



FUNCTIONAL SAFETY STANDARDS COMMITTEE

THE FUNCTIONAL SAFETY TERMINOLOGY LANDSCAPE

Authored by

Functional Safety Standards Committee White Paper Working Group

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

ACKNOWLEDGMENTS

Special thanks are given to all the members of FSSC White Paper Working Group. The following members contributed to this document:

Tali Arbel-Newman
Jyotika Athavale
Rohitaswa Bhattacharya
Rajiv Bongiwar
Wei-Ren Chen
Mike Diaz

Luca Di Mauro
Carolina Di Napoli
Darren Galpin
Sagar Kasrung
Veit Kleeberger
Stefano Lorenzini
Riccardo Mariani

Avi Patel
Hana Ptackova
Federico Reghenzani
Rob Schaaf
Max Turner
Baptiste Vignasse

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

Copyright © 2023 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 30 January 2023. Printed in the United States of America.

PDF: STDVA25917 978-1-5044-9383-3

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/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.

Find IEEE standards and standards-related product listings at: <http://standards.ieee.org>.

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA DOCUMENTS

This IEEE Standards Association (“IEEE SA”) publication (“Work”) is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the activity that produced this Work. IEEE and the FSSC SG expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the FSSC SG disclaim any and all conditions relating to: results; and workmanlike effort. This document is supplied “AS IS” and “WITH ALL FAULTS.”

Although the FSSC SG members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE-SA OR ICAP MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF 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 USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users 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. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder.

This Work is published with the understanding that IEEE and the FSSC SG members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

ABSTRACT.....	5
1. THE EXISTING LANDSCAPE	6
1.1. MOTIVATION.....	6
1.2. BASIC, GENERIC, AND SPECIFIC STANDARDS.....	6
1.3. ABOUT DIFFERENCES BETWEEN STANDARDS.....	7
1.3.1. EXAMPLE OF HOUSEHOLD APPLIANCES	7
1.3.2. TOPICS BASED STANDARDS CLASSIFICATION.....	9
1.4. THE DEFINITIONS CHALLENGE	11
2. THE TERMS.....	11
2.1. SYSTEM	11
2.2. SCOPE	12
2.3. SAFETY	13
2.4. SAFE-STATE	13
2.5. FAIL-OPERATIONAL	14
2.6. FAIL-DEGRADED	14
2.7. FAIL-SAFE.....	14
2.8. FAIL-UNSAFE	15
2.9. FAULT	15
2.10. FAILURE.....	16
2.11. RISK.....	17
2.11.1. RESIDUAL RISK	18
2.11.2. UNREASONABLE RISK	18
2.11.3. TOLERABLE RISK	18
2.12. LEVEL OF RIGOR.....	19
2.13. HAZARD.....	19
2.14. ELEMENT	20
2.15. ITEM	20
2.16. ERROR.....	21
2.17. RELIABILITY	21
2.18. AVAILABILITY	22
2.19. RECOVERABILITY	23
2.20. DEPENDABILITY.....	24
2.21. EQUIPMENT UNDER CONTROL	24
3. CONCLUSIONS.....	25
4. REFERENCES.....	25

THE FUNCTIONAL SAFETY TERMINOLOGY LANDSCAPE

ABSTRACT

This white paper, developed by the Functional Safety Standards Committee (FSSC), describes the landscape of functional safety terminology as used across multiple domains. It has been observed that there are multiple definitions for many of the terms—some of which are domain specific—and there is often an assumption that the terms are commonly understood. Some of the definitions have key differences, which could lead engineers to misunderstanding if they apply a definition that is used in one domain to another.

This white paper takes an overview of the existing landscape and establishes a subset of terminology for use in future standards sponsored by the FSSC. It discusses the different understandings of the terminologies used and where they differ and defines a single understanding of the terminology for future use. If the context of a future standard requires a deviation from the definition in this document, then the deviation should be explicitly marked and defined and should be flagged to the FSSC for consideration in future revisions of this document.

1. THE EXISTING LANDSCAPE

1.1. MOTIVATION

During the April 2022 International Quality & Productivity Center (IQPC) conference Application of ISO 26262 to Semiconductor, it was noted that there were more than 230 standards associated with connected automotive vehicles alone [1], and there are other standards that could apply, depending on how a domain is viewed. For example, with cars gaining increasingly complex automated driving features, should robotics standards also be applied to the automotive domain? With the re-use of Intellectual Property (IP) across multiple domains common practice, there is a need to standardize terms to help ensure a commonality of understanding. This is not helped by a multiplicity of standards organizations—each with different memberships—developing standards in parallel.

Safety overall is defined as the freedom from unacceptable risk of physical injury. Safety is articulated in various ways, depending on the specific safety risk:

- *System safety* follows a risk management strategy based on identification, analysis of hazards and application of remedial controls using a systems-based approach.
- *Functional safety* is the part of the overall safety relating to the Equipment Under Control (EUC) and its control system, which depends on the correct functioning of the electrical and electronic safety-related systems, other technology safety-related systems and external risk reduction facilities.
- *Safety Of The Intended Functionality* (SOTIF) is the absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons.

