



BSI Standards Publication

Functional safety - Safety instrumented systems for the process industry sector -

Part 1: Framework, definitions, system, hardware and application programming requirements

National foreword

This British Standard is the UK implementation of EN 61511-1:2017 +A1:2017. It is identical to IEC 61511-1:2016, incorporating amendment 1:2017. It supersedes BS EN 61511-1:2017 which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment 1 is indicated by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee GEL/65/1, System considerations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 96268 4

ICS 25.040.40; 13.110; 25.040.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2017.

Amendments/corrigenda issued since publication

Date	Text affected
28 February 2018	Implementation of IEC amendment 1:2017 with CENELEC endorsement A1:2017

English Version

Functional safety — Safety instrumented
systems for the process industry sector — Part 1:
Framework, definitions, system, hardware and
application programming Requirements (IEC 61511-
1:2016 + COR1:2016)

Sécurité fonctionnelle — Systèmes instrumentés
de sécurité pour le secteur des industries
de transformation — Partie 1: Cadre,
définitions, exigences pour le système, le
matériel et la programmation d'application
(IEC 61511-1:2016 + COR1:2016)

Funktionale Sicherheit — Sicherheitstechnische
Systeme für die Prozessindustrie — Teil 1:
Allgemeines, Begriffe, Anforderungen an Systeme,
Hardware und Anwendungsprogrammierung
(IEC 61511-1:2016 + COR1:2016)

This European Standard was approved by CENELEC on 2016-03-30. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 65A/777/FDIS, future edition 2 of IEC 61511-1, prepared by SC 65A "System aspects" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61511-1:2017.

The following dates are fixed:

- latest date by which the document has to be implemented at
• national level by publication of an identical national standard (dop) 2017-10-21
or by endorsement
- latest date by which the national standards conflicting with the (dow) 2020-04-21
document have to be withdrawn

This document supersedes EN 61511-1:2004.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 61511-1:2016 + COR1:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-3-2:2004	NOTE	Harmonized as EN 60300-3-2:2005 (not modified).
IEC 61025	NOTE	Harmonized as EN 61025.
IEC 61131-3:2013	NOTE	Harmonized as EN 61131-3:2013 (not modified).
IEC 61131-6:2012	NOTE	Harmonized as EN 61131-6:2012 (not modified).
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
IEC 61511-2	NOTE	Harmonized as EN 61511-2.
IEC 61511-3	NOTE	Harmonized as EN 61511-3.
IEC 61784-3:2010	NOTE	Harmonized as EN 61784-3:2010 (not modified).
IEC 62682:2014	NOTE	Harmonized as EN 62682:2015 (not modified).
ISO 9000:2005	NOTE	Harmonized as EN ISO 9000:2005 ¹⁾ (not modified).
ISO 9001:2008	NOTE	Harmonized as EN ISO 9001:2008 ²⁾ (not modified).
ISO 13849-1:2006	NOTE	Harmonized as EN ISO 13849-1:2006 ³⁾ (not modified).
ISO 13849-2:2012	NOTE	Harmonized as EN ISO 13849-2:2012 (not modified).
ISO 14224:2006	NOTE	Harmonized as EN ISO 14224:2006 (not modified).

European foreword to Amendment 1

The text of document 65A/777/FDIS, future edition 1 of IEC 61511-1:2016+A1:2017, prepared by SC 65A "System aspects" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61511-1:2017+A1:2017.

The following dates are fixed:

- latest date by which the document has to be implemented at
national level by publication of an identical national standard (dop) 2018-06-20
or by endorsement
- latest date by which the national standards conflicting with the (dow) 2020-09-20
document have to be withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 61511-1:2016 + A1:2017 was approved by CENELEC as a European Standard without any modification.

Replace the following references in the Bibliography of EN 61511-1:2017+A1:2017:

IEC 61511-2:2016	NOTE	Harmonized as EN 61511-2:2017.
IEC 61511-3:2016	NOTE	Harmonized as EN 61511-3:2017.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2010
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010

1) Superseded by
EN ISO 9000:2015
(ISO 9000:2015).

2) Superseded by
EN ISO 9001:2015
(ISO 9001:2015).

3) Superseded by
EN ISO 13849-1:2015
(ISO 13849-1:2015).

Contents

Page

FOREWORD	7
INTRODUCTION	9
1 Scope	1
2 Normative references	5
3 Terms, definitions and abbreviations	5
3.1 Terms	5
3.2 Terms and definitions	6
3.2.6 common cause	7
3.2.75 application programming languages	21
3.2.76 software & program types	22
3.3 Abbreviations	25
4 Conformance to the IEC 61511-1:2016	26
5 Management of functional safety	26
5.1 Objective	26
5.2 Requirements	26
5.2.1 General	26
5.2.2 Organization and resources	26
5.2.3 Risk evaluation and risk management	27
5.2.4 Safety planning	27
5.2.5 Implementing and monitoring	27
5.2.6 Assessment, auditing and revisions	28
5.2.7 SIS configuration management	31
6 Safety life-cycle requirements	31
6.1 Objectives	31
6.2 Requirements	32
6.3 Application program SIS safety life-cycle requirements	35
7 Verification	37
7.1 Objective	37
7.2 Requirements	37
8 Process H&RA	39
8.1 Objectives	39
8.2 Requirements	39
8.2.1 A H&RA shall be carried out on the materials, process and equipment. It shall result in:	39
9 Allocation of safety functions to protection layers	40
9.1 Objectives	40
9.2 Requirements of the allocation process	41
9.3 Requirements on the basic process control system as a protection layer	43
9.4 Requirements for preventing common cause, common mode and dependent failures	44
10 SIS safety requirements specification (SRS)	45
10.1 Objective	45
10.2 General requirements	45
10.3 SIS safety requirements	45
11 SIS design and engineering	47
11.1 Objective	47
11.2 General requirements	48
11.3 Requirements for system behaviour on detection of a fault	49
11.4 Hardware fault tolerance	49

