IEC 62541-15

Edition 1.0 2025-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

OPC Unified Architecture –
Part 15: Safety

Architecture unifiée OPC –
Partie 15: Sécurité

IEC 62541-15:2025-02(en-fr)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

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

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

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

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

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 62541-15

Edition 1.0 2025-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

OPC Unified Architecture – Part 15: Safety

Architecture unifiée OPC – Partie 15: Sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8327-0212-3

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

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 9
2 Normative references 9
3 Terms, definitions, symbols, abbreviated terms and conventions 10
3.1 Terms and definitions 10
3.1.1 Common terms and definitions 10
3.1.2 Additional terms and definitions 12
3.2 Symbols and abbreviated terms 14
3.2.1 Abbreviated terms from IEC 61784-3 14
3.2.2 Additional symbols and abbreviated terms 15
3.3 Conventions 15
3.3.1 General conventions 15
3.3.2 Conventions for requirements numbering 15
3.3.3 Conventions in state machines 16
4 Overview of OPC UA Safety 16
4.1 General 16
4.2 Implementation aspects 16
4.3 Features 17
4.4 Security policy 17
5 General 18
5.1 External documents providing specifications for the profile 18
5.2 Safety functional requirements 18
5.3 Safety measures 18
5.4 Safety communication layer structure 19
5.5 Requirements for CRC calculation 21
6 Safety communication layer services 21
6.1 General 21
6.2 Information models 22
6.2.1 General 22
6.2.2 Object and ObjectType Definitions 22
6.2.3 DataType definition 34
6.2.4 SafetyProvider version 38
6.2.5 DataTypes and length of SafetyData 38
6.2.6 Connection establishment 38
6.3 Service interfaces 38
6.3.1 Overview 38
6.3.2 OPC UA Platform interface (OPC UA PI) 39
6.3.3 SafetyProvider interfaces 39
6.3.4 SafetyConsumer interfaces 46
6.3.5 Cyclic and acyclic safety communication 53
6.3.6 Principle for "application variables with qualifier" 53
6.4 Diagnostics 53
6.4.1 General 53
6.4.2 Diagnostics messages of the SafetyConsumer 54
6.4.3 Method ReadSafetyDiagnostics of the SafetyProvider 56

7 Safety communication layer protocol 56
7.1 General 56
7.2 SafetyProvider and SafetyConsumer 56
7.2.1 SPDU formats 56
7.2.2 Behaviour 58
7.2.3 Subroutines 76
8 Safety communication layer management 82
8.1 General 82
8.2 Safety function response time part of communication 82
9 System requirements (SafetyProvider and SafetyConsumer) 84
9.1 Constraints on the SPDU parameters 84
9.1.1 SafetyBaseID and SafetyProviderID 84
9.1.2 SafetyConsumerID 85
9.2 Initialization of the MNR in the SafetyConsumer 86
9.3 Constraints on the calculation of system characteristics 86
9.3.1 Probabilistic considerations (informative) 86
9.3.2 Safety related assumptions (informative) 88
9.4 PFH and PFD values of a logical safety communication link 88
9.5 Safety manual 89
9.6 Indicators and displays 90
10 Assessment 90
10.1 Safety policy 90
10.2 Obligations 91
10.3 Index of requirements (informative) 91
11 Profiles and conformance units 94
12 Namespaces 94
12.1 Namespace metadata 94
12.2 Handling of IEC 62541 namespaces 95
Annex A (normative) Safety namespace and mappings 96
Annex B (informative) Additional information 97
B.1 CRC calculation using tables, for the polynomial 0xF4ACFB13 97
B.2 Use cases 98
B.2.1 Unidirectional communication 98
B.2.2 Bidirectional communication 99
B.2.3 Safety multicast 99
B.3 Use cases for operator acknowledgment 100
B.3.1 Explanation 100
B.3.2 Use case 1: unidirectional communication and OA on the SafetyConsumer side 100
B.3.3 Use case 2: bidirectional communication and dual OA 101
B.3.4 Use case 3: bidirectional communication and single, one-sided OA 101
B.3.5 Use case 4: bidirectional communication and single, two-sided OA 102
Annex C (informative) Information for assessment 103
Bibliography 104