1.2. BASIC, GENERIC, AND SPECIFIC STANDARDS

A summary of important standards covering functional safety topics by different standards development organizations (SDOs) can be seen in TABLE 1. In this table, the standards are classified according to the following:

- Basic standards that give basic concepts, principles for design, and general aspects that are applicable to a certain domain.
- Generic standards that deal with one safety aspect or one type of safety device that can be used across a wide range of applications.
- Specific standards that handle detailed safety guidelines for a particular application.

TABLE 1 Functional Safety Standards Landscape

	IEEE	ISO	IEC	Others
Specific	IEEE P2817	ISO 23374 ISO 23792 ISO 23793 ISO 22737	IEC 61800-5-2 IEC 61800-5-3 IEC 61131-6 EN 50402 IEC 60730 IEC 60335	SAE J3018 SAE J3092 SAE J3164
Generic	IEEE P2846 IEEE 1228 IEEE 7000 series IEEE 1848 IEEE C95 IEEE C37	ISO TS 5083 ISO 34501-5 ISO 17356 ISO 14971 ISO 13485 ISO PAS 8800 ISO PAS 8926 ISO TR 9839 ISO 13849 ISO 13850 ISO 14119 ISO 13856 ISO 13851 ISO 13482 ISO 15066 ISO 13854 ISO 13857 ISO 13855 ISO 14118 ISO 14120 ISO 3691-4	ISO/IEC DTR 5469 ISO/IEC 22989 IEC 60601 IEC 61496 IEC 60204 IEC 62046 IEC 62061 IEC 62998 EN 1525	UL 4600 MISRA SAE J3016 SAE J3131 DO-178B DO-254 SAE ARP 4754A SAE ARP 4761A ANSI/ITSDF B56.5 ANSI B11.0 ANSI/RIA R15.06 ANSI/RIA R15.08
Basic	IEEE P2851	ISO 26262 ISO 21448 ISO/SAE 21434	IEC 61508 IEC 61511 IEC 61784-3 IEC 62280 IEC 61513 IEC 63168	Accellera FSWG SAE J3187 ECSS-S-ST-00-01C
NOTE 1—The text is color coded – text in green refers to standards from the automotive domain. Text in red refers to standards from the industrial, machinery, robotics domains. Text in purple refers to standards from the medical domain. Blue text is for avionics, and text in black is cross-domain. NOTE 2—Title of each standard is described in Section 4.				

1.3. ABOUT DIFFERENCES BETWEEN STANDARDS

The classification shown in TABLE 1 needs to be evaluated while considering that certain standards have different views than others—sometimes major, sometimes minor.

1.3.1. EXAMPLE OF HOUSEHOLD APPLIANCES

Considering the world of household appliances, the approach to functional safety is slightly different than that of the automotive field. Standards for electronics are created by the International Electrotechnical Commission (IEC) and American National Standards Institute (ANSI)/United Laboratories (UL) in the United States (US) or by the IEC and the European Committee for Electrotechnical Standardization (CENELEC) in Europe. In household appliances, Europe and the US differ in the way a standard is used to prove the compliance of a product. For example:

- Europe uses harmonized standards. This means that when a standard is finally in the *harmonized* group, it is considered a technical interpretation of a European Union directive or regulation and acts as a legal way to prove the conformity of a product to the European Community.
- In the US, products use standards created by a reliable entity or brand such as UL, the Canadian Standards Association (CSA), IEEE, and others. Depending on the chosen brand and on the chosen

standard to get the brand, the way that product conformity assessment is performed or a certification is reached differs.

The IEC proposed a common method between all the countries of the world so differences would decrease over time. The method can also be associated with a “CB scheme” that permits all stakeholders to have a common base scheme for the conformity assessment of a product and to reuse most of the test results from a certification body/accredited test laboratory of one country in a certification body/accredited test laboratory of a different country.

In this landscape, functional safety is related to the part of a product that includes *complex electronics*. When complex electronics are present, a set of tests conducted on the product as a black box is no longer sufficient.

In IEC 60730, for example, functional safety is mainly considered in a specific annex (Annex H) alongside all the technical rules that a product has to respect to be compliant to a standard, such as:

- Earthing and wiring
- Restrictions for creepage, clearance, and solid insulation
- Endurance and stress test
- EMC tests for both immunity and emission
- Glow-wire and ball pressure test

Before the 1990s, functional safety was a matter for a few groups, and Programmable Electronic Systems (PESs) were first used for control functionality due to the operational and cost advantages, and only in years later were they used for protection functions. The first discussions on gas appliances started by presenting flame supervision performed by logic (PESs) that had to follow special requirements for functionalities and for safety of internal blocks needed to realize the “complex electronics.” Here safety was not intrinsic, but dependent on the response of system outputs in relation to the different combination of inputs. The first standards to speak about functional safety measures for hardware or software were UL 1998 in the US and EN 60730-1 in Europe. At this time the V-model did not yet exist as a concept, and an organization of checklists was used for a detailed systematic approach.

Simply, when a microcontroller was used, the electronic safety engineer had to analyze which functionalities were assigned to the microcontroller and had to activate the safety measures required by the specific standard for the specific block of the microcontroller (i.e., CPU, clock, volatile and not volatile memories, and so forth). The reference to IEC 61508 was only recently introduced as a basic standard for both software and hardware development and for the development process itself.

This does not mean that the questions of primary and secondary levels of safety mechanisms in association to the *mission* function are missing. On the contrary, they are strongly rooted in the development phase.

Another peculiarity of household appliances is the time lapse between the occurrence of a first fault and the need to consider a second one. In most of the household controls standards, a second fault is only considered after the next start-up cycle (if the system is not permanently working for more than 24 hours) or after a maximum of 24 hours (if the system is permanently powered). However, in IEC 60335, the concept of *second fault* is slightly different because the *second fault* is considered when the *safety functionality* is active.

1.3.2. TOPICS BASED STANDARDS CLASSIFICATION

TABLE 2 is an attempt to classify some of the standards listed in TABLE 1 based on a non-exhaustive list of topics.

TABLE 2 Topic-Based Standards Classification

	Application Generic				Automotive						Industrial, Robotics, Machinery, household appliance				Avionics		
Standard	ISO/IEC TR 5469	IEEE P1228	IEEE P2851		ISO 26262	ISO 21448	ISO/AWI PAS 8800	ISO/AWI TS 5083	IEEE P2846		IEC 61508	ISO 13849	IEC 60730		DO178C	DO 254	
Topic included																	
Contents specific to Integrated Circuits (ICs)	X	—	X		X	—	X	—	—		X	X	X		—	X	
Contents specific to Software (SW)	X	X	X		X	—	X	X	—		X	X	X		X	—	
Contents specific to Machine Learning	X	—	X		—	X	X	X	—		—	—	—		—	—	
Contents specific to system	X	—	X		X	X	X	X	X		X	X	X		—	—	
Quantitative metrics for Hardware failures	—	—	X		X	X	—	—	—		X	X	X		—	—	
Quantitative metrics for SW failures	—	X	—		—	—	—	—	—		—	—	X		—	—	
Second fault/latent fault concept	—	—	—		X	—	—	—	—		—	X	X		—	—	
Common Cause Failures	—	—	X		X	—	—	—	—		X	X	X		X	X	
Freedom from Interference	—	—	X		X	—	—	—	—		X	X	X		—	—	
Systematic capability of Hardware (HW)	—	—	X		X	—	—	—	—		X	X	X		—	X	
Systematic capability of SW	—	X	X		X	—	—	—	—		X	X	X		X	—	
Safety of Intended Functionality	—	—	X		—	X	—	X	—		—	—	—		—	—	
Fault injection	X	—	X		X	—	—	—	—		—	X	—		—	—	
Reference architectures	X	—	—		—	—	—	X	—		X	X	—		—	—	
Predictive maintenance	—	—	—		—	—	—	—	—		—	—	—		—	—	
Content not covering Electronic Engineering	—	—	—		—	—	—	—	—		—	—	—		—	—	
...																	

1.4. THE DEFINITIONS CHALLENGE

It should be noted that the problem of incompatible or conflicting definitions has previously been discussed; however, the discussion has considered either only a single domain, for example in Stolte et al. [2], or the entire electromechanical system. There is no in-between. The rest of this document will discuss a series of terms that the study group authoring this white paper regard as part of a required subset needed for the functional safety of semiconductor devices. It will discuss the different definitions and existing commonalities and will set a single unambiguous definition for each. The subset considered is in the following list:

- [System](#)
- [Safety](#)
- [Item](#)
- [Fail-safe](#)
- [Fail-unsafe](#)
- [Fail-operational](#)
- [Fail-degraded](#)
- [Risk](#)
- [Safe-state](#)
- [Availability](#)
- [Recoverability](#)
- [Dependability](#)
- [Equipment under control](#)
- [Element](#)
- [Error](#)
- [Failure](#)
- [Fault](#)
- [Hazard](#)
- [Level of rigor](#)
- [Reliability](#)
- [Scope](#)

It should be noted that not all the terms *have* to be used in all standards, only the terms germane to the standard being developed.

2. THE TERMS

2.1. SYSTEM

Avizienis et al. [8] defines a *system* as “an entity that interacts with other entities, i.e., other systems, including hardware, software, humans, and the physical world with its natural phenomena,” with *other systems* being the environment of a given system. Part 1, 3.163, of ISO 26262 [3] defines it as “a set of components or subsystems that relates at least a sensor, a controller and an actuator with one another,” which is a much more restrictive definition, as it removes the human element and removes the necessity of an environment. The ISO 26262 definition focuses on the interaction of elements within the given system, whereas that of Avizienis et al. [8] focuses on what the system interacts with—it makes no statement on what the system contains. The ISO 26262 definition is potentially too restrictive; if the system being developed is the microcontroller that is to be used in a larger system that does contain an actuator and sensor, then when considering the microcontroller in isolation, we are missing the other elements. The microcontroller itself could not be considered a system, even though it is defined as a *system on chip*.