11.5	Requirements for selection of devices	51
11.5.1	Objectives	51
11.5.2	General requirements	51
11.5.3	Requirements for the selection of devices based on prior use	51
11.5.3.2	The evidence of suitability shall include the following:	51
11.5.4	Requirements for selection of FPL programmable devices (e.g., field devices) based on prior use	52
11.5.5	Requirements for selection of LVL programmable devices based on prior use	53
11.5.6	Requirements for selection of FVL programmable devices	54
11.6	Field devices	54
11.7	Interfaces	54
11.7.1	General	54
11.7.2	Operator interface requirements	54
11.7.3	Maintenance/engineering interface requirements	55
11.7.4	Communication interface requirements	56
11.8	Maintenance or testing design requirements	56
11.9	Quantification of random failure	57
12	SIS application program development	58
12.1	Objective	58
12.2	General requirements	59
12.3	Application program design	60
12.3.5	The application program design shall ensure:	61
12.4	Application program implementation	61
12.5	Requirements for application program verification (review and testing)	62
12.6	Requirements for application program methodology and tools	63
13	Factory acceptance test (FAT)	63
13.1	Objective	63
13.2	Recommendations	64
13.2.6	The results of FAT shall be documented, stating	65
14	SIS installation and commissioning	65
14.1	Objectives	65
14.2	Requirements	65
15	SIS safety validation	66
15.1	Objective	66
15.2	Requirements	66
16	SIS operation and maintenance	69
16.1	Objectives	69
16.2	Requirements	69
16.3	Proof testing and inspection	72
16.3.1	Proof testing	72
16.3.2	Inspection	73
16.3.3	Documentation of proof tests and inspection	73
17	SIS modification	73
17.1	Objectives	73
17.2	Requirements	74
18	SIS decommissioning	74
18.1	Objectives	74
18.2	Requirements	75
19	Information and documentation requirements	75
19.1	Objectives	75
19.2	Requirements	75

Bibliography	77
---------------------	-----------

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- references and requirements to software replaced with references and requirements to application programming;
- functional safety assessment requirements provided with more detail to improve management of functional safety.
- management of change requirement added;

- security risk assessment requirements added;
- requirements expanded on the basic process control system as a protection layer;
- requirements for hardware fault tolerance modified and should be reviewed carefully to understand user/integrator options.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/777/FDIS	65A/784/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 61511 series, published under the general title *Functional safety – safety instrumented systems for the process industry sector*, can be found on the IEC website.

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

Safety instrumented systems (SISs) have been used for many years to perform safety instrumented functions (SIFs) in the process industries. If instrumentation is to be effectively used for SIFs, it is essential that this instrumentation achieves certain minimum standards and performance levels.

The IEC 61511 series addresses the application of SISs for the process industries. The IEC 61511 series also addresses a process Hazard and Risk Assessment (H&RA) to be carried out to enable the specification for SISs to be derived. Other safety systems' contributions are only considered with respect to the performance requirements for the SIS. The SIS includes all devices necessary to carry out each SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application: SIS safety life-cycle and safety integrity levels (SILs).

The IEC 61511 series addresses SISs which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of the IEC 61511 series should be applied to ensure the functional safety requirements are met. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of the IEC 61508 series.

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum principles. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. However in some instances this is not possible or not practical. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, and programmable electronic). To facilitate this approach, the IEC 61511 series:

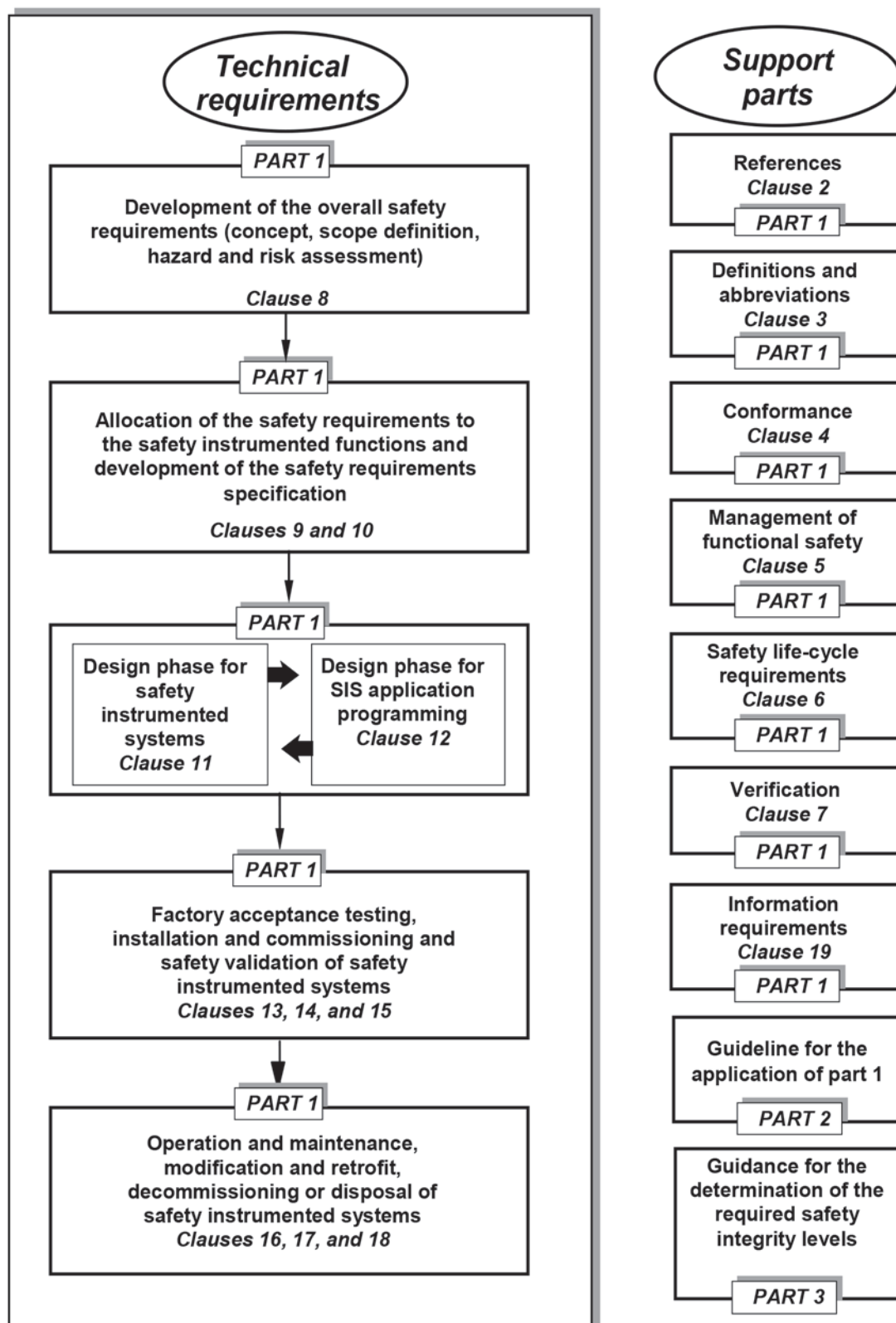
- addresses that a H&RA is carried out to identify the overall safety requirements;
- addresses that an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented means of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

The IEC 61511 series on SIS for the process industry:

- addresses all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (e.g., of underlying principles, terminology, and information) within the process industries. This should have both safety and economic benefits. [Figure 1](#) below shows an overall framework of the IEC 61511 series.

In jurisdictions where the governing authorities (e.g., national, federal, state, province, county, city) have established process safety design, process safety management, or other regulations, these take precedence over the requirements defined in the IEC 61511 series.



IEC

Figure 1 — Overall framework of the IEC 61511 series

Functional safety - Safety instrumented systems for the process industry sector - —

Part 1:

Framework, definitions, system, hardware and application programming requirements

1 Scope

This part of IEC 61511 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve or maintain a safe state of the process. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010.

In particular, IEC 61511-1:

- a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (e.g., designers, suppliers, owner/operating company, contractor). This responsibility will be assigned to different parties according to safety planning, project planning and management, and national regulations;
- b) applies when devices that meets the requirements of the IEC 61508 series published in 2010, or IEC 61511-1:2016 [11.5], is integrated into an overall system that is to be used for a process sector application. It does not apply to manufacturers wishing to claim that devices are suitable for use in SISs for the process sector (see IEC 61508-2:2010 and IEC 61508-3:2010);
- c) defines the relationship between IEC 61511 and IEC 61508 (see [Figures 2](#) and [3](#));
- d) applies when application programs are developed for systems having limited variability language or when using fixed programming language devices, but does not apply to manufacturers, SIS designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3:2010);
- e) applies to a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;

NOTE 1 Within the process sector some applications may have additional requirements that have to be satisfied.

- f) outlines the relationship between SIFs and other instrumented functions (see [Figure 4](#));
- g) results in the identification of the functional requirements and safety integrity requirements for the SIF taking into account the risk reduction achieved by other methods;
- h) specifies life-cycle requirements for system architecture and hardware configuration, application programming, and system integration;
- i) specifies requirements for application programming for users and integrators of SISs.
- j) applies when functional safety is achieved using one or more SIFs for the protection of personnel, protection of the general public or protection of the environment;
- k) may be applied in non-safety applications for example asset protection;
- l) defines requirements for implementing SIFs as a part of the overall arrangements for achieving functional safety;

- m) uses a SIS safety life-cycle (see [Figure 7](#)) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the SIS;
- n) specifies that a H&RA is to be carried out to define the safety functional requirements and safety integrity levels (SIL) of each SIF;

NOTE 2 [Figure 9](#) presents an overview of risk reduction means.

- o) establishes numerical targets for average probability of failure on demand (in demand mode) and average frequency of dangerous failures (in demand mode or continuous mode) for each SIL;
- p) specifies minimum requirements for hardware fault tolerance (HFT);
- q) specifies measures and techniques required for achieving the specified SIL;
- r) defines a maximum level of functional safety performance (SIL 4) which can be achieved for a SIF implemented according to IEC 61511-1;
- s) defines a minimum level of functional safety performance (SIL 1) below which IEC 61511-1 does not apply;
- t) provides a framework for establishing the SIL but does not specify the SIL required for specific applications (which should be established based on knowledge of the particular application and on the overall targeted risk reduction);
- u) specifies requirements for all parts of the SIS from sensor to final element(s);
- v) defines the information that is needed during the SIS safety life-cycle;
- w) specifies that the design of the SIS takes into account human factors;
- x) does not place any direct requirements on the individual operator or maintenance person:

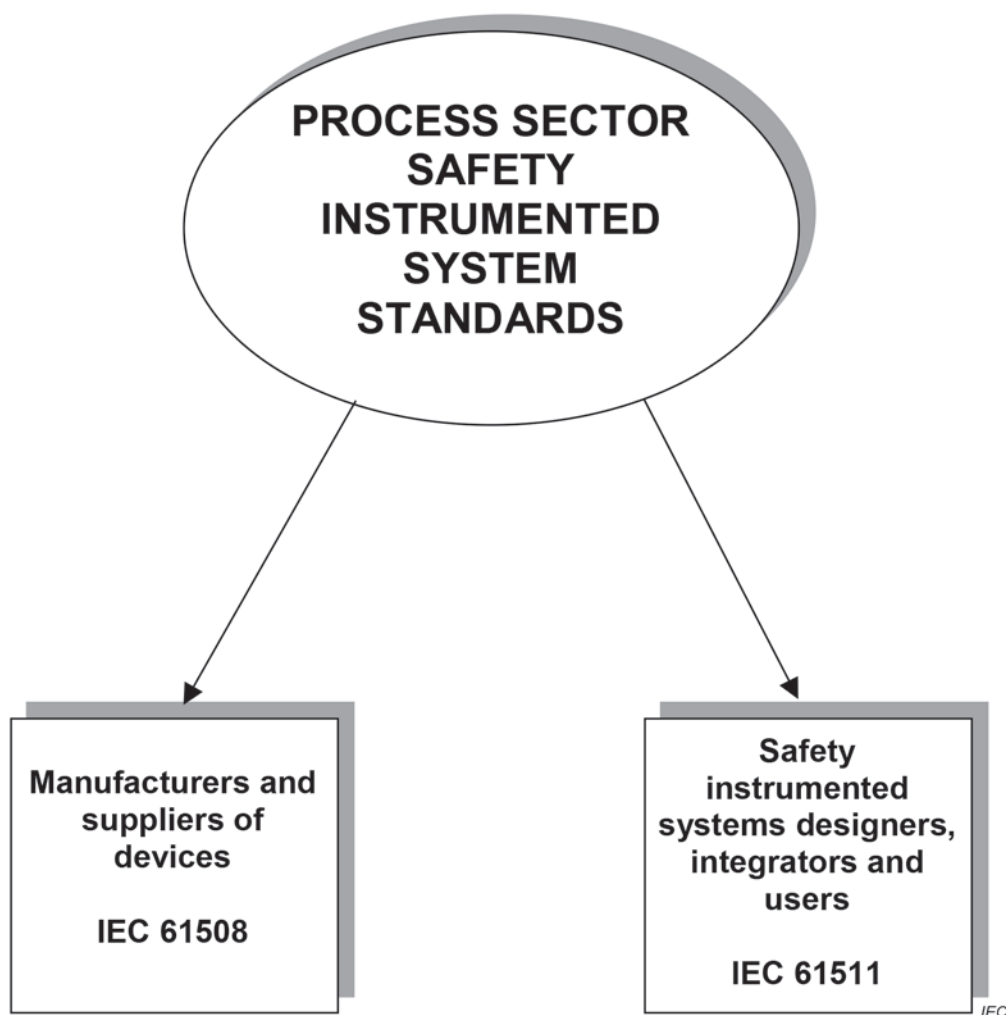
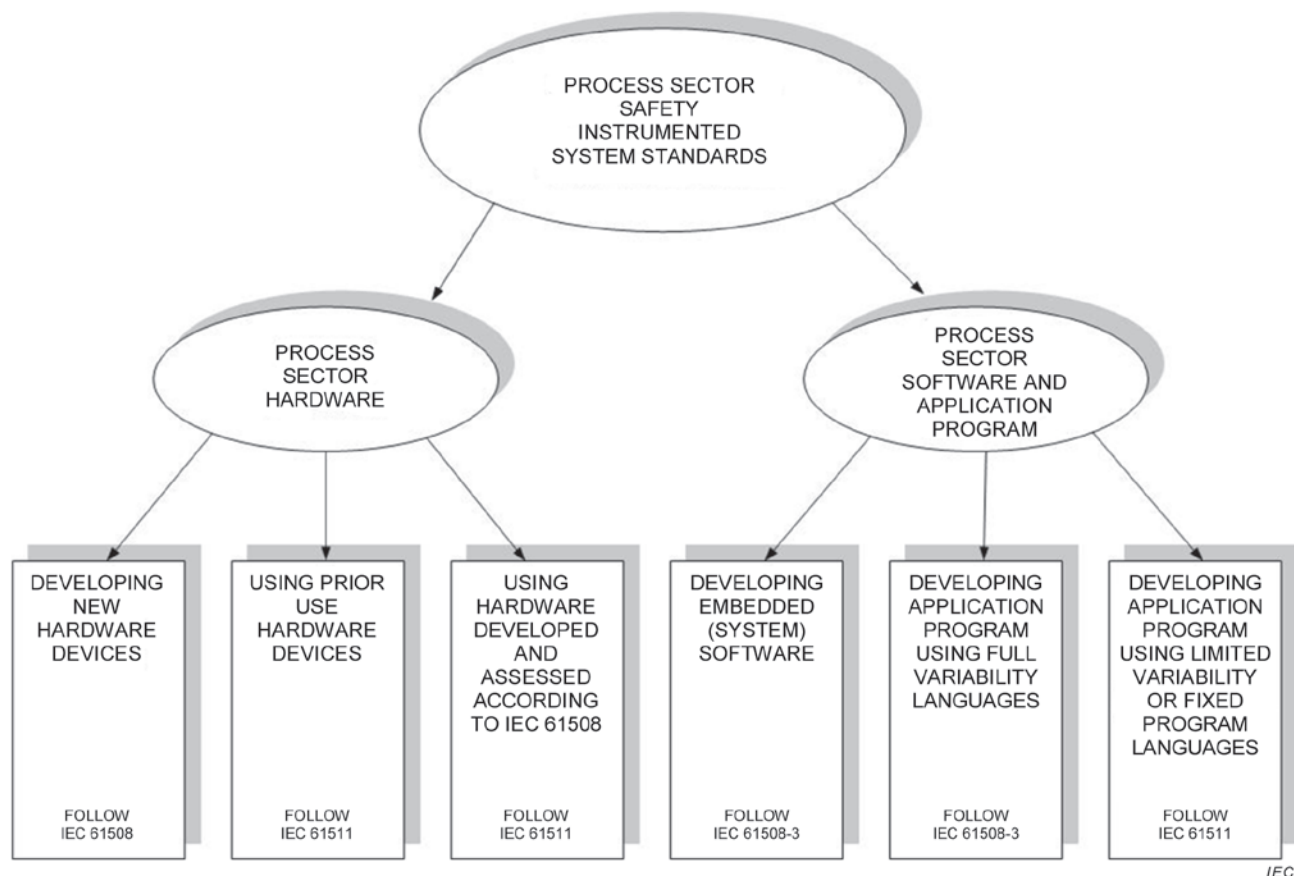


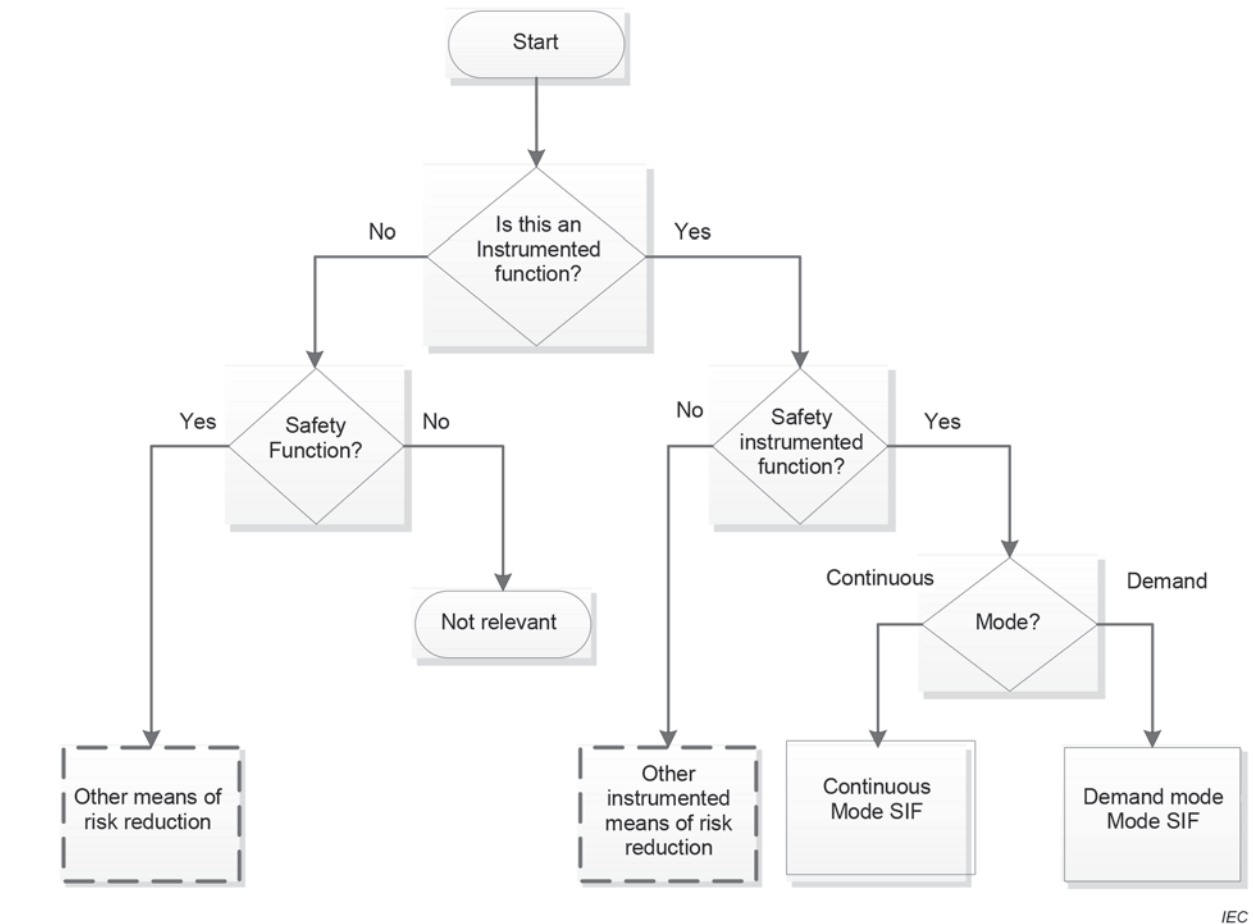
Figure 2 — Relationship between IEC 61511 and IEC 61508

NOTE 3 IEC 61508 is also used by safety instrumented designers, integrators and users where directed in IEC 61511.



NOTE 4 Subclause 7.2.2 in IEC 61511-1:2016 and A.7.2.2 in IEC 61511-2:2016 contain guidance on handling integration of sub-systems that comply with other standards (such as machinery , burner, etc.).

Figure 3 — Detailed relationship between IEC 61511 and IEC 61508



Standard specifies activities which are to be carried out but requirements are not detailed

Figure 4 — Relationship between safety instrumented functions and other functions

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General Requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

3 Terms, definitions and abbreviations

3.1 Terms

Terms are listed alphabetically in [3.2](#).

3.2 Terms and definitions

For the purposes of this document, the following definitions apply.

In some cases these definitions differ from the definitions of the same terms in IEC 61508-4:2010. In some cases this is due to the terminology used in the process sector. In other cases these definitions have been aligned with other relevant definitive references (e.g., IEC 60050 the International Electrotechnical Vocabulary, ISO/IEC Guide 51:2013). However, unless otherwise stated, there is no difference in the technical meaning between these definitions and the definitions of the same terms in IEC 61508-4:2010.

3.2.1

architecture configuration

specific configuration of hardware and software components in a system

Note 1 to entry: In the IEC 61511 series this can mean, for example, arrangement of SIS subsystems, the internal structure of a SIS subsystem or the internal structure of SIS application programs.

3.2.2

asset protection

function allocated to a system and designed for the purpose of preventing loss or damage to assets

3.2.3

basic process control system BPCS

system which responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any SIF

Note 1 to entry: A BPCS includes all of the devices necessary to ensure that the process operates in the desired manner.

Note 2 to entry: A BPCS typically may implement various functions such as process control functions, monitoring, and alarms.

3.2.4

bypass

action or facility to prevent all or parts of the SIS functionality from being executed

Note 1 to entry: Examples of bypassing include:

- the input signal is blocked from the trip logic while still presenting the input parameters and alarm to the operator;
- the output signal from the trip logic to a final element is held in the normal state preventing final element operation;
- a physical bypass line is provided around the final element;
- preselected input state (e.g., on/off input) or set is forced by means of an engineering tool (e.g., in the application program).

Note 2 to entry: Other terms are also used to refer to bypassing, such as override, defeat, disable, force, or inhibit or muting.

3.2.5

channel

device or group of devices that independently perform(s) a specified function

Note 1 to entry: The devices within a channel could include input/output (I/O) devices, logic solvers, sensors, and final elements.

Note 2 to entry: A dual channel (i.e., a two-channel) configuration is one with two channels that independently perform the same function. Channels may be identical or diverse.

Note 3 to entry: The term can be used to describe a complete system or a portion of a system (e.g., sensors or final elements).

Note 4 to entry: Channel describes SIS hardware architectural features often used to meet hardware fault tolerance requirements.

3.2.6 common cause

3.2.6.1

common cause failures, pl

concurrent failures of different devices, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: All the failures due to a common cause do not necessarily occur exactly at the same time and this may allow time to detect the occurrence of the common cause before a SIF is actually failed.

Note 2 to entry: Common cause failures can also lead to common mode failures.

Note 3 to entry: The potential for common cause failures reduces the effect of system redundancy or fault tolerance (e.g., increases the probability of failure of two or more channels in a multiple channel system).

Note 4 to entry: Common cause failures are dependent failures. They may be due to external events (e.g., temperature, humidity, overvoltage, fire, and corrosion), systematic fault (e.g., design, assembly or installation errors, bugs), human error (e.g., misuse), etc.

Note 5 to entry: By extension, a common cause failure (in singular form) is a failure belonging to a set of concurrent failures (plural form) according to [3.2.6.1](#) definition.

3.2.6.2

common mode failures, pl

concurrent failures of different devices characterized by the same failure mode (i.e., identical faults)

Note 1 to entry: Common mode failures may have different causes.

Note 2 to entry: Common mode failures can also be the result of common cause failures ([3.2.6.1](#)).

Note 3 to entry: The potential for common mode failures reduces the effectiveness of system redundancy and fault tolerance (e.g., failure of two or more channels in the same way, causing the same erroneous result).

Note 4 to entry: By extension, a common mode failure (in singular form) is a failure belonging to a set of concurrent failures (plural form) according to [3.2.6.2](#) definition.

3.2.7

compensating measure

temporary implementation of planned and documented methods for managing risks during any period of maintenance or process operation when it is known that the performance of the SIS is degraded

3.2.8

component

one of the parts of a system, SIS subsystem, or device performing a specified function

Note 1 to entry: Component may also include software.

3.2.9

configuration management

discipline of identifying the components and the arrangements of those components of an evolving system for the purposes of controlling changes to those components, and maintaining continuity of the system and traceability of any changes throughout the life-cycle

3.2.9.1

conservative approach

cautious way of doing analysis and calculations

Note 1 to entry: In the safety field, each time an analysis, assumptions, or calculation has to be done (about models, input data, computations, etc.) it can be chosen in order to be sure to produce pessimistic results.

3.2.10

control system

system which responds to input signals from the process and/or from an operator and generates output signals causing the process to operate in the desired manner

Note 1 to entry: The control system includes sensors and final elements and may be either a BPCS or a SIS or a combination of the two.

3.2.11

dangerous failure

failure which impedes or disables a given safety action

Note 1 to entry: A failure is "dangerous" only with regard to a given SIF.

Note 2 to entry:  When fault tolerance is implemented, a dangerous failure can lead to either:

- a degraded SIF where the safety action is available but there is either a higher PFD or a PFH, or 
- a disabled SIF where the safety action is completely disabled or the hazardous event has been induced. 

Note 3 to entry: When no fault tolerance is implemented, all dangerous failures lead to a disabled SIF.

3.2.12

dependent failure

failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it

Note 1 to entry: Two events A and B are dependent if the probability of occurrence of A and B, $P(A \text{ and } B)$, is greater than $P(A) \times P(B)$.

Note 2 to entry: See [9.4.2](#) and IEC 61511-3:2016, Annex J for consideration of dependent failures between protection layers.

Note 3 to entry: Dependent failures include common cause.

3.2.13

detected revealed overt

relating to hardware and software failures or faults which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods

Note 1 to entry: There are some differences in the use of these terms:

- Overt is used for failures or faults which announce themselves when they occur (e.g., due to the change of state). The repair of such failures can begin as soon as they have occurred.
- Detected is used for failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, operator intervention like physical inspection and manual tests). The repair of such failures can begin only after they have been revealed. See Note 2 for the specific use of this term in IEC 61511.
- Revealed is used for failures or faults that become evident due to being overt or as a result of being detected.

Note 2 to entry: When the detection is very fast (e.g., by diagnostic tests) then the detected failures or faults can be considered to be overt failures or faults.

When the detection is not very fast (e.g., by proof tests) the detected failures or faults cannot be considered to be overt failures or faults when addressing safety integrity levels.

Note 3 to entry: A dangerous revealed failure can only be treated as a safe failure if effective measures, automatic or manual, are taken in a short enough time to maintain process safety.

3.2.14

device

hardware, with or without software, capable of performing a specified function

Note 1 to entry: Examples are sensors, final elements and manual switches.

3.2.14.1

field device

SIS or BPCS device connected directly to the process or located in close proximity to the process

Note 1 to entry: Examples are sensors, final elements and manual switches.

3.2.15

diagnostics

frequent (in relation to the process safety time) automatic test to reveal faults

3.2.15.1

diagnostic coverage A_1

DC

A_1 fraction of dangerous failures rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof tests

Note 1 to entry: Diagnostic coverage is typically applied to SIS devices or SIS subsystems. E.g., the diagnostic coverage is typically determined for a sensor, final element or a logic solver.

Note 2 to entry: For safety applications the diagnostic coverage is typically applied to dangerous failures of SIS devices or SIS subsystems. For example, the diagnostic coverage for the dangerous failures of a device is $DC = \lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate. For a

SIS subsystem with internal redundancy, DC is time dependant: $DC(t) = \lambda_{DD}(t)/\lambda_{DT}(t)$

Note 3 to entry: When the diagnostic coverage (DC) and the total dangerous failure rate (λ_{DT}) are given, the detected (λ_{DD}) and undetected dangerous failures (λ_{DU}) can be computed as follows:

$$\lambda_{DD} = DC \times \lambda_{DT} \text{ and } \lambda_{DU} = (1-DC) \times \lambda_{DT}.$$

3.2.16

diversity

different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical means, different programming techniques, or different design approaches.

3.2.17

error

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

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.2.18

failure

loss of ability to perform as required

Note 1 to entry: A failure of a device is an event that results in a fault state of that device.

Note 2 to entry: When the loss of ability is caused by a latent fault, the failure occurs when a particular set of circumstances is encountered.

Note 3 to entry: Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure

Note 4 to entry:  Failures are either random or systematic (see [3.2.59](#) and [3.2.81](#)). 

[SOURCE: IEC 60050-192:2015, 192-03-01, modified - Notes to entry have been changed]

3.2.18.1

failure mode

manner in which failure occurs

Note 1 to entry: A failure mode may be defined by the function lost or the state transition that occurred.

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.2.19

fault

inability to perform as required, due to an internal state

Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life-cycle, such as specification, design, manufacture or maintenance.

Note 2 to entry: A fault of a device results in a failure when a particular set of circumstances is encountered.

[SOURCE: IEC 60050-192:2015, 192-04-01, modified - Some notes to entry have been changed, others have been deleted]

3.2.20

fault avoidance

use of techniques and procedures which aim to avoid the introduction of faults during any phase of the SIS safety life-cycle

3.2.20.1

fault exclusion

elimination from further consideration of faults due to improbable failure modes

Note 1 to entry: Further information about fault exclusion can be found in ISO 13849-1 and ISO 13849-2. After those standards fault exclusion can be based on

- the technical improbability of occurrence of some faults,
- generally accepted technical experience, independent of the considered application;
- technical requirements related to the application and the specific hazard.

Note 2 to entry: Failure modes, identified in the devices performing the safety function, can be excluded because their related dangerous failure rate(s) are very low compared to the target failure measure for the safety function under consideration. That is, the sum of the dangerous failure rates of all serial devices on which fault exclusion is being claimed, generally cannot exceed more than 1 % of the target failure measure.

3.2.21

fault tolerance

ability of a functional item to continue to perform a required function in the presence of faults or errors

3.2.22

final element

part of the BPCS or SIS that implements the physical action necessary to achieve or maintain a safe state

Note 1 to entry: Examples are valves, switch gear, and motors, including their auxiliary elements (such as solenoid valve and actuator used to operate a valve).

3.2.23

functional safety

part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers

3.2.24

functional safety assessment

FSA

investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers

3.2.25

functional safety audit

systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

Note 1 to entry: A functional safety audit may be carried out as part of a FSA.

3.2.26

hardware safety integrity

part of the safety integrity of the SIS relating to random hardware failures in a dangerous mode of failure

Note 1 to entry: **[A1]** The two failure measures that are relevant in this context are the average frequency of dangerous failure and the average probability of failure on demand. **[A1]**

Note 2 to entry: See [3.2.82](#).

Note 3 to entry: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.27

harm

injury or damage to the health of people, or damage to property or to the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.2.27.1

harmful event

hazardous event which has caused harm

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property, or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred. A hazardous event which has caused harm is termed a harmful event.

3.2.28

hazard

potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (e.g., fire and explosion) and also those that have a long-term effect on a person's health (e.g., release of a toxic substance or radioactivity).

[SOURCE: ISO/IEC Guide 51:2014, 3.2, modified - Note 1 to entry has been added]

3.2.28.1

hazardous event

event that can cause harm

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

[SOURCE: ISO/IEC Guide 51:2014: 3.3, modified - see Note 1]

3.2.28.2

hazardous situation

circumstance in which people, property or the environment are exposed to one or more hazards

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.2.29

human error

intended or unintended human action or inaction that produces an inappropriate result

Note 1 to entry: Mistakes, slips, and lapses are examples of human errors.

Note 2 to entry: This excludes malicious action.

3.2.30

impact analysis

activity of determining the effect that a change to a function or component will have to other functions or components in the system as well as in other systems

3.2.31

independent organization

organization that is separate and distinct, by management and other resources, from the organizations responsible for the activities that take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation

3.2.32

independent person

person who is separate and distinct from the activities which take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation and does not have direct responsibility for those activities

3.2.33

input function

function which monitors the process and its associated equipment in order to provide input information for the logic solver

Note 1 to entry: An input function could be a manual function.

3.2.34

instrument

apparatus used in performing an action (typically found in instrumented systems)

3.2.34.1

instrumented system

system composed of sensors (e.g., pressure, flow, temperature transmitters), logic solvers (e.g., programmable controllers, distributed control systems, discrete controllers), and final elements (e.g., control valves, motor control circuits)

Note 1 to entry: Instrumented systems perform instrumented functions including control, monitoring, alarm and protective functions. Instrumented systems can be SIS (see [3.2.67](#)) or BPCS (see [3.2.3](#)).

3.2.35

logic function

function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions)

Note 1 to entry: Logic functions provide the transformation from one or more input functions to one or more output functions.

Note 2 to entry: For further guidance, see IEC 61131-3:2012 and IEC 60617-12:1997.

3.2.36

logic solver

part of either a BPCS or SIS that performs one or more logic function(s)

Note 1 to entry: In IEC 61511 the following terms for logic solvers are used:

- electrical logic systems for electro-mechanical technology;
- electronic logic systems for electronic technology;
- PE logic system for programmable electronic systems.

Note 2 to entry: Examples are: electrical systems, electronic systems, programmable electronic systems, pneumatic systems, and hydraulic systems. Sensors and final elements are not part of the logic solver.

3.2.36.1

safety configured PE logic solver

general purpose industrial grade PE logic solver which is specifically configured for use in safety applications

Note 1 to entry: Further guidance can be found in [11.5](#).

3.2.37

maintenance/engineering interface

hardware and software provided to allow proper SIS maintenance or modification

Note 1 to entry: Maintenance/engineering interface can include instructions and diagnostics which may be found in software, programming terminals with appropriate communication protocols, diagnostic tools, indicators, bypass devices, test devices, and calibration devices.

3.2.37.1

mean repair time

MRT

expected overall repair time

Note 1 to entry: MRT encompasses the times (b), (c) and (d) of the times for MTTR (see [3.2.37.2](#)).

3.2.37.2

mean time to restoration

MTTR

expected time to achieve restoration

Note 1 to entry: MTTR encompasses:

- the time to detect the failure (a);
- the time spent before starting the repair (b);
- the effective time to repair (c);
- the time before the component is put back into operation (d).

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

3.2.37.3

maximum permitted repair time

MPRT

maximum duration allowed to repair a fault after it has been detected

Note 1 to entry: The MRT may be used as MPRT but the MPRT may be defined without regards to the MRT:

- A MPRT smaller than the MRT can be chosen to decrease the probability of hazardous event.

— A MPRT greater than the MRT can be chosen if the probability of hazardous event can be relaxed.

Note 2 to entry: When a MPRT has been defined it can be used in place of the MRT for calculating the probability of random hardware failures.

3.2.38 mitigation

action that reduces the consequence(s) of a hazardous event

Note 1 to entry: Examples include emergency depressurization or closing ventilation dampers on detection or confirmed fire or gas leak or initiation of deluge on confirmed fire detection.

3.2.39 mode of operation (of a SIF)

way in which a SIF operates which may be either low demand mode, high demand mode or continuous mode

- a) **low demand mode:** mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year.
- b) **high demand mode:** mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year.
- c) **continuous mode:** mode of operation where the SIF retains the process in a safe state as part of normal operation.

3.2.39.1 demand mode SIF

SIF operating in low demand mode ([3.2.39 a\)](#)) or high demand mode ([3.2.39 b\)](#))

Note 1 to entry: In the event of a dangerous failure of the SIF, a hazardous event can only occur

- if the failure is undetected and a demand occurs before the next proof test;
- if the failure is detected by the diagnostic tests but the related process and its associated equipment has not been moved to a safe state before a demand occurs.

Note 2 to entry: In high demand mode, it will normally be appropriate to use the continuous mode criteria.

Note 3 to entry: The safety integrity levels for SIF operating in demand mode are defined in [Tables 4](#) and [5](#).

3.2.39.2 continuous mode SIF

SIF operating in continuous mode ([3.2.39 c\)](#))

Note 1 to entry: In the event of a dangerous failure of the SIF a hazardous event will occur without further failure unless action is taken to prevent it within the process safety time.

Note 2 to entry: Continuous mode covers those SIF which implement continuous control to maintain functional safety.

Note 3 to entry: The safety integrity levels for SIF operating in continuous mode are defined in [Table 5](#).

3.2.40 module

self-contained part of a SIS application program (can be internal to a program or a set of programs) that performs a specified function (e.g., final element start/stop/test sequence, an application specific sequence within a SIF)

Note 1 to entry: In the context of IEC 61131-3:2012, a software module is a function or function block.

Note 2 to entry: Most modules have repetitive usage within an application program.

3.2.41

MooN

SIS, or part thereof, made up of “*N*” independent channels, which are so connected, that “*M*” channels are sufficient to perform the SIF

3.2.42

necessary risk reduction

risk reduction to be achieved by the SIS(s) and/or other protection layers to ensure that the tolerable risk is not exceeded

3.2.43

non-programmable system

(NP) system

system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software)

Note 1 to entry: Examples would include hard-wired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

3.2.44

operating environment

conditions inherent to the installation of a device that potentially affects its functionality and safety integrity, such as:

- external environment, e.g. , winterization needs, hazardous area classification;
- process operating conditions, e.g., extremes in temperature, pressure, vibration;
- process composition, e.g., solids, salts, or corrosives;
- process interfaces;
- integration within the overall plant maintenance and operating management systems;
- communication through-put, e.g., electro-magnetic interference; and
- utility quality, e.g., electrical power, air, hydraulics.

Note 1 to entry: Some process applications may have special operating environment requirements necessary to survive a major accident event. For example some equipment requires special enclosures, purging, or fire protection.

3.2.45

operating mode

process operating mode

any planned state of process operation, including modes such as start-up after emergency shutdown, normal start-up, operation, and shutdown, temporary operations, and emergency operation and shutdown

3.2.46

operator interface

means by which information is communicated between a human operator and the SIS (e.g., display interfaces, indicating lights, push-buttons, horns, alarms)

Note 1 to entry: The operator interface is sometimes referred to as the human-machine interface (HMI).

3.2.47

output function

function which controls the process and its associated equipment according to output information from the logic function

3.2.48

performance

accomplishment of a given action or task measured against the specification and the IEC 61511 series

3.2.49

phase

period within the SIS safety life-cycle where activities described in the IEC 61511 series take place

3.2.50

prevention

action that reduces the likelihood of occurrence of a hazardous event

3.2.51

prior use

documented assessment by a user that a device is suitable for use in a SIS and can meet the required functional and safety integrity requirements, based on previous operating experience in similar operating environments

Note 1 to entry: To qualify a SIS device on the basis of prior use, the user can document that the device has achieved satisfactory performance in a similar operating environment. Understanding how the equipment behaves in the operating environment is necessary to achieve a high degree of certainty that the planned design, inspection, testing, maintenance, and operational practices are sufficient.

Note 2 to entry: Proven in use is based on the manufacturer's design basis (e.g., temperature limit, vibration limit, corrosion limit, desired maintenance support) for his device. Prior use deals with device's installed performance within a process sector application in a specific operating environment which is often different than the manufacturer's design basis.

3.2.52

process risk

risk arising from the process conditions caused by abnormal events (including BPCS malfunction)

Note 1 to entry: The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e., the risk associated with functional safety).

Note 2 to entry: Process risk analysis is described in IEC 61511-3:2016. The main purpose of determining the process risk is to establish a reference point for the risk without taking into account the protection layers.

Note 3 to entry: Assessment of this risk can include associated human factor issues.

Note 4 to entry: This term equates to "EUC risk" in IEC 61508-4:2010.

3.2.52.1

process safety time

time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed

Note 1 to entry: This is a property of the process only. The SIF has to detect the failure and complete its action soon enough to prevent the hazardous event taking into account any process lag (e.g. cooling of a vessel).

3.2.53

programmable electronics

PE

item based on computer technology which may be comprised of hardware, software, and of input and/or output units

Note 1 to entry: This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories. Examples of process sector programmable electronics include:

- smart sensors and final elements;
- programmable electronic logic solvers including: