



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

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

STANDARDS

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

Recognized as an American National Standard

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

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 5 July 2024. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

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

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

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

¹Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

²Available 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.

³Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴Available 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.

⁵Available 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 Pisssoort

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 Pisssoort
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

1. Overview	11
1.1 Scope	11
1.2 Word usage	11
1.3 Field of application	11
1.4 Audience	13
1.5 Competency considerations	14
1.6 Regulatory considerations	14
1.7 Relationship to systems safety engineering life cycles	14
1.8 Relationship to systems and software engineering life cycles	15
1.9 Limitations	15
1.10 Disclaimer	15
2. Normative references	16
3. Definitions, acronyms, and abbreviations	16
3.1 Definitions	16
3.2 Acronyms and abbreviations	18
4. Conformance	19
5. Key concepts	19
5.1 Safety and fail-safe design	20
5.2 Risk	20
5.3 Unacceptable risk and residual risk	20
5.4 Hazardous events and situations	21
5.5 Events involving failure	21
5.6 Behavior and performance	21
5.7 Anomalous behavior	21
5.8 Temporal considerations	22
6. Fail-safe design capabilities, constraints, prerequisites, and characteristics	23
6.1 Design capabilities	23
6.2 Design constraints	23
6.3 Design prerequisite: ASOI	25
6.4 Design prerequisite: Event-Of-Interest set	26
6.5 Design characteristics: Minimum thresholds for design capabilities	27
7. Regulatory awareness process	28
7.1 Purpose	28
7.2 Outcomes	28
7.3 Activities and tasks	29
8. Fail-safe design in operation process	31
8.1 Purpose	31
8.2 Outcomes	31
8.3 Activities and tasks	31
9. Verification	33
9.1 Scope of verification	33
9.2 Property-of-interest	33
9.3 Property-of-interest specification	34
9.4 Baseline properties	34
9.5 Means of verification	35
9.6 Additional properties	35

Annex A (normative) Baseline ASOI System Requirements 36

Annex B (informative) Procedural interpretation of the fail-safe design in operation process 42

Annex C (informative) Bibliography 43

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.

⁶The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁷The 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.

⁸The numbers in brackets correspond to those of the bibliography in Annex C.

⁹Notes 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.