations.

1.10 Disclaimer

This standard establishes minimum requirements for the fail-safe design of autonomous and semi-autonomous systems. Implementing these requirements through the provision of ASOI, or elements thereof, according to this standard does not ensure an absence of hazards or hazardous behavior. Conformance with this standard does not absolve any party from any ethical, social, moral, financial, or legal obligations.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO/IEC Guide 51, Safety aspects—Guidelines for their inclusion in standards.[10,11]

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[12]

NOTE—For additional terms and definitions in the field of systems and software engineering, see ISO/IEC/IEEE 24765 [B10], which is published periodically as a "snapshot" of the SEVOCAB (Software and Systems Engineering Vocabulary) database and is publicly available at https://www.computer.org/sevocab.

attribute: Inherent property or characteristic of an entity that can be distinguished quantitatively or qualitatively by human or automated means (ISO/IEC/IEEE 29148:2018 [B12]).

NOTE—ISO 9000 distinguishes two types of attributes: a permanent characteristic existing inherently in something; and an assigned characteristic of a product, process, or system (e.g., the price of a product, the owner of a product).

condition: Measurable qualitative or quantitative attribute that is stipulated for a requirement and that indicates a circumstance or event under which a requirement applies (ISO/IEC/IEEE 29148:2018 [B12]).

consequence: Outcome of an event affecting one or more stakeholders (ISO/IEC/IEEE 16085:2021 [B9]).

NOTE 1—An event can lead to a range of consequences.

NOTE 2—A consequence can be certain or uncertain and have positive or negative effects on objectives.

NOTE 3—Consequences can be expressed qualitatively or quantitatively.

NOTE 4—Initial consequences can escalate through follow-on effects.

NOTE 5—Follow-on effects can alternatively be referred to as "avalanche", "cascade", "domino", or "knock-on effects." (This note is introduced in this standard; it is not included in ISO/IEC/IEEE 16085 [B9].)

NOTE 6—An objective is a result to be achieved (this note is introduced in this standard; it is not included in ISO/IEC/IEEE 16085 [B9]).

constraint: Externally imposed limitation on the system, its design, or implementation or on the process used to develop or modify a system (ISO/IEC/IEEE 29148:2018 [B12]).

NOTE 1—A constraint is a factor that is imposed on the solution by force or compulsion and may limit or modify the design.

[10]ISO/IEC Guide 51 was confirmed by ISO as being current following review in 2019.
[11]ISO/IEC Guide 51 is freely available online from the ISO Website https://www.iso.org/standards.html.
[12]*IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

NOTE 2—Alternative definitions of a constraint make no distinction between internal and external factors. (This note is introduced in this standard; it is not included in ISO/IEC/IEEE 29148 [B12].)

event: Occurrence or change of a particular set of circumstances.

NOTE 1—An event can be a change of status or condition.

NOTE 2—An event can comprise one or more occurrences and can have several causes.

NOTE 3—An event can consist of something not happening.

NOTE 4—An event can sometimes be referred to as an "incident" or "accident".

NOTE 5—An event that does not result in harm can also be referred to as a "near miss", "incident", "near hit" or "close call".

NOTE 6—An event can be certain or uncertain.

NOTE 7—The cause of an event can also be an event in a chain of events.

harm: Injury or damage to the health of people, or damage to property or the environment (ISO/IEC Guide 51:2014).[13]

NOTE 1—The natural environment is an integral part of the environment (this note is introduced in this standard; it is not included in ISO/IEC Guide 51).

NOTE 2—Non-human lifeforms are an integral part of the natural environment (this note is introduced in this standard; it is not included in ISO/IEC Guide 51).

NOTE 3—People includes anyone who can potentially be harmed, irrespective of whether identified as a stakeholder or not (this note is introduced in this standard; it is not included in ISO/IEC Guide 51).

hazard: Potential source of harm (ISO/IEC Guide 51:2014).[13]

hazardous event: Event that can cause harm (ISO/IEC Guide 51:2014).[13]

hazardous situation: Circumstance in which people, property or the environment is/are exposed to one or more hazards (ISO/IEC Guide 51:2014).[13]

information item: A separately identifiable body of information that is produced, stored, and delivered for human use (ISO/IEC/IEEE 15289:2019 [B8]).

likelihood: Chance of something happening (ISO/IEC/IEEE 16085:2021 [B9]).

NOTE 1—In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively, or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2—The English language term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term probability is often used. However, in English "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[13]©ISO. This material is reproduced from ISO/IEC Guide 51:2014 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

procedure: Information item that presents an ordered series of steps to perform a process, activity, or task (ISO/IEC/IEEE 15289:2019 [B8]).

NOTE—A procedure defines an established and approved way or mode of conducting business in an organization. It details permissible or recommended methods in order to achieve technical or managerial goals or outcomes.

requirement: Statement that translates or expresses a need and its associated constraints and conditions (ISO/IEC/IEEE 29148:2018 [B12]).

NOTE 1—Requirements exist at different levels in the system structure.

NOTE 2—A requirement is an expression of one or more particular needs in a specific, precise and unambiguous manner.

NOTE 3—A requirement always relates to a system, software or service, or other item of interest.

risk: Effect of uncertainty on objectives (ISO/IEC/IEEE 16085:2021 [B9]).

NOTE 1—An effect is a deviation from the expected — positive or negative. A positive effect is also known as an opportunity.

NOTE 2—Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

NOTE 3—Risk is often characterized by reference to potential events and consequences or a combination of these.

NOTE 4—Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5—Uncertainty is the state, even partial, of deficiency of information related to understanding of an event, its consequence or likelihood.

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 (ISO/IEC/IEEE 15288:2023 [B7]).

NOTE—Some stakeholders can have interests that oppose each other or oppose the system.

3.2 Acronyms and abbreviations

ASOI	Autonomous-System-Of-Interest
EOI	Event-Of-Interest
SCF	Safety-Critical-Function
SCS	Safety-Critical-System
SRF	Safety-Related-Function
SRS	Safety-Related-System
SXF	Safety-Exempt-Function
SXS	Safety-Exempt-System

4. Conformance

Conformance to this standard can be claimed by the provision of objective evidence to substantiate one of the following claims:

Claim A: all outcomes identified in Clause 7 and Clause 8 have been achieved.

Claim B: all tasks identified in Clause 7 and Clause 8 have been completed.

Claim C: all outcomes and all tasks identified in Clause 7 and Clause 8 have been achieved or completed.

In addition to substantiating one of the foregoing claims, conformance to this standard also requires objective evidence to substantiate each of the following claims:

Claim D: the solution for which conformance is claimed is in accordance with the design, capabilities, constraints, prerequisites, and characteristics as identified in Clause 6.

Claim E: the solution for which conformance is claimed fulfills all the system requirements identified in Annex A.

The chosen combination of claims (ADE, BDE or CDE) and supporting objective evidence in respect of a specific ASOI should be recorded in an Assurance Case; or an equivalent artefact in accordance with established safety engineering practice, if such practice exists for the domain. The ISO/IEC/IEEE 15026 series of standards, in particular ISO/IEC/IEEE 15026-1 [B4], ISO/IEC/IEEE 15026-2 [B5], and ISO/IEC/IEEE 15026-4 [B6], can be consulted in the absence of established practice in respect of assurance considerations.