Figure 1 – Relationships of OPC UA safety with other standards 8
Figure 2 – Safety layer architecture 20

Figure 3 – Server Objects for OPC UA Safety 24
Figure 4 – Instances of Server Objects for this document 25
Figure 5 – Safety multicast with three recipients using IEC 62541 PubSub 31
Figure 6 – Safety parameters for the SafetyProvider and the SafetyConsumer 32
Figure 7 – Safety communication layer overview 39
Figure 8 – SafetyProvider interfaces 40
Figure 9 – Example combinations of SIL capabilities 46
Figure 10 – SafetyConsumer interfaces 47
Figure 11 – RequestSPDU 56
Figure 12 – ResponseSPDU 57
Figure 13 – Sequence diagram for requests and responses (Client/Server) 59
Figure 14 – Sequence diagram for requests and responses (PubSub) 60
Figure 15 – Duration of demand example for missed demand value in case of currently available SafetyData not being provided until second change of MNR 61
Figure 16 – Duration of demand example for received demand value in case of currently available SafetyData being provided 62
Figure 17 – Simplified representation of the state diagram for the SafetyProvider 62
Figure 18 – Principle state diagram for SafetyConsumer 65
Figure 19 – Sequence diagram for OA 75
Figure 20 – Overview of task for SafetyProvider 76
Figure 21 – Calculation of the SPDU_ID 77
Figure 22 – Example for the calculation of SPDU_ID_1, SPDU_ID_2 and SPDU_ID_3 78
Figure 23 – Calculation of the CRC (on little-endian machines, CRC32_Backward) 81
Figure 24 – Calculation of the CRC (on big-endian machines, CRC32_Forward) 82
Figure 25 – Overview of delay times and watchdogs 83
Figure 26 – Conditional residual error probability of the CRC check 87
Figure 27 – Counter example: data lengths not supported by OPC Safety 88
Figure 28 – Facets and ConformanceUnits 94
Figure B.1 – Unidirectional communication 99
Figure B.2 – Bidirectional communication 99
Figure B.3 – Safety multicast 99
Figure B.4 – OA in unidirectional safety communication 100
Figure B.5 – Two-sided OA in bidirectional safety communication 101
Figure B.6 – One sided OA in bidirectional safety communication 101
Figure B.7 – One sided OA on each side is possible 102

Table 1 – Conventions used in state machines 16
Table 2 – Deployed safety measures to detect communication errors 18
Table 3 – SafetyACSet definition 22
Table 4 – SafetyObjectsType definition 26
Table 5 – SafetyProviderType definition 26
Table 6 – SafetyConsumerType definition 27
Table 7 – ReadSafetyData Method arguments 28
Table 8 – ReadSafetyData Method AddressSpace definition 29

Table 9 – ReadSafetyDiagnostics Method arguments 30
Table 10 – ReadSafetyDiagnostics Method AddressSpace definition 30
Table 11 – SafetyPDUsType definition 31
Table 12 – SafetyProviderParametersType definition 33
Table 13 – SafetyConsumerParametersType definition 34
Table 14 – InFlagsType values 35
Table 15 – InFlagsType definition 35
Table 16 – OutFlagsType values 35
Table 17 – OutFlagsType definition 36
Table 18 – RequestSPDUDataType structure 36
Table 19 – RequestSPDUDataType definition 36
Table 20 – ResponseSPDUDataType structure 37
Table 21 – ResponseSPDUDataType definition 37
Table 22 – NonSafetyDataPlaceholderDataType structure 37
Table 23 – SAPI of the SafetyProvider 41
Table 24 – SPI of the SafetyProvider 42
Table 25 – SAPI of the SafetyConsumer 47
Table 26 – SPI of the SafetyConsumer 50
Table 27 – Example "application variables with qualifier" 53
Table 28 – Safety layer diagnostic messages 54
Table 29 – Symbols used for state machines 62
Table 30 – SafetyProvider instance internal items 63
Table 31 – States of SafetyProvider instance 64
Table 32 – SafetyProvider transitions 64
Table 33 – SafetyConsumer internal items 66
Table 34 – SafetyConsumer states 70
Table 35 – SafetyConsumer transitions 71
Table 36 – Presentation of the SPDU_ID 77
Table 37 – Coding for the SafetyProviderLevel_ID 78
Table 38 – Examples for cryptographically strong random number generators 85
Table 39 – The total residual error rate for the safety communication channel 89
Table 40 – Information to be included in the safety manual 89
Table 41 – Index of requirements (informative) 92
Table 42 – NamespaceMetadata Object for this document 95
Table 43 – Namespaces used in a safety Server 95
Table B.1 – The CRC32 lookup table for 32-bit CRC signature calculations 98

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

OPC UNIFIED ARCHITECTURE –

Part 15: Safety

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62541-15 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

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

Draft	Report on voting
65C/1334/FDIS	65C/1339/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

Throughout this document and the referenced other parts of the IEC 62541 series, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in Clause 3 in one of the parts of the series.

Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.

The *italicized terms* and *names* are also, with a few exceptions, written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example, the defined term is *AddressSpace* instead of Address Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not separate definitions for Address and Space.

A list of all parts of the IEC 62541 series, published under the general title *OPC Unified Architecture*, can be found on the IEC website.

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

- reconfirmed,
- withdrawn, or
- revised.

INTRODUCTION

OPC UA safety extends OPC UA to fulfill the requirements of functional safety as defined in the IEC 61508 series and IEC 61784-3 series of standards.

Figure 1 shows the relationship between this document and the relevant safety and OPC UA standards in an industrial environment. An arrow from Document A to Document B means "Document A is referenced in Document B". This reference can be either normative or informative. Not all of these standards are applicable or required for a given product.

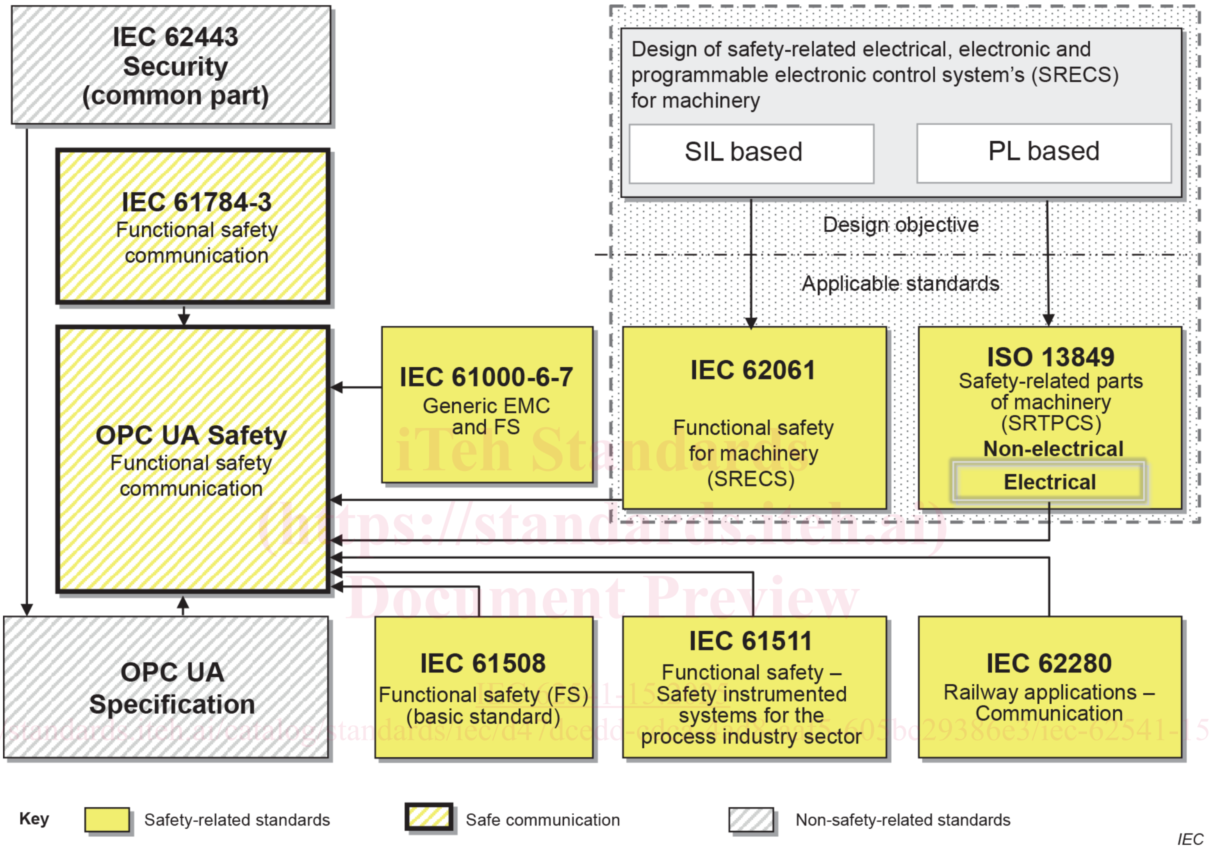
IEC 62443
Security
(common part)
IEC 61784-3
Functional safety communication
OPC UA Safety
Functional safety communication
IEC 61000-6-7
Generic EMC and FS
Design of safety-related electrical, electronic and programmable electronic control system's (SRECS) for machinery
SIL based
PL based
Design objective
Applicable standards
IEC 62061
Functional safety for machinery (SRECS)
ISO 13849
Safety-related parts of machinery (SRTPCS)
Non-electrical
Electrical
OPC UA
Specification
IEC 61508
Functional safety (FS)
(basic standard)
IEC 61511
Functional safety – Safety instrumented systems for the process industry sector
IEC 62280
Railway applications – Communication
Key
Safety-related standards
Safe communication
Non-safety-related standards
IEC

Figure 1 – Relationships of OPC UA safety with other standards

Implementing this document allows for detecting all types of communication errors encountered in the lower network layers. In case an error is detected, this information is shared with the safety applications in the user layer which can then act in an appropriate way, e.g. by switching to a safe state.

The document describes the behaviour of the individual endpoints for safe communication, as well as the OPC UA *Information Model* which is used to access these endpoints.

This document is application-independent and does not pose requirements on the structure and length of the application data. Application-specific requirements are expected to be described in appropriate companion specifications.

This document can be used for applications requiring functional safety up to the *safety integrity level* (*SIL*) 4.

OPC UNIFIED ARCHITECTURE –

Part 15: Safety

1 Scope

This document describes a *safety communication layer* (services and a protocol) for the exchange of *SafetyData* using IEC 62541 mechanisms. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this *safety communication layer*. This *safety communication layer* is intended for implementation in *safety* devices only.

NOTE 1 This document targets controller-to-controller communication. However, easy expandability to other use-cases (e.g. OPC UA field level communication) has already been considered in the design of this document.

NOTE 2 This document does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This document defines mechanisms for the transmission of safety-relevant messages among participants within a network using OPC UA technology in accordance with the requirements of the IEC 61508 series and IEC 61784-3 for functional safety. These mechanisms can be used in various industrial applications such as process control, manufacturing, automation, and machinery.

This document provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 3 The resulting *SIL* claim of a system depends on the implementation of this document within the system – implementation of this document in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

IEC 62541-1:2020, *OPC Unified Architecture – Part 1: Overview and Concepts*

IEC 62541-3:2020, *OPC Unified Architecture – Part 3: Address Space Model*

IEC 62541-4:2020, *OPC Unified Architecture – Part 4: Services*

IEC 62541-5:2020, *OPC Unified Architecture – Part 5: Information Model*

IEC 62541-6:2020, *OPC Unified Architecture – Part 6: Mappings*

IEC 62541-14, *OPC Unified Architecture – Part 14: PubSub*

ISO/IEC 9834-8:2014, *Information technology – Procedures for the operation of object identifier registration authorities – Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62541-1:2020, IEC 62541-3:2020, IEC 62541-4:2020, IEC 62541-6:2020 and the following apply.

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

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

NOTE This document uses concepts of IEC 62541 information modeling to describe the concepts in this document.

3.1.1 Common terms and definitions

3.1.1.1
Cyclic Redundancy Check
CRC
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this document to refer to the redundant data.

[SOURCE: IEC 61784-3:2021, 3.10]

3.1.1.2
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

Note 2 to entry: Errors do not necessarily result in a failure or a fault.

[SOURCE: IEC 60050-192:2024, 192-03-02, modified – notes added]

3.1.1.3
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure can be due to an error (for example, problem with hardware/software design or message disruption).

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures deleted, new note to entry added]

3.1.1.4
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEV 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]

message
<information theory and communication theory>ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123031, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.1.5
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2023, 3.1.5]

3.1.1.6
residual error probability
probability of an error undetected by the *SCL* safety measures

[SOURCE: IEC 61784-3:2021, 3.1.35]

3.1.1.7
residual error rate
statistical rate at which the *SCL* safety measures fail to detect errors

[SOURCE: IEC 61784-3:2021, 3.1.36]

3.1.1.8
safety communication layer
SCL
communication layer above the IEC 62541 communication stack that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

Note 1 to entry: The *SCL* provides several services, the most important ones being the *SafetyProvider* and the *SafetyConsumer*.

[SOURCE: IEC 61784-3:2021, 3.1.39, modified – "FAL" replaced by "IEC 62541 communication stack", note to entry added]

3.1.1.9
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

Note 1 to entry: This concept is introduced in IEC 61784-3:2021, 5.2.4 and is addressed by the functional safety communication profiles defined in the IEC 61784-3 series of documents.

[SOURCE: IEC 61784-3:2021, 3.1.44]

3.1.1.10
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four *safety integrity levels* are specified in Table 2 and Table 3 of IEC 61508-1:2010.

Note 2 to entry: *Safety integrity levels* are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A *safety integrity level* (*SIL*) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "*SIL* n safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a *safety integrity level* up to n.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.1.11
safety measure
measure to control possible communication errors that is designed and implemented in compliance with the requirements of IEC 61508

Note 1 to entry: In practice, several safety measures are combined to achieve the required *safety integrity level*.

Note 2 to entry: Communication errors and related safety measures are detailed in IEC 61784-3:2021, 5.3 and 5.4.

[SOURCE: IEC 61784-3:2021, 3.1.46]

3.1.1.12
safety PDU
SPDU
PDU transferred through the *safety communication channel*

Note 1 to entry: The SPDU may include more than one copy of the *SafetyData* using differing coding structures and hash functions together with explicit parts of additional protections such as a key, a sequence count, or a time stamp mechanism.

Note 2 to entry: Redundant *SCLs* may provide two different versions of the SPDU for insertion into separate fields of the IEC 62541 frame.

[SOURCE: IEC 61784-3:2021, 3.1.47]

3.1.2 Additional terms and definitions

3.1.2.1
fail-safe
ability of a system that, by adequate technical or organizational measures, prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Equivalent to functional safety.

3.1.2.2
fail-safe substitute values
FSV
values which are issued or delivered instead of process values when the safety function is set to a fail-safe state

Note 1 to entry: In this document, the fail-safe substitute values (FSV) are always set to binary "0".

3.1.2.3
flag
one-bit value used to indicate a certain status or control information