Competent stakeholders are responsible for specifying and agreeing the nature and extent of objective evidence appropriate for the specific ASOI and application for which conformance to this standard is claimed.

In addition to substantiation of the chosen combination of claims, conformance to this standard requires fulfillment of all normative requirements, as denoted by *shall* statements in Clause 1 through Clause 6 and Clause 9.

NOTE—In respect of the claims:

— Claim A is a “full conformance to outcomes” claim.

— Claim B is a “full conformance to tasks” claim.

As identified in Clause 7 (Claims of conformance to a process) of ISO/IEC/IEEE 24774:2021 [B11].

5. Key concepts

This clause identifies and explains essential concepts employed in this standard. The information contained in this clause is intended to enable stakeholders to make use of the standard having taken due account of their specific context of application.

5.1 Safety and fail-safe design

Terminology in respect of safety varies. Reflecting the lack of a universally accepted definition of safety, all instances of the term *safety* in this standard are in reference to *freedom from unacceptable risk of harm.*

Similarly, all instances of the term *fail-safe* in this standard are in reference to the capability of an ASOI to *preserve freedom from unacceptable risk of harm in the event of failure of the ASOI*. A fail-safe design incorporates a capability for such preservation into an ASOI during the design phase of ASOI manufacture.

5.2 Risk

Consideration of risk in this standard is limited to that necessary to enable a fail-safe design for ASOI. The standard does not address other categories of risk that can exist but do not have the potential to cause harm. In general terms risk can be addressed by risk management strategies; safety being treated as one category, or profile, of risk to be managed. In accordance with such treatments, and as identified in 3.1, risk is the effect of uncertainty on objectives; an effect being a deviation from the expected. Deviations can be either positive or negative. Generally, the focus for risk management activities is on reducing (mitigating) negative deviations (ISO/IEC/IEEE 16085 [B9]).

This standard is concerned with negative deviations in freedom from unacceptable risk of harm, in the event of failure. Consideration of positive deviations is limited to those the purpose of which is to preserve this freedom during such events. Additional opportunities, in the form of positive deviations, to reduce risk beyond that which is already considered acceptable are not addressed in this standard.

As applied to risk, this standard treats the terms *acceptable* and *tolerable* as being synonymous. This treatment is in accordance with that identified in ISO Guide 51.[14] This standard utilizes the term acceptable in preference to tolerable. The terms *unacceptable* and *intolerable* are likewise considered synonymous for the purposes of this standard; unacceptable is used in preference to intolerable.

NOTE—Further information on risk profiles can be found in ISO/IEC/IEEE 16085 [B9].

5.3 Unacceptable risk and residual risk

For any engineered system there is an upper limit to acceptable risk beyond which risk becomes unacceptable. Such a limit applies irrespective of whether the system is autonomous or not. The threshold between acceptable and unacceptable risk can be characterized as the upper limit to a tolerance interval. Risk that lies within the tolerance interval is acceptable; risk beyond the upper limit of the interval is not.

As a matter of practicality, the total elimination of all risk from a system irrespective of whether autonomous or not is rarely, if ever, possible. Consequently, there is always a lower limit on the tolerance interval reflecting the level of risk that exists regardless of the resources expended to mitigate (reduce) the risk. Risk that remains following risk mitigation (treatment) is referred to as residual risk. The extent of residual risk varies depending upon the specific details of the system and application involved. For applications of any complexity exhaustive assessment and complete mitigation of all risks is usually not possible.

NOTE—Reference can be made to ISO Guide 51 for further details in respect of the relationships between hazards and risk, residual risk, and acceptability considerations.

5.4 Hazardous events and situations

A hazard is a potential source of harm, a hazardous event being an event that has the potential to cause harm. A hazardous situation is one in which stakeholders are exposed to one or more hazards. Stakeholders that can be exposed to hazards include non-human forms of life and the environment.

Stakeholders considering the adoption of this standard are responsible for determining whether any hazards attributable to a proposed ASOI have sufficient potential to cause harm that the application of this standard is appropriate.

[14]Information on references can be found in Clause 2.

5.5 Events involving failure

In broad terms, an event involving failure is an occurrence of a particular set of circumstances that can result in loss. Any loss that does occur is a consequence of the failure event. A fail-safe ASOI design addresses any potential loss of safety in the event of failure of the ASOI through the provision of capabilities to preserve freedom from unacceptable risk of harm. References in this document to events involving failure, alternatively *failure events*, are limited to this aspect of loss. This limitation applies regardless of the other aspects of loss that can also occur in the event of failure.

NOTE—Terminology in respect of failure and the relationships to the causes of failure varies considerably between different domains and sectors. Reflecting the lack of a commonly accepted definition, use of the term *failure* in this standard is only ever in the context of an event, or a set of events.

5.6 Behavior and performance

For the purposes of this standard the term *behavior* characterizes the responses that can be observed when an ASOI reacts to circumstances and associated stimuli. Such responses can be intended, unintended or a combination of both. Intentional responses reflect design intent as realized through manufacture and thereafter operation of the ASOI.

The subset of observable behaviors exhibited by an ASOI that are subject to measurement, assessment and/or evaluation characterize the *performance* of the ASOI. Such activities are typically conducted to verify the performance of the ASOI during the development and operational deployment of the ASOI. Similar activities are also typically conducted to maintain delivery of the required performance by the ASOI during operation.

NOTE—Verification provides confirmation, through objective evidence, that specified requirements have been fulfilled; thereby providing an answer to the question of whether the product (ASOI) has been built right. Verification considerations can be addressed through the application of the Verification process (6.4.9) identified in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] or alternative but comparable processes.

5.7 Anomalous behavior

Inherently an ASOI has the potential to exhibit unexpected or unintended behaviors to an extent in excess of systems that are not capable of exhibiting the Distinguishing Characteristics. To address the consequences when this potential is realized all events resulting in unexpected ASOI behaviors are, for the purposes of this standard, *behavioral anomalies*. This characterization applies irrespective of the cause of the behavior and includes, but is not limited to, behavioral anomalies attributable to events involving failure. Events that can result in behavioral anomalies are a source of substantial and significant uncertainty, particularly during the design of ASOI. Not all events that can cause or contribute to hazardous situations during ASOI operation can be identified at the design stage: certain events are exposed, and hence identified, only following occurrence during operation of the ASOI.

NOTE 1—Emergent behaviors are a defining characteristic of complex systems irrespective of whether natural or artificial in origin. For the purposes of this standard all such behaviors exhibited by ASOI are instances of behavioral anomalies; irrespective of whether the deviation resulting from an observed emergent behavior is positive or negative.

NOTE 2—In scientific and associated technical contexts the concept of uncertainty is refined to categorize uncertainty as being either aleatoric or epistemic. The first category of uncertainty is attributable to the fundamental indeterminacy or randomness that characterizes and is inherent in the physical world. The second category reflects an absence of knowledge. While the extent of aleatoric uncertainty is determined by limits of the physical world, in theory at least, given sufficient enquiry epistemic uncertainty can be eliminated. The extent of elimination of epistemic uncertainty that is possible varies in practice; total elimination being unlikely. Consequently, both categories of uncertainty typically contribute to risk and there is no requirement in this standard that any distinction be made between the two categories.

5.8 Temporal considerations

Preserving safety in the event of failure requires recognition of the onset of hazardous situations and the capability to recover from the failure event in an acceptable manner: if such recovery is necessary. Fundamental to preserving safety is the amount of time available from onset of such situations until the subsequent point in time at which risk can become unacceptable if no action is taken: the more time there is to recognize and react to a hazardous situation the more likely it is that safety can be preserved.

The circumstances of hazardous situations depend upon multiple factors: some of these factors are known, some are unknown, and others cannot be known (unknowable) until the situation occurs. Nevertheless, any hazardous situation is the consequence of one or more *initiating events*. Such events include but are not limited to those directly attributable to failure. Not all events are intrinsically and immediately hazardous in nature. In isolation initiating events can lack the potential to be hazardous. Such events can, however, contribute to the onset of hazardous situations when interacting with other concurrent events and/or influencing subsequent events through follow-on effects.

This standard employs the following parameters to characterize temporal aspects of hazardous, or potentially hazardous situations:

a) *Time-To-Recovery:* The worst-case elapsed time as measured from the onset of a hazardous situation until completion of any recovery action such that the level of post-recovery risk is acceptable.

b) *Time-To-Violation:* The minimum elapsed time as measured from the onset of a hazardous situation until risk can become unacceptable if no action is taken.

c) *Time-To-Harm:* The minimum elapsed time as measured from the onset of a hazardous situation until the occurrence of harm.

Post-recovery risk is the level of risk that remains on completion of recovery. Whether such recovery can restore risk to the level that was acceptable prior to the onset of the hazardous situation is determined by the conditions and events causing the hazardous situation. If such recovery is not possible then post-recovery risk will continue to deviate negatively relative to the acceptable level prior to the onset of the hazardous situation. What action, if any, is required in respect of any persistent deviation is determined by whether the post-recovery risk remains within tolerance of the acceptable risk.

The ability to fail safely necessitates that the Time-To-Recovery should not exceed the Time-To-Violation and never exceed the Time-To-Harm.

NOTE 1—An initiating event can also be referred to as a *triggering event*.

NOTE 2—The start, or onset, of an event can be referred to as the leading edge of the event; the end, or termination, of the event being the trailing edge. The elapsed time between the leading and trailing edges of an event represents the event duration.

NOTE 3—In respect of ASOI performance other than safety, recovery does not necessitate, nor imply restoration of what would be regarded as normal service. Performance during and following recovery can and is likely to be reduced relative to what is considered as "normal or business as usual" performance.

6. Fail-safe design capabilities, constraints, prerequisites, and characteristics

This clause identifies the design capabilities, constraints, prerequisites, and characteristics required by this standard of ASOI as a basis for enabling fail-safe operation when the design is realized.

6.1 Design capabilities

An ASOI conforming to this standard shall be capable, when in operation, of the following:

a) Monitoring the behavior of the conforming ASOI.

b) Detecting incidents of anomalous ASOI behavior.

c) Identifying incidents of anomalous ASOI behavior with the potential to cause loss of freedom from unacceptable risk of harm.

d) Moderating ASOI behavior to preserve freedom from unacceptable risk of harm.

e) Modifying ASOI behavior to preserve freedom from unacceptable risk of harm.

f) Reporting incidents and the extent of any loss and any recovery of freedom from unacceptable risk of harm.

g) Learning from incidents.

h) Exhibiting the foregoing capabilities, to a specified extent, during operation in a specified regulatory context.

To enable these design capabilities to be incorporated into the ASOI the specification of design constraints, prerequisites and characteristics is required.

Engineering activities to specify the constraints, prerequisites, and characteristics identified in this clause should coincide with the process of eliciting requirements that define the operational capabilities of the intended ASOI, unless these activities precede such elicitation. The necessary specifications can be achieved through the application of engineering processes such as those identified in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] or alternative but comparable processes.

NOTE—Achievement of the design constraints, prerequisites and characteristics typically involves an iterative process of specification, analysis, and revision as definition of the required ASOI evolves and improves during the engineering life cycle.

6.2 Design constraints

To enable achievement of the design capabilities this standard distinguishes three fundamental *classes of systems*; individual instances of which can each form integral elements of an ASOI:

— A Safety-Critical-System (SCS).

— A Safety-Related-System (SRS).

— A Safety-Exempt-System (SXS).

One or more instances of systems in each of these classes are typically incorporated within an ASOI.

A system shall be classified as safety-critical if the system provides functions, the loss or incorrect operation of which results in unacceptable risk of harm. A system may be classified as safety-exempt if the risk of harm attributable to the system is unconditionally acceptable regardless of the operational status of the system. Safety-related systems are neither safety-critical nor safety-exempt. Such systems lie on a continuum ranging from those at the threshold of being classified as safety-exempt to those at the threshold of being classified as safety-critical.

This standard distinguishes three fundamental *categories of function*; individual instances of which can each form elements of a system integral to an ASOI:

— A Safety-Critical-Function (SCF).

— A Safety-Related-Function (SRF).

— A Safety-Exempt-Function (SXF).

Functions satisfy defined objectives of a system through action. Each category of function shares the same relationship to risk and acceptability as that of the equivalent class of system.

NOTE—Functions are system-level capabilities and are distinct from the concept of a software function that is a feature of many computer programming languages. For systems that utilize software, multiple software functions typically contribute to a single system level function. All references in this standard are to functions at the system level, unless explicitly identified as being in reference to software functions.

The provision of any Safety-Critical-Function (SCF) by an integral element (system) capable of exhibiting the Distinguishing Characteristics is not permitted if conformance to this standard is to be claimed. This exclusion is a preventive measure to assist in reducing uncertainty in respect of the behavior of safety-critical functions and systems. This exclusion is consistent with the principle of inherently safe design, as identified in 6.3 of ISO/IEC Guide 51.

The inclusion of any Safety-Critical-Function (SCF) in an instance of an integral element, irrespective of the extent of such functions, necessitates classification of the integral element as a Safety-Critical-System (SCS). No exemption to this constraint is permitted if conformance to this standard is to be claimed.

Any system that is not classified as safety-critical shall, by default, be classified as being safety-related until there is sufficient and robust evidence to validate an alternative classification.

If agreed by competent stakeholders, the default system classification may be altered to safety-critical. A default system classification of safety-exempt is not permitted if conformance to this standard is to be claimed.

Any function that is not categorized as safety-critical shall, by default, be categorized as being safety-related until there is sufficient and robust evidence to validate an alternative categorization.

If agreed by competent stakeholders, the default function categorization may be set to safety-critical. A default function categorization of safety-exempt is not permitted if conformance to this standard is to be claimed.

Competent stakeholders are responsible for establishing the necessary thresholds in respect of evidence sufficiency and robustness to enable the classification and categorization of systems and functions.

The use of the acronyms identified in 3.2 for System classes and Function categories is intended to assist human comprehension of this standard. These acronyms are not suitable for, nor intended to be incorporated into, or employed in the manufacture of an ASOI implementation. The long-form name of each class or category is suitable and intended for such uses. This limitation is applicable throughout the life cycle of an ASOI.

6.3 Design prerequisite: ASOI

To enable achievement of the design capabilities the ASOI shall be defined and recorded.

At minimum, the definition of the ASOI shall include the following:

a) The individual systems incorporated in the ASOI, with each system uniquely identified.

b) The individual functions incorporated in the ASOI, with each function uniquely identified.

c) The classification of each uniquely identified system incorporated in the ASOI.

d) The categorization of each uniquely identified function provided by the ASOI.

e) The uniquely identified system to which each uniquely identified function provided by the ASOI is allocated.

f) The uniquely identified functions provided by the ASOI that are allocated to each uniquely identified system incorporated in the ASOI.

A combination of the Distinguishing Characteristics and Key Characteristics as identified in 1.3 can be applied to define the ASOI.

There should be agreement between competent stakeholders as to an initial definition of the ASOI prior to further application of this standard to the development of a fail-safe design. Such agreement is typically subject to revision as definition of the ASOI evolves and improves during the engineering life cycle.

Identification of ASOI functions can be achieved through the application of engineering processes such as the Business or Mission Analysis (6.4.1) and Stakeholder Needs and Requirement Definition (6.4.2) processes identified in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] or alternative comparable processes.

Elaboration of the constituent functions and systems of the ASOI can be achieved through the application of engineering processes such as the System Requirements, Architecture and Design Definition processes (6.4.3, 6.4.4 and 6.4.5 respectively) identified in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] or alternative but comparable processes.

Table 1—Permitted allocations of systems and functions.

		Function Category		
		SCF	**SRF**	**SXF**
System Class	**SCS**	P	NR	NR
	SRS	NP	P	NR
	SXS	NP	NP	P

Allocation of functions shall be in accordance with the scheme shown in Table 1. Allocations that are Not Permitted are identified as NP. Permitted allocations are identified as P. Allocations identified as Not Recommended (NR) should be avoided unless individual instances of such an allocation can be justified to the satisfaction of competent stakeholders.

NOTE—The identification, elaboration, and allocation of functions to categories and systems typically involves an iterative process of revision as definition of stakeholder needs, the requirements, and the design of the ASOI evolves and improves during the engineering life cycle.

6.4 Design prerequisite: Event-Of-Interest set

To enable achievement of the design capabilities an Event-Of-Interest (EOI) set for the ASOI shall be identified and recorded.

6.4.1 Event Inclusion

At minimum, the Event-Of-Interest set shall include each of the following:

a) A uniquely identified event attributable to the ASOI that has the potential to be hazardous.

b) A uniquely identified event attributable to the ASOI that has the potential to contribute to hazardous situations through influence on, and/or interaction with, other events.

Identification of the Event-Of-Interest set shall include all known events until a justification for exclusion of an event is approved by competent stakeholders. The total loss of function of the ASOI shall be included as an event that is of interest. Consideration shall also be given to whether the total physical loss of the ASOI represents a separate event: if such loss is possible.

Where possible, established safety engineering practices should be employed to derive the Event-Of-Interest set. In addition to the application of relevant analytical approaches, information, and knowledge employed during derivation of the Event-Of-Interest set should include, but not be limited to, the sources identified in 7.3.1 in ISO/IEC Guide 51.

Causal factors for events can be intrinsic to the ASOI itself, the environment in which the ASOI operates, or a combination of both. Consideration should be given to potential follow-on effects.

6.4.2 Event Information

At minimum, the following information for each event that is of interest shall be recorded:

a) A unique identifier for the event

b) The Time-To-Recovery

c) The Time-To-Violation

d) The Time-To-Harm

e) The criticality of the event

For the EOI set an absolute minimum value of Time-To-Violation shall be identified. This is the absolute minimum Time-To-Violation value for all the events in the EOI set.

The absolute minimum value of Time-To-Violation provides a basis for the temporal considerations necessary to fulfill the baseline system requirements identified in Annex A.

Event criticality can be specified quantitatively or qualitatively taking account of established engineering practice in this respect if such practice exists. In the absence of applicable practice competent stakeholders should inform themselves of candidate schemes for specifying criticality by examining proven schemes applied in comparable or adjacent domains; regardless of whether these schemes apply to autonomous systems or not.

NOTE—Specification of the EOI set, and the information required for each event typically involves an iterative process of identification, analysis, and revision as definition of stakeholder needs, and the requirements, architecture, and design of the ASOI evolve and improve during the engineering life cycle.

6.5 Design characteristics: Minimum thresholds for design capabilities

To enable achievement of the design capabilities a set of minimum thresholds for the ASOI shall be specified for the following:

a) The likelihood of incidents of anomalous ASOI behavior being detected by the ASOI.

b) The likelihood of incidents of anomalous ASOI behavior with the potential to cause loss of freedom from unacceptable risk of harm being identified by the ASOI.

c) The likelihood of the ASOI moderating behavior to preserve freedom from unacceptable risk of harm.

d) The likelihood of the ASOI modifying behavior to preserve freedom from unacceptable risk of harm.

e) The likelihood of the ASOI reporting incidents of anomalous behavior and the extent of any loss and any recovery of freedom from unacceptable risk of harm.

f) The likelihood of the ASOI learning from incidents of anomalous behavior.

Each of the foregoing minimum thresholds a) through f) shall be calculated for a specified interval of time. All calculations of the minimum thresholds a) through f) shall employ the same specified interval of time. The onset of this interval shall either be assumed to coincide with the onset of anomalous ASOI behavior or, alternatively, be assumed to precede the onset of anomalous ASOI behavior by a specified invariant amount of time. Regardless of the option selected the onset of the required interval of time shall not be later than the onset of anomalous ASOI behavior.

Competent stakeholders are responsible for specifying the information required to set the minimum thresholds a) through f).

There should be agreement between competent stakeholders as to initial minimum thresholds and the specified interval duration prior to further application of this standard to the development of a fail-safe design. Specification of the means of verifying achievement of the minimum thresholds during operation of the ASOI should also be agreed in accordance with Clause 9 of this standard.

When in operation, achievement by the ASOI of the minimum thresholds a) through f), without exception, is necessary if conformance to this standard is to be claimed.

NOTE 1—The minimum thresholds a) through f) form the basis for the Design Capabilities specifications identified in 6.1. This basis includes the temporal considerations identified in this clause.

NOTE 2—The onset of ASOI anomalous behavior is typically preceded by, rather than being, coincident with the leading edge of the initiating event or events that are the cause of the anomalous behavior.

NOTE 3—Specification of the necessary minimum thresholds for design capabilities typically involves an iterative process of analysis and revision as definition of stakeholder needs and the requirements, architecture, and design of the ASOI evolve and improve during the engineering life cycle.

7. Regulatory awareness process

7.1 Purpose

The purpose of the regulatory awareness process is to incorporate into the design of an ASOI a capability for fail-safe operation in an identified regulatory context.

The scope of regulatory awareness required by this process is limited to fail-safe aspects of operation. Though the regulatory context for an ASOI typically extends significantly beyond fail-safe capabilities such extensions are not addressed by this standard.

Initiation of this process should commence no later than the elicitation of requirements that define the operational capabilities of the intended ASOI. Conformance to this process is required throughout the life cycle of the ASOI. Accordingly, this process extends from the inception of the ASOI until the final and irrevocable disposal of the ASOI after removal from operation. Termination of this process is only possible following completion of these activities. The requirement for conformance through life does not preclude claims of conformance in accordance with Clause 4 being made prior to such disposal, nor necessarily invalidate any such claims that are made.

NOTE 1—The Disposal process (6.4.14) in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] identifies outcomes expected of a disposal process of a system.

As required by this process, a *plan* can comprise multiple information items produced and thereafter revised as necessary throughout the life cycle of the ASOI. It is not necessary that a plan be constrained to a single information item and be maintained as such. Augmentation of information items required by established systems safety engineering and/or systems engineering practice can contribute to achieving the outcomes of this process. In such instances competent stakeholders are responsible for determining whether the resulting augmentation is sufficient to claim conformance to this process without the need to produce additional information items that address planning considerations of relevance to this process.

NOTE 2—The Project Planning process (6.3.1) in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] identifies outcomes expected of planning throughout the life cycle of a project (ASOI).

7.2 Outcomes

The following outcomes are a result of the successful implementation of the regulatory awareness process:

a) The ASOI to be regulated is identified.

b) The regulatory context within which the ASOI is to operate is identified.

c) Regulatory requirements for ASOI fail-safe operation in the regulatory context are identified.

d) Information and evidential requirements for the regulatory context of an ASOI are identified.

e) A plan for an ASOI design capable of fail-safe operation within the regulatory context is defined.

f) A plan for an ASOI design capable of fail-safe operation within the regulatory context is validated.

g) A validated plan for an ASOI design capable of fail-safe operation within the regulatory context is implemented.

h) The implementation of a validated plan for an ASOI design capable of fail-safe operation within the regulatory context is verified.

i) The validity of the plan for an ASOI design capable of fail-safe operation within the regulatory context is maintained throughout the life cycle of the ASOI.

NOTE—The Maintenance process (6.4.13) in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] identifies outcomes expected of a maintenance process for a system.

7.3 Activities and tasks

Adopters of this standard shall implement the following activities and tasks in accordance with the regulatory awareness process (this process).

a) **Identify the ASOI to be regulated (RAP1).** This activity consists of the following tasks:

1) Stakeholders of the intended ASOI are identified.

2) Stakeholder needs in respect of the intended ASOI are defined.

3) The ASOI is identified.

NOTE 1—Stakeholder needs are addressed by the Stakeholder Needs and Requirements Definition processes (6.4.2) in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3]. Account should also be taken of the Operation process (6.4.12), outcome (a) in particular.

NOTE 2—Completion of task 3 of this activity (RAP1) is dependent upon achievement of the ASOI design prerequisite identified in 6.3.

b) **Identify the ASOI regulatory context (RAP2).** This activity consists of the following tasks:

1) Competent stakeholders authorized to specify a regulatory context for an ASOI are identified.

2) The regulatory context for the ASOI is agreed upon by stakeholders.

3) Specifications necessary to define the regulatory context are identified.

NOTE 1—Specifications defining necessary behaviors for ASOI should be agreed with competent stakeholders authorized to specify the regulatory context.

NOTE 2—Specifications defining incident reporting criteria for ASOI should be agreed with competent stakeholders authorized to specify the regulatory context. At minimum, these specifications should identify criteria for incident identification, the recording, and the reporting of individual incidents.

NOTE 3—Specifications defining necessary learning criteria for ASOI should be agreed with competent stakeholders authorized to specify the regulatory context.

NOTE 4—Identification of the regulatory context should include any cross-jurisdictional or regulatory alignment considerations or equivalent that it is necessary to account for in respect of ASOI operation.

c) **Identify regulatory design requirements (RAP3).** This activity consists of the following tasks:

1) Regulatory requirements to be fulfilled by the design of an ASOI are identified.

2) The conditions and constraints associated with the identified regulatory requirements are identified.

NOTE 1—ISO/IEC/IEEE 29148 [B12] addresses the treatment of requirements during the engineering life cycle.

NOTE 2—The regulatory requirements can include any specifications defining the regulatory context identified on completion of task 3 of this activity (RAP3).

d) **Identify regulatory information and evidential requirements (RAP4).** This activity consists of the following tasks:

1) Regulatory requirements to be fulfilled by the provision of information relating to an ASOI are identified.

2) Regulatory requirements to be fulfilled by the provision of evidence relating to an ASOI are identified.

NOTE 1—ISO/IEC/IEEE 15289 [B8] provides examples of the types of information item and constituent elements that can be relevant throughout the engineering life cycle.

NOTE 2—Evidential requirements should specify the evidence required in respect of an Assurance Case or equivalent, as a basis for claims of conformance to this standard as identified in Clause 4.

e) **Validate a plan for an ASOI design capable of fail-safe operation in an identified regulatory context (RAP5).** This activity consists of the following tasks:

1) A plan for an ASOI design capable of fail-safe operation in an identified regulatory context is defined.

2) The plan is reviewed by competent stakeholders.

3) The plan is revised, as necessary.

4) The plan is approved by authorized and competent stakeholders.

NOTE—Validation provides confirmation, through objective evidence, that the requirements for an intended use have been fulfilled thereby providing an answer to the question of whether the right product (ASOI) has been built. Validation considerations can be addressed through the application of the Validation process (6.4.11) identified in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] or alternative but comparable processes.

f) **Implement the validated plan for an ASOI design capable of fail-safe operation in an identified regulatory context (RAP6).** This activity consists of the following tasks:

1) A validated plan for an ASOI design capable of fail-safe operation is integrated into processes to be applied throughout the life cycle of the ASOI.

2) Information requirements identified in the validated plan are fulfilled.

3) Evidential requirements identified in the validated plan are fulfilled.

g) **Verify the implementation of the validated plan for an ASOI design capable of fail-safe operation in an identified regulatory context (RAP7).** This activity consists of the following tasks:

1) Fulfillment of all identified design constraints, prerequisites, and characteristics is verified.

2) Fulfillment of all identified information requirements is verified.

3) Fulfillment of all identified evidential requirements is verified.

NOTE—The EOI set defined in 6.4 shall include events relating to the total or partial loss of capabilities necessary to conform to this (Regulatory Awareness) process. Such inclusion shall extend to the partial or total loss of stakeholder contributions to the achievement of the outcomes of this process.

h) **Maintain the validity of the plan for an ASOI design capable of fail-safe operation in an identified regulatory context throughout the life cycle of the ASOI (RAP8).** This activity consists of the following tasks:

1) The regulatory context is monitored throughout the life cycle of the ASOI.

2) The plan is revised as necessary to maintain validity.

3) The Regulatory Awareness Process (this process) is invoked as necessary.

4) Revised behavior specifications are incorporated into the ASOI as necessary.

NOTE—Task 3 of this activity (RAP8) is intentionally recursive.

8. Fail-safe design in operation process

8.1 Purpose

The purpose of the fail-safe design in operation process is to incorporate into the design of an ASOI a capability to preserve freedom from unacceptable risk of harm in the event of failure of the ASOI during operation.

The scope of this process is limited to fail-safe aspects of the realized ASOI design, when in operation. Considerations of the operational context beyond those necessary to preserve freedom from unacceptable risk of harm in the event of failure of the ASOI are not addressed by this standard.

NOTE—The Operation process (6.4.12) in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3] identifies outcomes expected of an operation process for a system.

8.2 Outcomes

The following outcomes are a result of the successful implementation of the fail-safe design in operation process; in accordance with the Design Constraints, Prerequisites, and Characteristics defined in Clause 6:

a) The behavior of the ASOI is monitored.

b) Incidents of anomalous behavior attributable to the ASOI are detected.

c) Incidents of anomalous ASOI behavior with the potential to cause loss of freedom from unacceptable risk of harm are identified.

d) As necessary, ASOI behavior is moderated for the purpose of preserving freedom from unacceptable risk of harm.

e) As necessary, ASOI behavior is modified for the purpose of preserving freedom from unacceptable risk of harm.

f) The extent to which any loss of freedom from unacceptable risk of harm is recovered by the ASOI is evaluated.

g) Incidents of anomalous behaviors, the extents of any loss and any recovery from loss of freedom from unacceptable risk of harm are reported by the ASOI.

h) The ASOI learns from incidents for the purpose of preserving freedom from risk of unacceptable harm.

8.3 Activities and tasks

The ASOI shall implement the following activities and tasks in accordance with the fail-safe design in operation process (this process), the Design Constraints, Prerequisites, and Characteristics defined in Clause 6.

a) **Monitor behavior (DIOP1)**. This activity consists of the following tasks:

   1) The ASOI monitors ASOI behavior.

   2) The ASOI issues periodic requests to continue execution.

b) **Detect incidents of anomalous behavior (DIOP2).** This activity consists of the following tasks:

   1) The ASOI detects behavioral anomalies.

   2) The ASOI verifies specified behaviors.

c) **Diagnose incidents of anomalous behavior (DIOP3).** This activity consists of the following tasks:

1) The ASOI identifies behavioral anomalies with the potential to cause a loss of freedom from unacceptable risk of harm.

2) The ASOI labels identified behavioral anomalies as deviations.

3) The ASOI identifies the root causes of deviations.

4) The ASOI calculates the confidence level in the identification of the root causes of deviations.

5) The ASOI calculates deviation criticality.

6) The ASOI calculates a target recovery threshold for freedom from unacceptable risk of harm.

7) The ASOI reports:

i) Behavioral anomalies detected.

ii) Behavioral anomalies labelled as deviations.

iii) The calculated criticality of each deviation.

iv) The calculated confidence level for each deviation.

v) The calculated target recovery threshold for the ASOI.

8) The ASOI issues a request to continue execution.

NOTE—In the context of this process all behavioral anomalies labelled as deviations are negative (entail actual loss or the potential for such loss).

d) **Moderate behavior (DIOP4).** This activity consists of the following tasks:

1) The ASOI identifies moderating behaviors capable of preserving freedom from unacceptable risk of harm.

2) The ASOI selects moderating responses.

3) The ASOI initiates the selected moderating responses.

4) The ASOI evaluates the extent of freedom from unacceptable risk of harm.

5) The ASOI reports the extent of deviations.

6) The ASOI decides whether to issue a request to continue execution.

7) The ASOI issues an optional request to continue execution.

NOTE—The need to execute task 7 is determined by completion of task 6 when conducting this activity (DIOP4).

e) **Modify behavior (DIOP5).** This activity consists of the following tasks:

1) The ASOI identifies modifying behaviors capable of preserving freedom from unacceptable risk of harm.

2) The ASOI selects behavioral modifications.

3) The ASOI initiates selected behavioral modifications.

4) The ASOI evaluates the extent to which freedom from unacceptable risk of harm is acceptable.

5) The ASOI decides whether to issue a request to continue execution.

6) The ASOI issues an optional request to continue execution.

NOTE—The need to execute task 6 is determined by completion of task 5 when conducting this activity (DIOP5).

f) **Evaluate the extent of freedom from unacceptable risk of harm (DIOP6).** This activity consists of the following tasks:

1) The ASOI evaluates the extent to which freedom from unacceptable risk of harm is acceptable.

2) The ASOI decides whether to issue a request to continue execution.

3) The ASOI issues an optional request to continue execution.

NOTE—The need to execute task 3 is determined by completion of task 2 when conducting this activity (DIOP6).

g) **Report an incident (DIOP7).** This activity consists of the following tasks:

1) The ASOI reports the incident.

2) The ASOI reports the moderating responses initiated.

3) The ASOI reports the behavioral modifications initiated.

4) The ASOI reports the extent of freedom from unacceptable risk of harm.

5) The ASOI issues a request to continue execution.

h) **Learn from incident (DIOP8).** This activity consists of the following tasks:

1) The ASOI identifies any changes in behavior to be learned from an incident.

2) The ASOI identifies any changes to behavior specifications necessitated by the identified behavior changes to be learned.

3) The ASOI identifies any consequential changes to behavior limits necessitated by the identified behavior changes to be learned.

4) The ASOI validates the identified changes to behavior specifications and resultant changes to behavior limits that are necessary.

5) The ASOI incorporates validated changes to behavior specifications and resultant changes to behavior limits that are necessary.

NOTE—This activity (DIOP8) is typically achieved iteratively to enable the ASOI to respond to instances of changes to behavior specifications that are determined to be invalid.

9. Verification

9.1 Scope of verification

Consideration of verification in this standard is limited to that required to verify the fail-safe capabilities of the ASOI. Verification of other capabilities of an ASOI is not within the scope of this standard.

9.2 Property-of-interest

This standard utilizes the concept of *property-of-interest* identified in ISO/IEC/IEEE 15026-1 [B4] as the basis for verification. To fulfill the baseline ASOI System Requirements identified in Annex A it is necessary that the implementation incorporated in the ASOI can be characterized by each property-of-interest identified in this clause to a specified extent for specified requirements. The realization of an ASOI design becomes less capable of failing safely when the extent to which the realization achieves a required property-of-interest is diminished relative to the extent specified as being necessary to preserve safety. Ultimately, any ASOI design, as realized, becomes incapable of failing safely if the discrepancy between the actual extent of a property-of-interest achieved by the realization and that specified by the design becomes excessive.

NOTE—What constitutes excessive is determined by the context of the specific application of an ASOI and hence is a consideration to be addressed by competent stakeholders.

A property-of-interest comprises one or more *attributes*.

To claim conformance to this standard the conforming ASOI shall exhibit the following properties-of-interest:

a) In accordance with the System Requirements specified in Annex A.

b) In accordance with the properties-of-interest and constituent attributes identified in 9.4.

c) To an extent determined and agreed upon by competent stakeholders.

d) Under conditions determined and agreed by competent stakeholders.

9.3 Property-of-interest specification

Each property-of-interest in this standard is specified by the following elements:

a) The title of the property-of-interest.

b) A statement defining the property-of-interest.

c) The reference source of element b).

d) The following for each constituent attribute required for the property-of-interest:

   1) The title of the attribute.

   2) A statement defining the attribute required.

   3) The reference source of element 2) for the attribute.

NOTE—Reference can be made to ISO/IEC/IEEE 15289 [B8] for further details of the elements required for the description of a Specification.

9.4 Baseline properties

The properties identified in this subclause constitute the baseline set required to enable claims of conformance to this standard. No conformance to this standard can be claimed if any property-of-interest or constituent attribute identified in this subclause is removed.

a) **Dependability:** ability to perform as and when required (IEC 60050-192 ed 1.0 [B1]).[15]

   The minimum attributes required for this property are the following:

   1) **Availability:** ability to be in a state to perform as required (IEC 60050-192 ed 1.0 [B1]).[15]

   2) **Maintainability:** ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance (IEC 60050-192 ed 1.0 [B1]).[15]

   3) **Reliability:** ability to perform as required, without failure, for a given time interval, under given conditions (IEC 60050-192 ed 1.0 [B1]).[15]

   4) **Robustness:** the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions (ISO/IEC/IEEE 24765 [B10]).

By agreement between competent stakeholders, element b) of the specification for the Dependability property-of-interest (9.3) may be amended or substituted to enable the adoption of an alternative, but comparable statement to define the Dependability property-of-interest.

[15]IEC 60050-192 ed.1.0 [B1], Copyright © 2015 IEC Geneva, Switzerland: www.iec.ch.

By agreement between competent stakeholders, element 2) of the specification for the Dependability property-of-interest (9.3) may be amended or substituted to enable the adoption of alternative, but comparable statements to define individual constituent attributes of the Dependability property-of-interest.

An alternative statement in respect of either element b) or 2) from 9.3 can be considered comparable if there is credible evidence that the alternative statement is widely recognized and understood by competent stakeholders to be a substitute for the statement provided in this standard. A narrow or specialized statement that cannot obviously be associated with, or easily recognized and comprehended to be an alternative statement would not satisfy this test of equivalence.

No other alteration to the specification for this property-of-interest is permitted if conformance to this standard is to be claimed.

By agreement between competent stakeholders, additional attributes may be specified for this property-of-interest.

b) **Predictability:** the ability to facilitate accurate estimation of the likelihood of specified events in the future. (This standard is the reference source for this property-of-interest).

   The minimum attribute required for this property is:

   1) **Temporal predictability:** the ability to facilitate accurate estimation of the time of occurrence of specified events in the future. (This standard is the reference source for this attribute).

By agreement between competent stakeholders, additional attributes may be specified for this property-of-interest. No further alteration to the specification for this property-of-interest is permitted if conformance to this standard is to be claimed.

9.5 Means of verification

This standard does not assume, establish, nor require the application of any technique, method, methodologies or equivalent as a means of verifying the extent to which solutions are characterized by each required property-of-interest. Competent stakeholders are responsible for the selection and agreement of means of verification that are appropriate for the application of this standard.

NOTE—Reference can be made to ISO/IEC/IEEE 29148:2018 (6.5.2) [B12] for further information regarding standard verification methods employed to obtain objective evidence that requirements have been fulfilled.

9.6 Additional properties

If competent stakeholders agree to the introduction of any additional property-of-interest, at minimum, the specification of each such property-of-interest shall be in accordance with the Property-of-interest specification identified in 9.3.

Annex A

(normative)

Baseline ASOI System Requirements

A.1 Introduction

This annex identifies a baseline set of System Requirements that an ASOI conforming to this standard shall fulfill. These requirements are additional to the functional and non-functional requirements specified by stakeholders when defining the ASOI. The set of requirements identified in this annex can be employed as the basis for elaborating derived requirements suitable for specifying the lower-level details of the fail-safe capabilities required of the ASOI realization.

Conformance to this standard cannot be claimed if any of the requirements identified in this annex are removed, amended, substituted, or otherwise transformed except for purposes of eliciting derived (child) requirements.

A.2 Additional baseline system requirements

By agreement, competent stakeholders may specify additional baseline System Requirements. Such requirements shall include, at minimum, the following *requirement attributes*:

a) Requirement unique identifier.

b) A statement of the requirement.

c) The rationale for the requirement.

d) Enumerated statements of applicable conditions.

e) Enumerated statements of applicable constraints.

f) Enumerated properties-of-interest for the purpose of verification.

NOTE 1—ISO/IEC/IEEE 29148 [B12] can be consulted for an elaboration upon the requirements engineering processes identified in ISO/IEC/IEEE 15288 [B7] and ISO/IEC/IEEE 12207 [B3].

NOTE 2—Requirement attributes constitute an integral element of a well-formed requirement. Refer to 5.2.8 of ISO/IEC/IEEE 29148:2018 [B12].

A.3 System Requirements

Unique Identifier	7009-ASR-001
Statement	The ASOI shall incorporate functions by designated category.
Rationale	This requirement addresses the incorporation in conforming ASOI of means to realize the design constraints identified in 6.2.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	Categories comprise: (a) Safety-Critical Function (SCF), (b) Safety-Related Function (SRF), (c) Safety Exempt Function (SXF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-002
Statement	The ASOI shall provide means to maintain separation between each category (a, b, c) of function.
Rationale	Separation facilitates differentiation between each category of function that is integral to an ASOI. This requirement contributes to preventing unintended interference between categories of function. The prevention of such interference is necessary to realize the design capabilities identified in 6.1 and the design characteristics identified in 6.5.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 2	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-003
Statement	The ASOI shall provide means to maintain isolation between each category (a, b, c) of function.
Rationale	Isolation facilitates limitations on the extent to which the behaviour of a function in one category can be determined by a function in another category: if any such limitations are necessary. This requirement contributes to preventing unintended interference between categories of functions. The prevention of such interference is necessary to realize the design capabilities identified in 6.1 and the design characteristics identified in 6.5.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 2	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-004
Statement	The ASOI shall incorporate means of inhibiting execution of individual safety-related functions (SRF).
Rationale	This requirement addresses the incorporation in conforming ASOI of means to realize the behavioral aspects of the design capabilities identified in 6.1 in accordance with the design characteristics identified in 6.5. This requirement addresses the realization that is necessary in respect of safety-related functions.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	Fulfilment of this requirement is limited to ASOI capabilities provided by safety-critical functions (SCF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-005
Statement	The ASOI shall incorporate means of inhibiting execution of individual safety-exempt functions (SXF).
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize the behavioral aspects of the design capabilities identified in 6.1 in accordance with the design characteristics identified in 6.5. This requirement addresses the realization that is necessary in respect of safety-exempt functions.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	Fulfilment of this requirement is limited to ASOI capabilities provided by safety-critical functions (SCF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-006
Statement	The ASOI shall incorporate means of inhibiting execution of all safety-related functions (SRF) at regular intervals of time.
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize the design capabilities identified in 6.1 in accordance with the temporal aspects of the design characteristics identified in 6.5. This requirement addresses the realization that is necessary in respect of safety-related functions.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	Fulfilment of this requirement is limited to ASOI capabilities provided by safety-critical functions (SCF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability
Property-of-interest 2	Predictability

Unique Identifier	7009-ASR-007
Statement	The ASOI shall incorporate means of inhibiting execution of all safety-exempt functions (SXF) at regular intervals of time.
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize the design capabilities identified in 6.1 in accordance with the temporal aspects of the design characteristics identified in 6.5. This requirement addresses the realization that is necessary in respect of safety-exempt functions.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	Fulfilment of this requirement is limited to ASOI capabilities provided by safety-critical functions (SCF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability
Property-of-interest 2	Predictability

Unique Identifier	7009-ASR-008
Statement	The ASOI shall incorporate means of requesting authorization to execute specified functions.
Rationale	This requirement enables the incorporation in conforming ASOI of means to achieve the outcomes identified in Clause 8.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	ASOI functions that can be specified are limited to those categorized as safety-related (SRF) or safety-exempt (SXF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-009
Statement	The ASOI shall incorporate means of inhibiting the execution of specified functions in the event that no authorization to continue execution of the specified functions is available to the ASOI.
Rationale	This requirement enables the incorporation in conforming ASOI of means to achieve the outcomes identified in Clause 8.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	ASOI functions that can be specified are limited to those categorized as safety-related (SRF) or safety-exempt (SXF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-010
Statement	The ASOI shall incorporate means of inhibiting specified functions in the event that the necessary authorization to execute the specified functions becomes invalid.
Rationale	This requirement enables the incorporation in conforming ASOI of means to achieve the outcomes identified in Clause 8.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	ASOI functions that can be specified are limited to those categorized as safety-related (SRF) or safety-exempt (SXF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-011
Statement	The ASOI shall incorporate means of inhibiting the execution of specified functions in the event that no authorization to execute the specified functions is available to the ASOI.
Rationale	This requirement enables the incorporation in conforming ASOI of means to achieve the outcomes identified in Clause 8.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	ASOI functions that can be specified are limited to those categorized as safety-related (SRF) or safety-exempt (SXF).
Constraint 2	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 3	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-012
Statement	The ASOI shall incorporate means of detecting violations of the specified limits of ASOI behavior.
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize design capabilities (b) and (c) identified in 6.1.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 2	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-013
Statement	The ASOI shall incorporate means of inhibiting safety-related functions (SRF) that are in violation of the specified limits of ASOI behavior.
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize design capability (d) identified in 6.1.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 2	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-014
Statement	The ASOI shall incorporate means of inhibiting safety-exempt functions (SXF) that are in violation of the specified limits of ASOI behavior.
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize design capability (d) identified in 6.1.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 2	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-015
Statement	The ASOI shall incorporate means of inhibiting the execution of safety-related functions (SRF) in the event that such execution would violate the specified limits of ASOI behavior.
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize design capability (d) identified in 6.1.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 2	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Unique Identifier	7009-ASR-016
Statement	The ASOI shall incorporate means of inhibiting the execution of safety-exempt functions (SXF) in the event that such execution would violate the specified limits of ASOI behavior.
Rationale	This requirement enables the incorporation in conforming ASOI of means to realize design capability (d) identified in 6.1.
Condition 1	This requirement applies whenever the ASOI is capable of exhibiting the Distinguishing Characteristics.
Constraint 1	When Condition 1 applies, the total loss of the ASOI capability fulfilling this requirement is a failure event.
Constraint 2	When Condition 1 applies, a partial loss of the ASOI capability fulfilling this requirement is a failure event: irrespective of the extent of loss of the capability.
Property-of-interest 1	Dependability

Annex B

(informative)

Procedural interpretation of the fail-safe design in operation process

The ordering of Outcomes and the Activities and Tasks in Clause 8 reflects the design capabilities and characteristics defined in Clause 6. This ordering corresponds to the sequence of activities that are necessary following detection of incidents of anomalous behavior.

The sequence of Activities and Tasks identified in Clause 8 provide the basis for a procedural approach to achieve the outcomes defined in that clause. If such an approach is adopted by an ASOI design then the sequence of activities, and hence tasks, shall be as identified below.

Step	Label	Activity
1	DIOP1	Monitor behavior.
2	DIOP2	Detect anomalous behavior.
3	DIOP3	Diagnose incidents of anomalous behavior.
4	DIOP4	Moderate behavior as necessary.
5	DIOP5	Modify behavior as necessary.
6	DIOP6	Evaluate behavior.
7	DIOP7	Report incidents.
8	DIOP8	Learn from incidents.

NOTE—This procedural interpretation of the Activities and Tasks defined in Clause 8 addresses the recommendation in respect of sequencing constraints identified in 5.4.2 of ISO/IEC/IEEE 24774:2021 [B11].

Annex C

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] IEC 60050-192 International Electrotechnical Vocabulary—Part 192: Dependability.[16]

[B2] IEC/IEEE 82079-1, Preparation of information for use (instructions for use) of products—Part 1: Principles and general requirements.

[B3] ISO/IEC/IEEE 12207, Systems and software engineering—Software life cycle processes.

[B4] ISO/IEC/IEEE 15026-1, Systems and software engineering—Systems and software assurance—Part 1: Concepts and vocabulary.

[B5] ISO/IEC/IEEE 15026-2, Systems and software engineering—Systems and software assurance—Part 2: Assurance case.

[B6] ISO/IEC/IEEE 15026-4, Systems and software engineering—Systems and software assurance—Part 4: Assurance in the life cycle.

[B7] ISO/IEC/IEEE 15288, Systems and software engineering—System life cycle processes.

[B8] ISO/IEC/IEEE 15289, Systems and software engineering—Content of life-cycle information items (documentation).

[B9] ISO/IEC/IEEE 16085, Systems and software engineering—Life cycle processes—Risk management.

[B10] ISO/IEC/IEEE 24765, Systems and software engineering—Vocabulary.

[B11] ISO/IEC/IEEE 24774, Systems and software engineering—Life cycle management—Specification for process description.

[B12] ISO/IEC/IEEE 29148, Systems and software engineering—Life cycle process—Requirements engineering.

[B13] ISO 9001:2015, Quality management systems—Requirements.

[16]IEC publications are available from the International Electrotechnical Commission (https://www.iec.ch) and the American National Standards Institute (https://www.ansi.org/).

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE