

INTERNATIONAL STANDARD



Functional safety – Safety instrumented systems for the process industry sector –
Part 1: Framework, definitions, system, hardware and software application programming requirements



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.



IEC 61511-1

Edition 2.0 2016-02
REDLINE VERSION

INTERNATIONAL STANDARD



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.01

ISBN 978-2-8322-3216-3

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	2
1 Scope.....	9
2 Normative references.....	14
3 Terms , definitions and abbreviations	15
3.1 Terms	15
3.2 Terms and definitions	15
3.3 Abbreviations	38
4 Conformance to the IEC 61511-1:2016.....	39
5 Management of functional safety.....	39
5.1 Objective	39
5.2 Requirements.....	39
5.2.1 General	39
5.2.2 Organization and resources.....	39
5.2.3 Risk evaluation and risk management.....	40
5.2.4 Safety planning	40
5.2.5 Implementing and monitoring.....	40
5.2.6 Assessment, auditing and revisions	41
5.2.7 SIS configuration management.....	44
6 Safety life-cycle requirements	44
6.1 Objectives.....	44
6.2 Requirements.....	45
6.3 Application program SIS safety life-cycle requirements	47
7 Verification	50
7.1 Objective	50
7.2 Requirements	50
8 Process H&RA.....	52
8.1 Objectives.....	52
8.2 Requirements.....	52
9 Allocation of safety functions to protection layers	53
9.1 Objectives.....	53
9.2 Requirements of the allocation process	54
~~9.3 Additional requirements for safety integrity level 4~~	~~56~~
9.3 Requirements on the basic process control system as a protection layer	56
9.4 Requirements for preventing common cause, common mode and dependent failures	58
10 SIS safety requirements specification (SRS).....	58
10.1 Objective	58
10.2 General requirements.....	58
10.3 SIS safety requirements	58
11 SIS design and engineering	60
11.1 Objective	61
11.2 General requirements.....	61
11.3 Requirements for system behaviour on detection of a fault.....	63
11.4 ~~Requirements for~~ Hardware fault tolerance	~~63~~

11.5	Requirements for selection of ~~components and subsystems~~ devices	65
11.5.1	Objectives	67
11.5.2	General requirements	67
11.5.3	Requirements for the selection of ~~components and subsystems~~ devices based on prior use	67
11.5.4	Requirements for selection of FPL programmable ~~components and subsystems~~ devices (e.g., field devices) based on prior use	69
11.5.5	Requirements for selection of LVL programmable ~~components and subsystems (for example, logic solvers)~~ devices based on prior use	69
11.5.6	Requirements for selection of FVL programmable ~~components and subsystems (for example, logic solvers)~~ devices	70
11.6	Field devices	70
11.7	Interfaces	71
11.7.1	General	71
11.7.2	Operator interface requirements	71
11.7.3	Maintenance/engineering interface requirements	72
11.7.4	Communication interface requirements	73
11.8	Maintenance or testing design requirements	73
11.9	~~SIF probability of failure~~ Quantification of random failure	74
12	~~Requirements for application software, including selection criteria for utility software~~	
12.1	~~Application software safety life cycle requirements~~	
12.2	~~Application software safety requirements specification~~	
12.3	~~Application software safety validation planning~~	
12.4	~~Application software design and development~~	
12.5	~~Integration of the application software with the SIS subsystem~~	
12.6	~~FPL and LVL software modification procedures~~	
12.7	~~Application software verification~~	
12	SIS application program development	92
12.1	Objective	92
12.2	General requirements	92
12.3	Application program design	93
12.4	Application program implementation	94
12.5	Requirements for application program verification (review and testing)	95
12.6	Requirements for application program methodology and tools	96
13	Factory acceptance test (FAT)	76
13.1	Objective	96
13.2	Recommendations	96
14	SIS installation and commissioning	98
14.1	Objectives	98
14.2	Requirements	98
15	SIS safety validation	99
15.1	Objective	99
15.2	Requirements	99
16	SIS operation and maintenance	102
16.1	Objectives	102
16.2	Requirements	102
16.3	Proof testing and inspection	104
16.3.1	Proof testing	104
16.3.2	Inspection	104

16.3.3	Documentation of proof tests and inspection	105
17	SIS modification	105
17.1	Objectives	105
17.2	Requirements	106
18	SIS decommissioning	106
18.1	Objectives	106
18.2	Requirements	107
19	Information and documentation requirements	107
19.1	Objectives	107
19.2	Requirements	107
	Bibliography	108

Figure 1	– Overall framework of the IEC 61511 series	8
----------	---	---

Figure 2	– Relationship between IEC 61511 and IEC 61508	11
----------	--	----

Figure 3	– Detailed relationship between IEC 61511 and IEC 61508 (see clause 1)	12
----------	--	----

Figure 4	– Relationship between safety instrumented functions and other functions	14
----------	--	----

Figure 5	– Programmable electronic system (PES): structure and terminology	28
----------	---	----

Figure 7 6	– Example of SIS architectures comprising three SIS subsystems	32
------------	--	----

Figure 8 7	– SIS safety life-cycle phases and FSA stages	45
------------	---	----

Figure 10 8	– Application program safety life-cycle and its relationship to the SIS safety life-cycle	48
-------------	---	----

Figure 9	– Typical protection layers and risk reduction methods found in process plants means	57
----------	--	----

Figure 11	– Application software safety life cycle (in realization phase)	
-----------	---	--

Figure 12	– Software development life cycle (the V-model)	
-----------	---	--

Figure 13	– Relationship between the hardware and software architectures of SIS	
-----------	---	--

Table 1	– Abbreviations used in IEC 61511	38
---------	---	----

Table 2	– SIS safety life-cycle overview (1 of 2)	46
---------	---	----

Table 3 4	– Application program safety life-cycle: overview (1 of 2)	49
-----------	--	----

Table 3 4	– Safety integrity levels requirements: probability of failure on demand PFDavg	54
-----------	---	----

Table 4 5	– Safety integrity levels requirements: average frequency of dangerous failures of the SIF	54
-----------	--	----

Table 5	– Minimum hardware fault tolerance of PE logic solvers	
---------	--	--

Table 6	– Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers	
---------	---	--

Table 6	– Minimum HFT requirements according to SIL	66
---------	---	----

Table 7	– Application software safety life cycle: overview	
---------	--	--

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY –
SAFETY INSTRUMENTED SYSTEMS
FOR THE PROCESS INDUSTRY SECTOR –****Part 1: Framework, definitions, system,
hardware and ~~software~~ application programming requirements****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.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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.

The contents of the corrigendum of September 2016 have been included in this copy.

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

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 ~~requires~~ 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 ~~so that their contribution can be taken into account when considering with respect to~~ the performance requirements for the SIS. The SIS includes all ~~components and subsystems~~ 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 ~~(see Annex A)~~.

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum ~~standards~~ 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:

- ~~requires~~ addresses that a H&RA is carried out to identify the overall safety requirements;
- ~~requires~~ addresses that an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented ~~methods~~ 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 ~~requirements~~ regulations, these take precedence over the requirements defined in the IEC 61511 series.

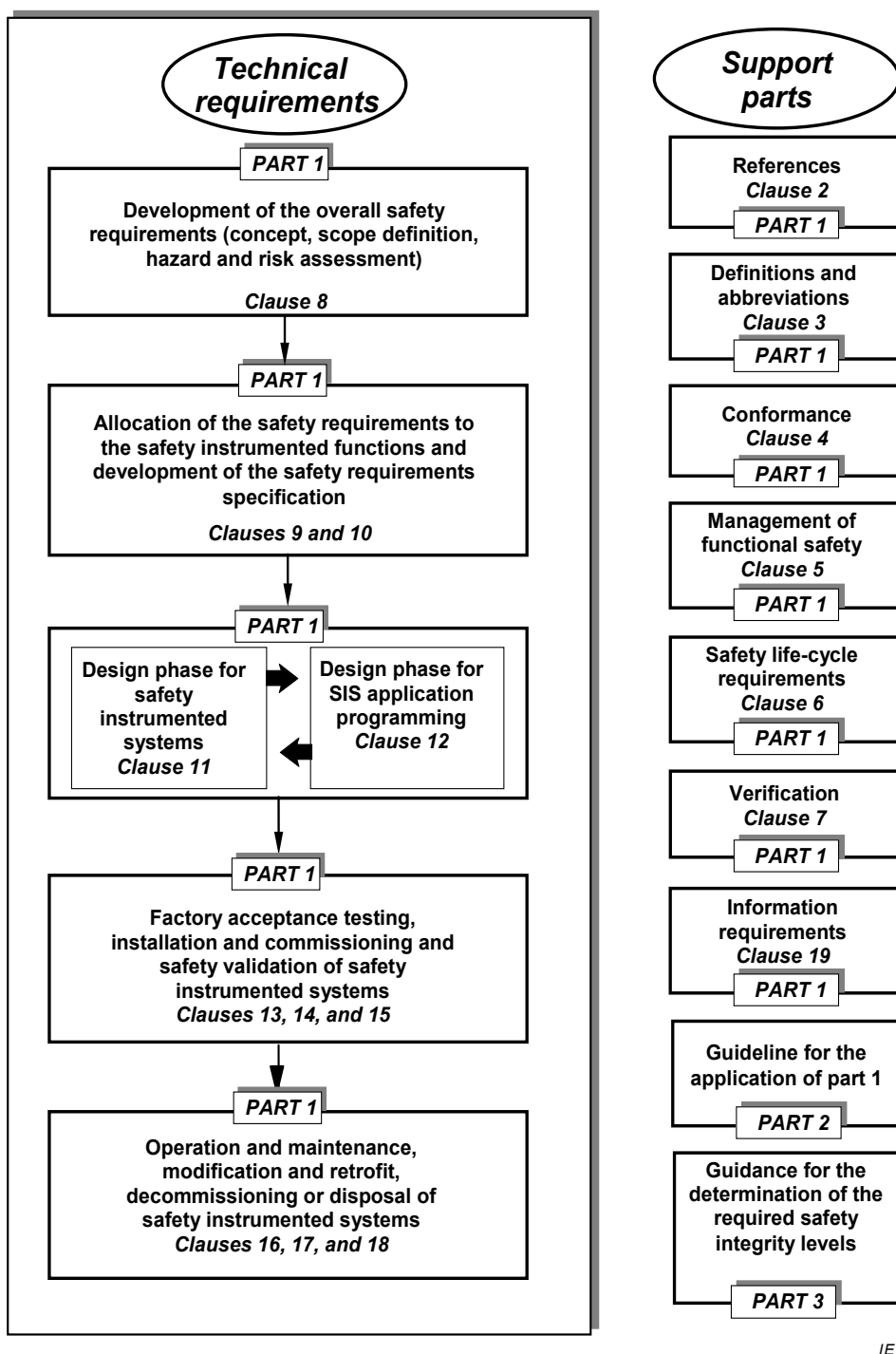


Figure 1 – Overall framework of the IEC 61511 series

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and ~~software~~ 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 ~~place and/~~ 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 ~~equipment~~ 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 ~~software is~~ programs are developed for systems having limited variability language or when using fixed ~~programmes~~ 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 refining~~, oil and gas ~~production~~, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;

NOTE 1 Within the process sector some applications, ~~(for example, off shore)~~, 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 ~~means~~ methods;
- h) specifies life-cycle requirements for system architecture and hardware configuration, application ~~software~~ programming, and system integration;
- i) specifies requirements for application ~~software~~ programming for users and integrators of SISs ~~(clause 12)~~.
In particular, requirements for the following are specified:

- ~~safety life-cycle phases and activities that are to be applied during the design and development of the application software (the software safety life-cycle model). These requirements include the application of measures and techniques, which are intended to avoid faults in the software and to control failures which may occur;~~
- ~~information relating to the software safety validation to be passed to the organization carrying out the SIS integration;~~

- ~~— preparation of information and procedures concerning software needed by the user for the operation and maintenance of the SIS;~~
- ~~— procedures and specifications to be met by the organization carrying out modifications to safety software;~~

- 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) ~~requires~~ **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 ~~methods~~ **means**.

- o) establishes numerical targets for average probability of failure on demand (**in demand mode**) and **average** frequency of dangerous failures ~~per hour for the safety integrity levels (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) ~~requires~~ **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;

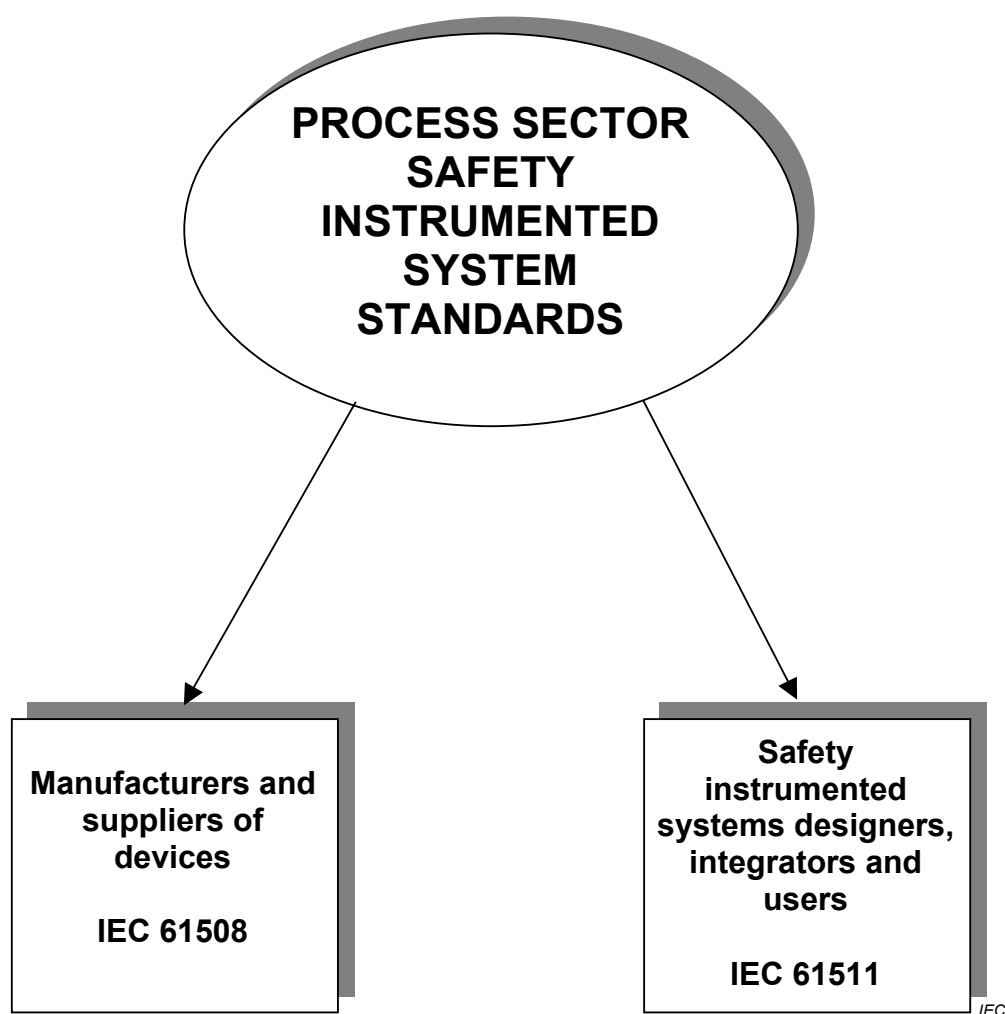


Figure 2 – Relationship between IEC 61511 and IEC 61508

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

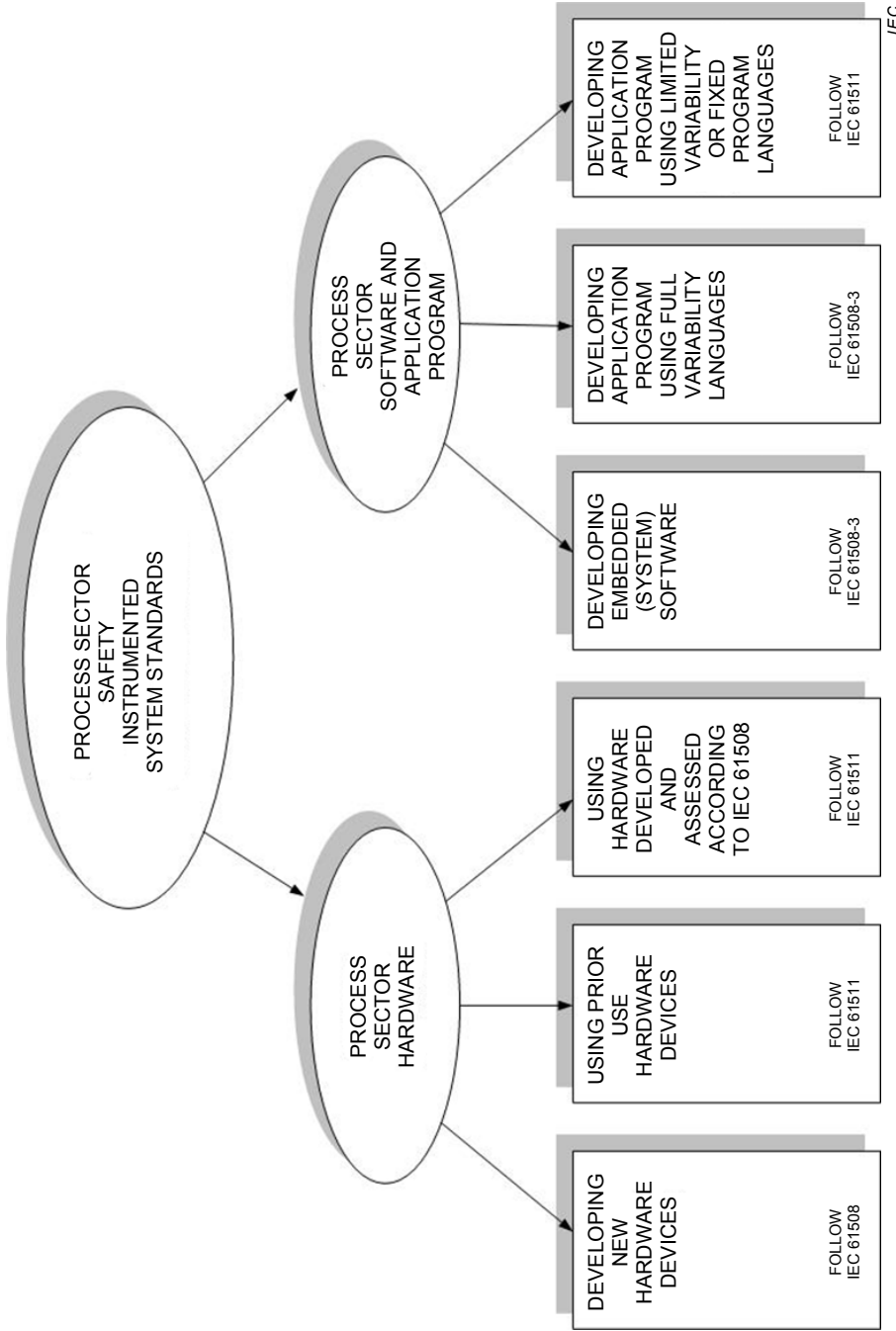
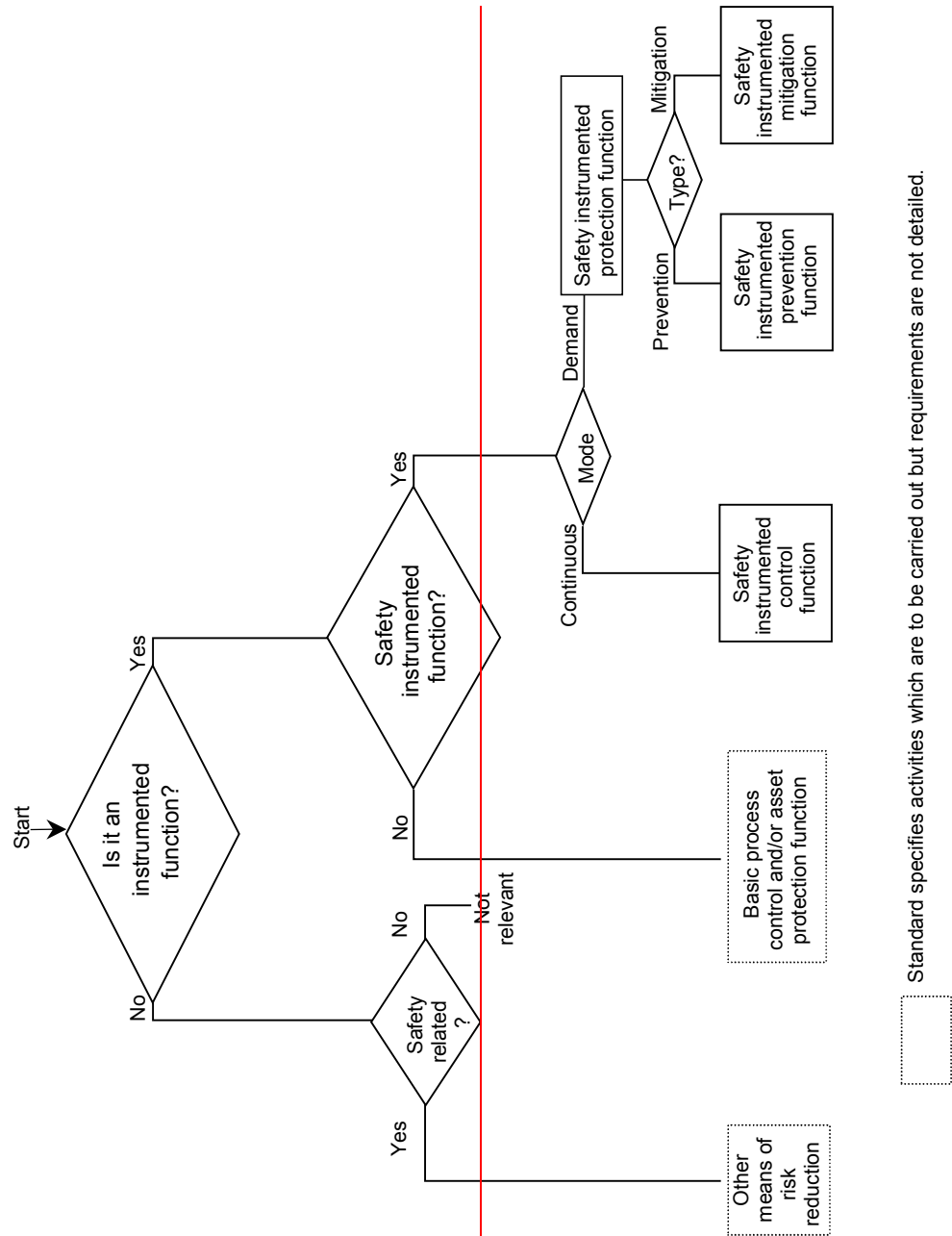


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508 (~~see clause 4~~)

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



IEC 3243/02

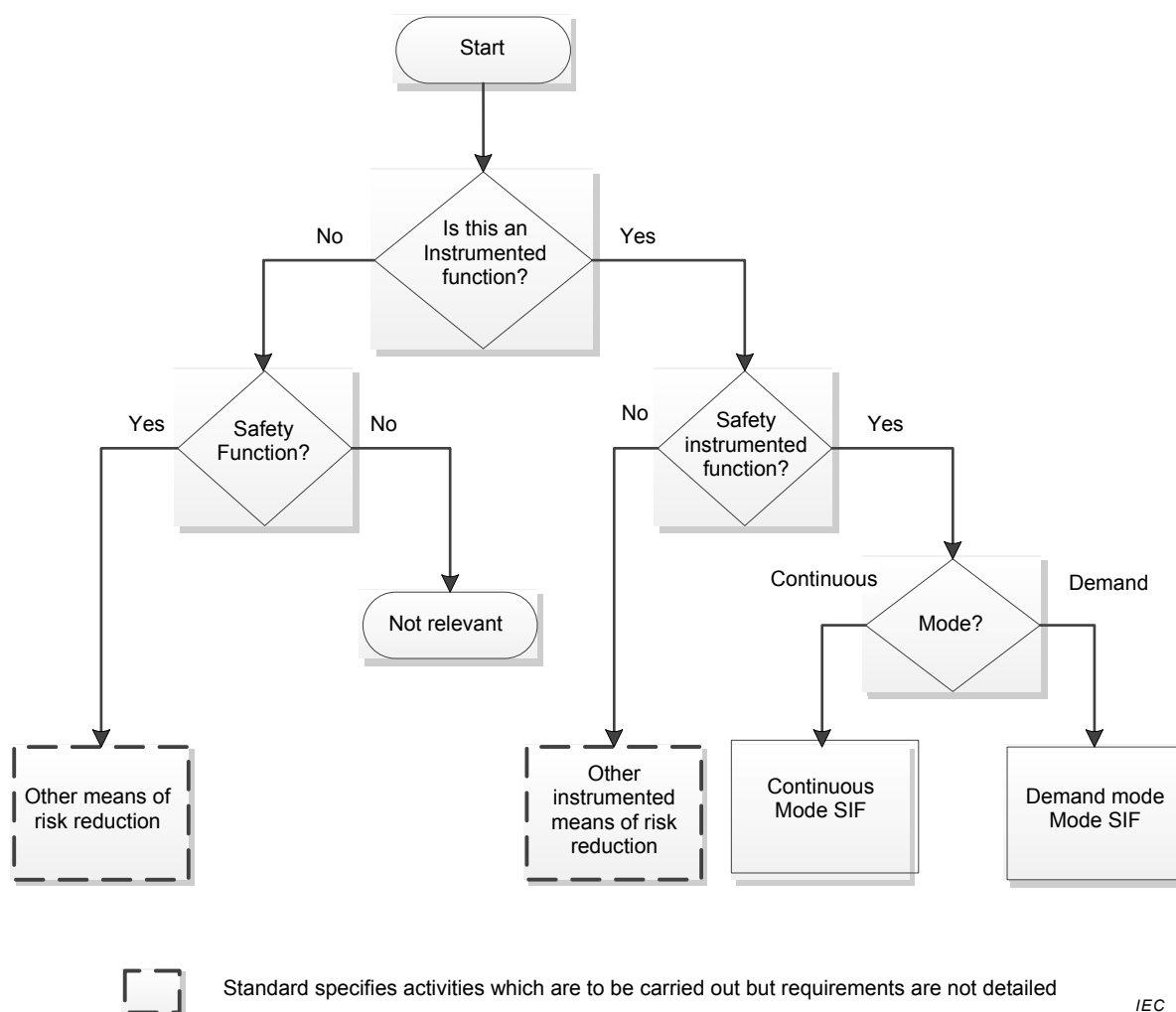


Figure 4 – Relationship between safety instrumented functions and other functions

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 60654-1:1993, Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions~~

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

~~IEC 60654-3:1998, Industrial-process measurement and control equipment – Operating conditions – Part 3: Mechanical influences~~

~~IEC 61326-1:Electrical equipment for measurement, control and laboratory use – EMC 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*

~~IEC 61511-2: Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines in the application of IEC 61511-1~~

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

~~arrangement~~ specific configuration of hardware and/or software ~~elements~~ components in a system

~~NOTE This term differs from the definition in IEC 61508-4 to reflect differences in the process sector terminology.~~

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 ~~arrangement of software programs~~ or the internal structure of SIS application programs.

3.2.2

asset protection

function allocated to a system ~~design~~ 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 ~~with a claimed SIL ≥ 1~~

~~NOTE See Clause A.2.~~

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

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

Note 1 to entry: The ~~elements~~ devices within a channel could include input/output (I/O) ~~modules~~ devices, logic ~~systems~~ solvers (~~see 3.2.40~~), 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.

~~3.2.5~~
~~coding~~
~~see “programming”~~

3.2.6 common cause

3.2.6.1

common cause failures, pl

~~failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure~~
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

~~failure of two or more channels in the same way, causing the same erroneous result~~
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.

~~3.2.8~~

~~configuration~~

~~see "architecture"~~

3.2.9

configuration management

discipline of identifying the components and the arrangements of those components of an evolving ~~(hardware and software)~~ 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 ~~input devices~~ 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 ~~has the potential to put the safety instrumented system in a hazardous or fail-to-function state~~ impedes or disables a given safety action

~~NOTE Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall hazardous or fail-to-function state.~~

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 (demand mode of operation) or a higher likelihood of initiating a hazardous event (continuous mode of operation), or
- a disabled SIF where the safety action is completely disabled (demand mode of operation) or the hazardous event has been induced (continuous mode of operation).

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, ~~where $P(z)$ is the probability of event z, only~~ 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 ~~(see 3.2.6)~~.

3.2.13

detected revealed overt

relating to hardware and software failures or faults, which are not hidden because they announce themselves or are ~~detected by the diagnostic tests or~~ 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: In IEC 61511 and except when the context suggests another meaning, the term *dangerous detected failures/faults* is related to dangerous failures detected by diagnostic tests.

Note 3 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 4 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

~~functional unit of~~ hardware, with or without software, ~~or both,~~ capable of performing a specified ~~purpose~~ function

Note 1 to entry: Examples are ~~field devices; equipment connected to the field side of the SIS I/O terminals; such equipment includes~~ sensors, logic solvers, final elements, ~~and those~~ operator interfaces ~~devices hard wired to SIS I/O terminals~~ and field wiring.

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

diagnostics coverage

DC

~~ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests.~~ fraction of dangerous failures rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof tests.

~~NOTE 1 The diagnostic coverage is used to compute the detected ($\lambda_{\text{detected}}$) and undetected failure rates ($\lambda_{\text{undetected}}$) from the total failure rate ($\lambda_{\text{total failure rate}}$) as follows: $\lambda_{\text{detected}} = \text{DC} \times \lambda_{\text{total failure rate}}$ and $\lambda_{\text{undetected}} = (1 - \text{DC}) \times \lambda_{\text{total failure rate}}$.~~

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

Note 2 to entry: For safety applications the diagnostics coverage is typically applied to ~~the safe and~~ dangerous failures of ~~a component~~ SIS devices or SIS subsystems. For example, the diagnostics coverage for the dangerous failures of a ~~component or subsystem~~ device is $\text{DC} = \lambda_{\text{DD}} / \lambda_{\text{DT}}$, 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: $\text{DC}(t) = \lambda_{\text{DD}}(t) / \lambda_{\text{DT}}(t)$.

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

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

3.2.16

diversity

different means of performing a required function

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

3.2.17

electrical/electronic/programmable (E/E/PE)

~~based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology~~

~~NOTE The term is intended to cover any and all devices or systems operating on electrical principles and would include~~

- ~~— electro-mechanical devices (electrical);~~
- ~~— solid state non-programmable electronic devices (electronic);~~
- ~~— electronic devices based on computer technology (programmable electronic) (see 3.2.55).~~

3.2.17

error

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

~~NOTE Adapted from IECV 191-05-24 by excluding the notes.~~

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

3.2.19

external risk reduction facilities

~~measures to reduce or mitigate the risks, which are separate and distinct from the SIS~~

~~NOTE 1 Examples include a drain system, fire wall, bund (dike).~~

~~NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector terminology.~~

3.2.18

failure

~~termination of the ability of a functional unit to perform a required function~~ loss of ability to perform as required

~~NOTE 1 This definition (excluding these notes) matches ISO/IEC 2382-14-01-09:1997.~~

~~NOTE 2 For further information, see IEC 61508-4.~~

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 3.2.61 and 3.2.83).

[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

~~abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function~~ inability to perform as required, due to an internal state

~~NOTE IEC 101-05-01 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. [ISO/IEC 2382-14-01-09]~~

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 ~~unit~~ item to continue to perform a required function in the presence of faults or errors

~~NOTE The definition in IEC 191-15-05 refers only to sub-item faults. See the note for the term fault in 3.2.21.~~

~~[ISO/IEC 2382-14-04-06]~~

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 ~~if involved in the safety instrumented function 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

~~NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

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

~~NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

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.

3.2.28

functional unit

~~entity of hardware or software, or both, capable of accomplishing a specified purpose~~

~~NOTE 1 In IEC 191-01-01 the more general term "item" is used in place of functional unit. An item may sometimes include people.~~

~~NOTE 2 This is the definition given in ISO/IEC 2382-14-01-01.~~

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: ~~The term relates to failures in a dangerous mode. That is, those failures of a safety instrumented function that would impair its safety integrity.~~ The two ~~parameters~~ failure measures that are relevant in this context are the ~~overall~~ average frequency of dangerous failure ~~rate~~ (continuous mode of operation) and the average probability of failure ~~to operate~~ on demand (demand mode of operation).

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

~~physical~~ injury or damage to the health of people, ~~either directly or indirectly, as a result of or~~ damage to property or to the environment

~~NOTE This definition matches ISO/IEC Guide 51.~~

[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 This definition (without notes) matches 3.4 of ISO/IEC Guide 51.~~

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

~~mistake~~

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

~~NOTE This is the definition found in ISO/IEC 2382-14-02-03 and differs from that given in IEC 191-05-25 by the addition of "or inaction".~~

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

3.2.34**independent department**

~~department which is separate and distinct from the departments responsible for the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation~~

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**

NOTE 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. ~~In special cases,~~ 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 ~~systems~~ 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

~~where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands~~ 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 2—In demand mode applications where the demand rate is more frequent than once per year, the hazard rate will not be higher than the dangerous failure rate of the safety instrumented function. In such a case, it will normally be appropriate to use the continuous mode criteria.~~

~~NOTE 3—The target failure measures for safety instrumented functions operating in demand mode and continuous mode are defined in Tables 3 and 4.~~

~~NOTE 4—This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

Note 1 to entry: In the event of a dangerous failure of the SIF a ~~potential hazard~~ 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 assembly of hardware components that performs a specified hardware function (i.e., digital input module, analogue output module), or reusable application program (can be internal to a program or a set of programs) that support a specific function, for example, portion of a computer program that carries out a specific function~~

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—This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.~~

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 ~~required to ensure that the risk is reduced to a tolerable level~~ 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., ~~GRTs~~ 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).

3.2.49**~~other technology safety related systems~~**

~~safety related systems that are based on a technology other than electrical, electronic, or programmable electronic~~

NOTE – A relief valve is “another technology safety related system”. “Other technology safety related systems” may include hydraulic and pneumatic systems.

3.2.47**output function**

function which controls the process and its associated equipment according to ~~final actuator~~ 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 ~~frequency~~ likelihood of occurrence of a hazardous event

3.2.51**prior use**

~~see “proven-in-use” (see 3.2.60)~~

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 ~~should~~ 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**

~~electronic component or device forming part of a PES and~~ item based on computer technology. ~~The term encompasses both~~ which may be comprised of hardware, software, and of input and/or output units

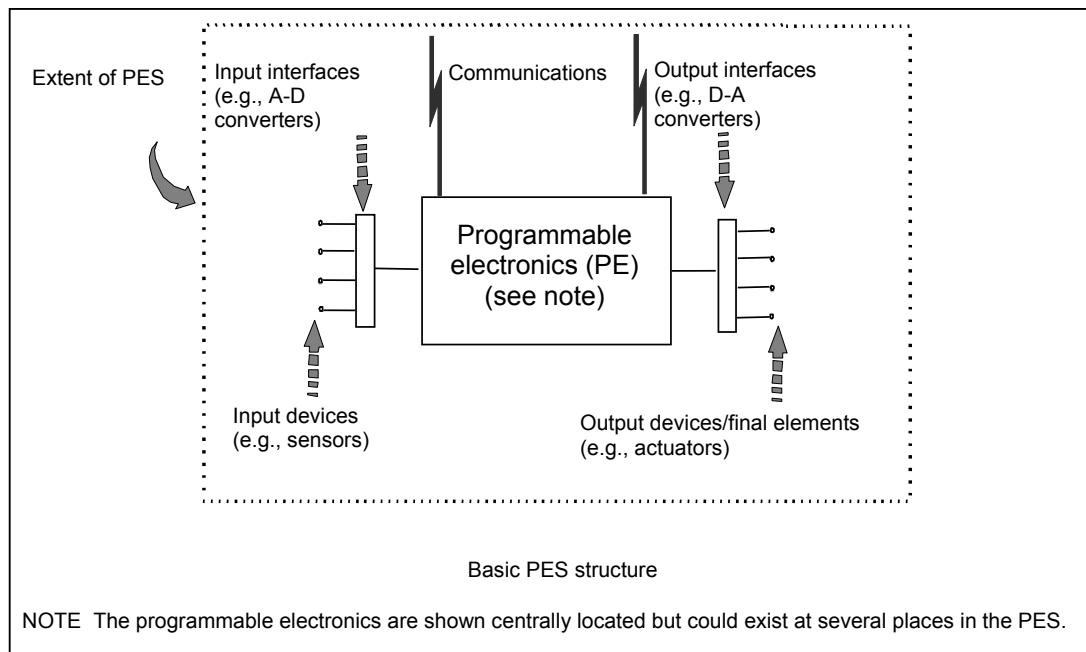
Note 1 to entry: This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories. Examples of process sector programmable electronics include:

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

~~NOTE 2 This term differs from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

3.2.54 programmable electronic system PES

system for control, protection or monitoring based on one or more programmable electronic devices, including all ~~elements~~ **devices** of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices (see Figure 5)



IEC

Figure 5 – Programmable electronic system (PES): structure and terminology

3.2.55 programming coding

process of designing, writing and testing a set of instructions for solving a problem or processing data

Note 1 to entry: In the IEC 61511 series, programming is typically associated with PE.

3.2.56 proof test

periodic test performed to ~~reveal undetected~~ **detect dangerous hidden** faults in a SIS so that, if necessary, ~~the system a repair can be restored to its designed functionality~~ **restore the system to an 'as new' condition or as close as practical to this condition**

3.2.57 protection layer

any independent mechanism that reduces risk by control, prevention or mitigation

Note 1 to entry: It ~~could~~ **can** be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical ~~engineering~~ mechanism such as a relief valve, a SIS or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions (see Figure 9).

~~3.2.60~~

~~proven-in-use~~

~~when a documented assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system (see "prior use" in 11.5)~~

~~NOTE This term deviates from IEC 61508 to reflect differences in process sector technology.~~

3.2.58

quality

totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs

Note 1 to entry: See ISO 9000 for more details.

3.2.59

random hardware failure

failure, occurring at a random time, which results from ~~a variety~~ **one or more** of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e., random) times.

Note 2 to entry: ~~A major distinguishing feature between random hardware failures and systematic failures (see 3.2.85) is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted but systematic failures, by their very nature, cannot be predicted. That is, system failure rates arising from random hardware failures can be quantified but those arising from systematic failures cannot be statistically quantified because the events leading to them cannot easily be predicted.~~

Two major differences distinguish the random hardware failures and the systematic failures:

- a random hardware failure involves only the system itself while a systematic failure involves both the system itself (a fault) and a particular condition (see 3.2.81). Then a random hardware failure is characterized by a single reliability parameter (i.e., the failure rate) while a systematic failure is characterized by two reliability parameters (i.e., the probability of the pre-existing fault and the hazard rate of the particular condition).
- a systematic failure can be eliminated after being detected while random hardware failures cannot.

This implies that the reliability parameters of random hardware failures can be estimated from field feedback while it is very difficult to do the same for systematic failures. A qualitative approach is preferred for systematic failures.

[SOURCE: IEC 61508-4:2010, 3.6.5, modified – The notes have been changed]

3.2.60

redundancy

~~use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy)~~

the existence of more than one means for performing a required function or for representing information

Note 1 to entry: Examples are the use of duplicate ~~functional components~~ **devices** and the addition of parity bits.

Note 2 to entry: Redundancy is used primarily to improve reliability or availability.

~~NOTE 3 The definition in IEC 191-15-01 is less complete [ISO/IEC 2382-14-01-11].~~

~~NOTE 4 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

[SOURCE: IEC 61508-4:2010, 3.4.6]

3.2.61

risk

combination of the ~~frequency~~ probability of occurrence of harm and the severity of that harm

~~NOTE For more discussion on this concept, see Clause 8.~~

Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation, the occurrence of a hazardous event, and the possibility to avoid or limit the harm.

[SOURCE: ISO/IEC Guide 51:2014, 3.8]

3.2.62

safe failure

failure which ~~does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state~~ favours a given safety action

~~NOTE 1 Whether or not the potential is realized may depend on the channel architecture of the system.~~

~~NOTE 2 Other names used for safe failure are nuisance failure, spurious trip failure, false trip failure or fail-to-safe failure.~~

Note 1 to entry: A failure is "safe" only with regard to a given safety function.

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

- operation where the safety action is available but with a higher probability of success on demand (demand mode of operation) or a lower likelihood to cause a hazardous event (continuous mode of operation);
- a spurious operation where the safety action is initiated.

Note 3 to entry: When no fault tolerance is implemented, safe failures result in the initiation of the safety action regardless of the process condition. This is also known as a spurious trip.

Note 4 to entry: A spurious trip may be safe with regard to a given safety function but may be dangerous with regard to another safety function.

Note 5 to entry: Spurious trips may also have detrimental effects on the production availability of the process.

~~3.2.65.1~~

~~safe failure fraction~~

~~fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure~~

3.2.63

safe state

state of the process when safety is achieved

Note 1 to entry: Some states are safer than others and in going from a ~~potentially~~ hazardous condition to the final safe state, or in going from the nominal safe condition to a hazardous condition, the process may have to go through a number of intermediate safe-states.

Note 2 to entry: For some situations, a safe state exists only so long as the process is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

Note 3 to entry: A state which is safe with regard to a given safety function may increase the probability of hazardous event with regard to another given safety function. In this case, the maximum allowable average spurious trip frequency (see 10.3.2) for the first function can consider the potential increased risk associated with the other function.

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

3.2.64

safety

freedom from ~~unacceptable~~ risk which is not tolerable

Note 1 to entry: ~~This definition is~~ According to ISO/IEC Guide 51, the terms "acceptable risk" and "tolerable risk" are considered to be synonymous.

[SOURCE: ISO/IEC Guide 51:2014, 3.14, modified – The note has been added]

3.2.65

safety function

function to be implemented by ~~an SIS, other technology safety related system or external risk reduction facilities~~ one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

~~NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

3.2.69

safety instrumented control function

~~safety instrumented function with a specified SIL operating in continuous mode which is necessary to prevent a hazardous condition from arising and/or to mitigate its consequences~~

3.2.70

safety instrumented control system

~~instrumented system used to implement one or more safety instrumented control functions~~

~~NOTE Safety instrumented control systems are rare within the process industries. Where such systems are identified, they will need to be treated as a special case and designed on an individual basis. The requirements within this standard should apply but further detailed analysis may be required to demonstrate that the system is capable of achieving the safety requirements.~~

3.2.66

safety instrumented function

SIF

~~safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function~~ to be implemented by a safety instrumented system (SIS)

Note 1 to entry: A SIF is designed to achieve a required SIL which is determined in relationship with the other protection layers participating to the reduction of the same risk.

3.2.67

safety instrumented system

SIS

~~instrumented system used to implement one or more SIFs. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s) (for example, see Figure 7)~~

~~NOTE 1 This can include either safety instrumented control functions or safety instrumented protection functions or both.~~

~~NOTE 2 Manufacturers and suppliers of SIS devices should refer to Clause 1 a) through d) inclusive.~~

~~NOTE 4 See Clause A.2.~~

~~NOTE 5 When a human action is a part of an SIS, the availability and reliability of the operator action must be specified in the SRS and included in the performance calculations for the SIS. See IEC 61511-2 for guidance on how to include operator availability and reliability in SIL calculations.~~

Note 1 to entry: A SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s) (e.g., see Figure 6). It also includes communication and ancillary equipment (e.g., cables, tubing, power supply, impulse lines, heat tracing).

Note 2 to entry: A SIS may include software.

Note 3 to entry: A SIS may include human action as part of a SIF (see ISA TR84.00.04:2015, part 1).

SIS architecture and safety instrumented function example with different devices shown

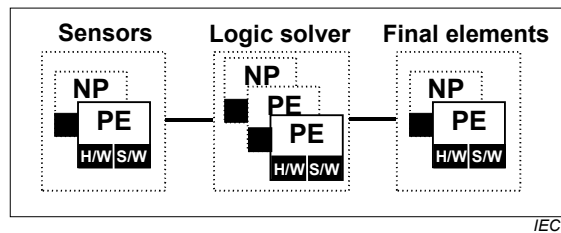


Figure 7 6 – Example of SIS architectures comprising three SIS subsystems

3.2.68 safety integrity

average probability ability of the SIS to perform ~~satisfactorily~~ the required SIF ~~functions under all the stated conditions within a stated period of time as and when required~~

~~NOTE 1—The higher the safety integrity level, the higher the probability that the required safety instrumented function (SIF) will be carried out.~~

~~NOTE 2—There are four levels of safety integrity for safety instrumented functions.~~

Note 1 to entry: This definition is equivalent to the dependability of the SIS with regard to the required SIF. Dependability, being often understood as an economical rather than a safety concept, has not been used to avoid confusion.

Note 2 to entry: Ability includes both the functional response (e.g., closing a specified valve within a specified time) and the likelihood that the SIS will act as required.

Note 3 to entry: In determining safety integrity, all causes of ~~failures (both random hardware failures and systematic failures)~~ which lead to an unsafe state ~~should~~ can be included (e.g., hardware failures, software induced failures and failures due to electrical interferences). Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the **average dangerous failure rate frequency in the dangerous mode of failure** or the probability of ~~a safety instrumented function failing to operate~~ failure on demand. However, safety integrity ~~of an SIF~~ also depends on many systematic factors, which cannot be accurately quantified ~~but can only be considered~~ and are often considered qualitatively throughout the life-cycle. The likelihood that systematic failures result in dangerous failure of the SIS is reduced through hardware fault tolerance (see 11.4) or other methods and techniques.

Note 4 to entry: Safety integrity comprises hardware safety integrity (see 3.2.26) and systematic safety integrity (see 3.2.82), but complex failures caused by the conjunction of both hardware and systematic interaction can also be considered.

3.2.69 safety integrity level SIL

discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements **to be achieved by the SIS**

~~NOTE 1—The target failure measures for the safety integrity levels are specified in Tables 3 and 4.~~

~~NOTE 2—It is possible to use several lower safety integrity level systems to satisfy the need for a higher level function (for example, using a SIL 2 and a SIL 1 system together to satisfy the need for a SIL 3 function).~~

Note 1 to entry: The higher the SIL, the lower the expected PFDavg for demand mode or the lower the average frequency of a dangerous failure causing a hazardous event for continuous mode.

Note 2 to entry: The relationship between the target failure measure and the SIL is specified in Tables 4 and 5.

Note 3 to entry: SIL 4 is related to the highest level of safety integrity; SIL 1 is related to the lowest

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

3.2.69.1 safety integrity requirements **specification**, pl

~~specification that contains the safety integrity requirements of the safety instrumented functions that have to be performed by the safety instrumented system(s)~~

set of the IEC 61511 requirements which shall be satisfied by a SIS to claim a given SIL for a SIF implemented by this SIS

~~NOTE 1 This specification is one part (the safety integrity part) of the safety requirements specification (see 3.2.78).~~

~~NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

Note 1 to entry: The safety integrity requirements are strengthened when the related SIL increases.

3.2.70

SIS safety life-cycle

necessary activities involved in the implementation of SIF occurring during a period of time that starts at the concept phase of a project and finishes when all of the SIF are no longer available for use

Note 1 to entry: The term “functional safety life-cycle” is strictly more accurate, but the adjective “functional” is not considered necessary in this case within the context of the IEC 61511 series.

Note 2 to entry: The SIS safety life-cycle model used in IEC 61511 is shown in Figure 7.

3.2.71

safety manual

functional safety manual

~~manual~~ information that defines how a SIS device, subsystem or system can be safely applied

Note 1 to entry: The safety manual may include inputs from the manufacturer as well as from the user.

Note 2 to entry: For IEC 61508 compliant devices, the manufacturer's input is the safety manual,

Note 3 to entry: This could be a generic stand-alone document, ~~an instructional manual, a programming manual, a standard document, or included in the user document(s) defining application limitations~~ or a collection of documents.

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

3.2.72

safety requirements specification

SRS

specification containing the functional requirements for the SIFs ~~that have to be performed by the safety instrumented systems~~ and their associated safety integrity levels

[SOURCE: IEC 61508-4:2010, 3.5.11, modified – Aligned with IEC 61511 terminology]

3.2.73

sensor

~~device or combination of devices~~ part of the BPCS or SIS that measures or detects the process condition

Note 1 to entry: Examples are transmitters, transducers, process switches and position switches)

3.2.79

safety software

~~software in a safety instrumented system with application, embedded or utility software functionality~~

3.2.74

software

~~intellectual creation comprising the~~ programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

Note 1 to entry: Software is independent of the medium on which it is recorded.

~~NOTE 2—This definition without note 1 differs from ISO 2382-1, and the full definition differs from ISO 9000-3 by the addition of the word data.~~

Note 2 to entry: For examples of different types of software, see 3.2.75 and 3.2.76.

3.2.75

~~software languages in SIS subsystems~~ application programming languages

3.2.75.1

fixed program language

FPL

language in which the user is limited to adjustment of a few pre-defined and fixed set of parameters ~~(for example, range of the pressure transmitter, alarm levels, network addresses)~~

Note 1 to entry: Typical examples of device applications with FPL are: smart sensor (e.g., pressure transmitter without control algorithms, smart ~~valve~~ final element (e.g. valve without control algorithms), sequence of events controller recorder, ~~dedicated smart alarm box, small data logging systems~~ set points for dedicated smart alarm box). The use of FPL is often referred to as "configuration of the device".

3.2.75.2

limited variability language

LVL

programming language for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application as defined by the associated safety manual. The notation of this language may be textual or graphical or have characteristics of both.

Note 1 to entry: This type of language is designed to be easily understood by process sector users, and provides the capability to combine predefined, application specific, library functions to implement the SRS. LVL provides a close functional correspondence with the functions required to achieve the application.

Note 2 to entry: IEC 61511 assumes that the constraints necessary to achieve the safety properties are achieved by the combination of the safety manual, the closeness of the language notations to the functions the application programmer needs to define the process control algorithms, and the compile time and run time checks which the logic solver provider embeds into the logic solver system program and the logic solver development environment. The constraints identified in the certification report and safety manual can ensure the relevant requirements of IEC 61508-3:2010 are satisfied.

Note 3 to entry: LVL is the most commonly used language when the IEC 61511 series refers to "application program".

3.2.75.3

full variability language

FVL

language designed to be comprehensible to computer programmers and that provides the capability to implement a wide variety of functions and applications

Note 1 to entry: Typical example of systems using FVL are general purpose computers.

Note 2 to entry: In the process sector, FVL is found in embedded software and rarely in application ~~software programming~~.

Note 3 to entry: FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

3.2.76

software & program types

3.2.76.1

~~application software~~ program

~~software~~ program specific to the user application containing, in general, logic sequences, permissives, limits and expressions that control the ~~appropriate~~ input, output, calculations, and decisions necessary to meet the SIS functional requirements. ~~See fixed and limited variability language~~

3.2.76.2

embedded software

software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user.

Note 1 to entry: Embedded software is also referred to as firmware or system software. See 3.2.75.3, full variability language

3.2.76.3

utility software

software tools for the creation, modification, and documentation of application programs.

Note 1 to entry: These software tools are not required for the operation of the SIS

3.2.77

~~software~~ application program life-cycle

activities occurring during a period of time that starts when ~~software~~ the application program is conceived and ends when the ~~software~~ application program is permanently disused

Note 1 to entry: An ~~software~~ application program life-cycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and modification phase.

Note 2 to entry: Software, including application program, cannot be maintained; rather, it is modified.

~~3.2.83~~

~~subsystem~~

~~see “system”~~

3.2.78

SIS subsystem

independent part of a SIS whose disabling dangerous failure results in a disabling dangerous failure of the SIS

Note 1 to entry: Figure 6 illustrates a SIS made of three SIS subsystems.

Note 2 to entry: From the cut set approach point of view (see IEC 61025) a minimal cut set of a SIS subsystem is also a minimal cut set of the whole SIS. Therefore the SIFs implemented within a SIS are entirely dependent on the SIS subsystems of this SIS (i.e., when a SIS subsystem fails, the related SIFs also fail).

3.2.79

system

set of ~~elements~~ devices, which interact according to a ~~design~~ specification; ~~an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction~~

Note 1 to entry: A person can be part of a system.

Note 2 to entry: This definition ~~differs from IEC 351-01-01~~ deviates from the definition in IEC 61508 to reflect differences in process sector terminology.

NOTE 3 ~~A system includes the sensors, the logic solvers, final elements, communication and ancillary equipment belonging to SIS (for example, cables, tubing, power supply).~~

3.2.80

systematic capability

measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual

Note 1 to entry: Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults in IEC 61508-2:2010 and IEC 61508-3:2010.

Note 2 to entry: The systematic failure mechanism depends on the nature of the device. For a device comprised solely of hardware, only hardware failure mechanisms are considered. For a device comprised of hardware and software, it is necessary to consider the interactions between hardware and software failure mechanisms.

Note 3 to entry: A systematic capability of SC N for a device means that the systematic safety integrity of SC N has been met when the device is applied in accordance with the instructions specified in the device safety manual for SC N.

3.2.81 systematic failure

failure related ~~in a deterministic way to a certain cause~~ to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors

~~NOTE 3 This definition (up to note 2) matches IEC 101-04-19.~~

Note 1 to entry: The cause of systematic failures of the software may be known as "bugs".

Note 2 to entry: Corrective maintenance without modification would usually not eliminate the failure cause which involves the failure under particular conditions.

Note 3 to entry: A systematic failure can be ~~induced by simulating the failure cause~~ reproduced by deliberately applying the same conditions, although not all reproducible failures are systematic.

Note 4 to entry: Examples of faults leading to systematic failure ~~causes~~ include human error that originates in:

- the SRS;
- the design, manufacture, installation, operation or maintenance of the hardware;
- the design ~~and/or~~ implementation of software (including application program).

Note 5 to entry: Similar devices designed, installed, operated, implemented or maintained in the same way are likely to contain the same faults. Therefore they are subject to common cause failures when the particular conditions occur.

3.2.82 systematic safety integrity

part of the safety integrity of the ~~SIF~~ SIS relating to systematic failures ~~(see note 3 of 3.2.73)~~ in a dangerous mode of failure

Note 1 to entry: Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity).

Note 2 to entry: See 3.2.26 also.

3.2.83 target failure measure

~~intended probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either the average probability of failure to perform the design function on demand (for a demand mode of operation) or the frequency of a dangerous failure to perform the SIF per hour (for a continuous mode of operation)~~ performance required from the SIF and specified in terms of either the average probability of failure to perform the SIF on demand for demand mode of operation or the average frequency of a dangerous failure for continuous mode of operation

Note 1 to entry: The ~~numerical values for~~ relationship between the target failure measures and the SIL are given in Tables 4 and 5.

3.2.84 template software template

~~structured non-specific piece of application software that can be easily altered to support specific functions while retaining the original structure; for example, an interactive screen template controls the process flow of the application screens, but is not specific to the data being presented; a programmer may take the generic template and make function-specific revisions to produce a new screen for the users~~

~~NOTE The related term "software template" is sometimes used. Typically, it refers to an algorithm or collection of algorithms that have been programmed to perform a desired function or set of functions and is constructed so it can be used in many different instances. In the context of IEC 61131-3, it is a program that can be selected for use in many applications.~~

3.2.84**tolerable risk**

level of risk which is accepted in a given context based on the current values of society

Note 1 to entry: See IEC 61511-3:2016, Annex A.

[SOURCE: ISO/IEC Guide 51:2014, 3.15]

3.2.85**undetected****unrevealed****covert**

~~in relation to hardware and software faults not found by the diagnostic tests or during normal operation~~ not detected or not revealed or not overt

~~NOTE—This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.~~

Note 1 to entry: In IEC 61511 and except when the context suggests another meaning, the term “dangerous undetected failures/faults” is related to dangerous failures/faults not detected by diagnostic tests.

3.2.86**validation**

~~activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification~~

confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: In the IEC 61511 series this means demonstrating that the SIF(s) and SIS after installation meet the SRS in all respects.

3.2.87**verification**

confirmation by examination and provision of objective evidence that the requirements have been fulfilled

Note 1 to entry: In the IEC 61511 series this is the activity of demonstrating for each phase of the relevant SIS safety life-cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

Note 2 to entry: Example verification activities include:

- reviews on outputs (documents from all phases of the safety life-cycle) to ensure compliance with the objectives and requirements of the phase taking into account the specific inputs to that phase;
- design reviews;
- tests performed on the designed products to ensure that they perform according to their specification;
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

3.2.88**watchdog**

combination of diagnostics and an output device (typically a switch) for monitoring the correct operation of the programmable electronic (PE) device and taking action upon detection of an incorrect operation

Note 1 to entry: The watchdog confirms that the software system is operating correctly by the regular resetting of an external device (e.g., hardware electronic watchdog timer) by an output device controlled by the software.

Note 2 to entry: The watchdog can be used to de-energize a group of safety outputs when dangerous failures are detected in order to ~~put the process into~~ achieve or maintain a safe state of the process with respect to the hazardous event. The watchdog is used to increase the on-line diagnostic coverage of the PE logic solver (see 3.2.13 and 3.2.15).

3.3 Abbreviations

Abbreviations used throughout IEC 61511 are given in Table 1. Also included are some common abbreviations related to process sector functional safety.

Table 1 – Abbreviations used in IEC 61511

Abbreviation	Full expression
AC/DC	Alternating current/direct current
AICHE	American Institute of Chemical Engineers
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
AP	Application program
BPCS	Basic process control system
CCPS	Centre for Chemical Process Safety (AIChE)
DC	Diagnostic coverage
E/E/PE	Electrical/electronic/programmable electronic
~~E/E/PES~~	~~Electrical/electronic/programmable electronic system~~
EMC	Electro-magnetic compatibility
FAT	Factory acceptance test
FPL	Fixed program language
FSA	Functional safety assessment
FSMS	Functional safety management system
FTA	Fault tree analysis
FVL	Full variability language
HFT	Hardware fault tolerance
H&RA	Hazard & risk assessment
~~HRA~~	~~Human reliability analysis~~
~~H/W~~	~~Hardware~~
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
~~IEV~~	~~International Electrotechnical Vocabulary~~
ISA	~~Instrumentation, Systems and Automation Society~~ International Society of Automation
ISO	International Organization for Standardization
LVL	Limited variability language
MooN	“M” out of “N” ~~(see 3.2.45)~~ channel architecture
MPRT	Maximum permitted repair time
MRT	Mean repair time
MTTR	Mean time to restoration
NFPA	National Fire Protection Association(US)
NP	Non-programmable
OEM	Original Equipment Manufacturer
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of dangerous failure on demand
PFD _{avg}	Average probability of dangerous failure on demand
PFH	Probability (average frequency of dangerous failures) of failure per hour



Abbreviation	Full expression
pl	Plural
PLC	Programmable logic controller
SAT	Site acceptance test
SC	Systematic capability
~~SFF~~	~~Safe failure fraction~~
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification
~~SAW~~	~~Software~~

4 Conformance to the IEC 61511-1:2016

To conform to the IEC 61511-1:2016, it shall be shown that each of the requirements outlined in Clause 5 through Clause 19 has been satisfied to the defined criteria and therefore the clauses' objectives have been met.

5 Management of functional safety

5.1 Objective

The objective of the requirements of Clause 5 is to identify the management activities that are necessary to ensure the functional safety objectives are met.

NOTE 1: Clause 5 is solely aimed at the achievement and maintenance of the functional safety of SIS and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

5.2 Requirements

5.2.1 General

5.2.1.1 The policy and strategy for achieving functional safety shall be identified together with the ~~means~~ methods for evaluating their achievement and shall be communicated within the organization.

~~5.2.1.2 A safety management system shall be in place so as to ensure that where safety instrumented systems are used, they have the ability to place and/or maintain the process in a safe state.~~

5.2.2 Organization and resources

5.2.2.1 Persons, departments, organizations or other units which are responsible for carrying out and reviewing each of the SIS safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them ~~(including where relevant, licensing authorities or safety regulatory bodies).~~

5.2.2.2 Persons, departments or organizations involved in SIS safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

NOTE ~~As a minimum,~~ The following items ~~should~~ shall be addressed and documented when considering the competence of persons, departments, organizations or other units involved in SIS safety life-cycle activities:

- a) engineering knowledge, training and experience appropriate to the process application;
- b) engineering knowledge, training and experience appropriate to the applicable technology used (e.g., electrical, electronic or programmable electronic);
- c) engineering knowledge, training and experience appropriate to the sensors and final elements;
- d) safety engineering knowledge (e.g., process safety analysis);
- e) knowledge of the legal and regulatory **functional** safety requirements;
- f) adequate management and leadership skills appropriate to their role in **the SIS** safety life-cycle activities;
- g) understanding of the potential consequence of an event;
- h) the SIL of the SIF;
- i) the novelty and complexity of the application and the technology.

5.2.2.3 A procedure shall be in place to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.

5.2.3 Risk evaluation and risk management

Hazards shall be identified, risks evaluated and the necessary risk reduction determined as defined in Clause 8.

NOTE It may be beneficial to consider also potential capital losses, for economic reasons.

5.2.4 Safety planning

Safety planning shall take place to define the activities that are required to be carried out along with the persons, departments, organizations or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire SIS safety life-cycle (see Clause 6) **and carried out to a detailed activity level commensurate with the role the individual or organization is performing in the SIS safety life-cycle.**

NOTE The safety planning ~~may~~ **can** be incorporated in

- a section in the quality plan entitled “**SIS Safety Life-cycle Plan**”; or
- a separate document entitled “**SIS Safety Life-cycle Plan**”; or
- several documents which may include company procedures or working practices.

5.2.5 Implementing and monitoring

5.2.5.1 Procedures shall be implemented to ensure prompt follow-up and satisfactory resolution of recommendations pertaining to the SIS arising from

- a) hazard analysis and risk assessment;
- b) ~~assessment and auditing~~ **assurance** activities;
- c) verification activities;
- d) validation activities;
- e) **FSAs**;
- f) **functional safety audits**;
- g) post-incident and post-accident activities.

5.2.5.2 Any supplier, providing products or services to an organization that has overall responsibility for one or more phases of the SIS safety life-cycle, shall deliver products or services as specified by that organization and shall have a quality management system. Procedures shall be in place to demonstrate the adequacy of the quality management system.

If a supplier makes any functional safety claims for a product or service, which are used by the organization to demonstrate compliance with the requirements of this part of IEC 61511, the supplier shall have a functional safety management system. Procedures shall be in place to demonstrate the adequacy of the functional safety management system.

The functional safety management system shall meet the requirements of the basic safety standard IEC 61508-1:2010, Clause 6, or the functional safety management requirements of the standard derived from IEC 61508 to which functional safety claims are made.

5.2.5.3 Procedures shall be implemented to evaluate the performance of the SIS against its safety requirements to:

- identify and prevent systematic failures which could jeopardize safety;
- **monitor and** assess whether ~~dangerous failure rates~~ **reliability parameters** of the SIS are in accordance with those assumed during the design;

~~NOTE 1 Dangerous failures are revealed by means of proof testing, diagnostics or failure to operate on demand.~~

~~NOTE 2 Procedures should be considered that~~

- define the necessary corrective action to be taken if the failure rates are greater than what was assumed during design;
- ~~assessing~~ **compare** the demand rate on the SIF during actual operation ~~to verify with~~ the assumptions made during risk assessment when the SIL requirements were determined.

5.2.5.4 For existing SIS designed and constructed in accordance with code, standards, or practices prior to the issue of this standard the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

5.2.6 Assessment, auditing and revisions

5.2.6.1 Functional safety assessment (FSA)

5.2.6.1.1 A procedure shall be defined and executed for a FSA in such a way that a judgement can be made as to the functional safety and safety integrity achieved by **every SIF** of the SIS. The procedure shall require that ~~an assessment~~ **FSA** team be appointed which includes the technical, application and operations expertise needed for the particular ~~installation~~ **application**.

5.2.6.1.2 The membership of the ~~assessment~~ **FSA** team shall include at least one senior competent person not involved in the project design team **(for stages 1, 2 and 3) or not involved in the operation and maintenance of the SIS (for stages 4 and 5).**

~~NOTE 2~~ **5.2.6.1.3** The following ~~should~~ **shall** be considered when planning a FSA:

- the scope of the FSA;
- who is to participate in the FSA;
- the skills, responsibilities and authorities of the FSA team;
- the information that will be generated as a result of any FSA activity;
- the identity of any other safety bodies involved in the FSA;
- the resources required to complete the FSA activity;
- the level of independence of the FSA team;
- the ~~means~~ **methods** by which the FSA will be revalidated after modifications.

NOTE When the ~~assessment~~ **FSA** team is large, consideration ~~should~~ **can** be given to having more than one senior competent individual on the team who is independent from the project team.

5.2.6.1.4 A FSA team shall review the work carried out on all phases of the safety life cycle prior to the stage covered by the assessment that have not been already covered by previous FSAs. If previous FSAs have been carried out then the FSA team shall consider the conclusions and recommendations of the previous assessments. The stages in the SIS safety life-cycle at which the FSA activities are to be carried out shall be identified during the safety planning.

NOTE 1 Additional FSA activities ~~may need to~~ can be introduced as new hazards are identified, after modification and at periodic intervals during operation.

NOTE 2 Consideration ~~should~~ can be given to carrying out FSA activities at the following stages (see Figure 7).

- Stage 1 – After the H&RA has been carried out, the required protection layers have been identified and the SRS has been developed.
- Stage 2 – After the SIS has been designed.
- Stage 3 – After the installation, pre-commissioning and final validation of the SIS has been completed and operation and maintenance procedures have been developed.
- Stage 4 – After gaining experience in operating and maintenance.
- Stage 5 – After modification and prior to decommissioning of a SIS.

NOTE 3 The number, size and scope of FSA activities ~~should~~ can depend upon the specific circumstances. The factors in this decision are likely to include:

- size of project;
- degree of complexity;
- SIL;
- duration of project;
- consequence in the event of failure;
- degree of standardization of design features;
- safety regulatory requirements;
- previous experience with a similar design;
- giving consideration to relevant factors such as:
 - time in operation;
 - number and scope of changes in operation;
 - proof test frequency.

5.2.6.1.5 ~~At least one functional safety assessment shall be undertaken. This functional safety assessment shall be carried out to make sure the hazards arising from a process and its associated equipment are properly controlled. As a minimum, one assessment shall be carried out.~~ Prior to the ~~identified~~ hazards being present (~~i.e., stage 3~~), the FSA team shall undertake functional safety assessment(s) and shall confirm:

- the H&RA has been carried out (see 8.1);
- the recommendations arising from the H&RA that apply to the SIS have been implemented or resolved;
- project design change procedures are in place and have been properly implemented;
- the recommendations arising from ~~the previous~~ any FSA have been resolved;
- the SIS is designed, constructed and installed in accordance with the SRS, any differences having been identified and resolved;
- the safety, operating, maintenance and emergency procedures pertaining to the SIS are in place;
- the SIS validation planning is appropriate and the validation activities have been completed;
- the employee training has been completed and appropriate information about the SIS has been provided to the maintenance and operating personnel;
- plans or strategies for implementing further FSAs are in place.

5.2.6.1.6 Where **design**, development and production tools are used for any **SIS** safety life-cycle activity, they shall themselves be subject to an ~~an-functional safety~~ assessment demonstrating that they do not have any negative impact on the **SIS** or the output of the tools shall be confirmed by verification procedures.

NOTE 1 The degree to which such tools ~~should need to~~ **can** be addressed will depend upon their impact on the ~~safety risk level~~ to be achieved.

NOTE 2 Examples of development and production tools include simulation and modelling tools, measuring equipment, test equipment, equipment used during maintenance activities and configuration management tools.

NOTE 3 ~~Functional safety assessment~~ **Quality assurance** of tools includes, but is not limited to, traceability to calibration standards, operating history and defect list.

5.2.6.1.7 The results of the FSA shall be available together with any recommendation coming from this assessment.

5.2.6.1.8 All relevant information shall be made available to the FSA team upon their request.

5.2.6.1.9 In cases where a FSA is carried out on a modification the assessment shall consider the impact analysis carried out on the proposed modification and confirm that the modification work performed is in compliance with the requirements of IEC 61511.

NOTE Safety life cycle (including FSA) requirements related to SIS modifications can be found in 17.2.3.

5.2.6.1.10 A FSA shall also be carried out periodically during the operations and maintenance phase to ensure that maintenance and operation are being carried out according to the assumptions made during design and that the requirements within IEC 61511 for safety management and verification are being met.

5.2.6.2 ~~Auditing~~ Functional safety audit and revision

5.2.6.2.1 The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.

5.2.6.2.2 All procedures identified as necessary resulting from all safety life-cycle activities shall be subject to safety audit.

5.2.6.2.3 Functional safety audit shall be performed by an independent person not undertaking work on the SIS to be audited. Procedures shall be defined and executed for auditing compliance with requirements including:

- the frequency of the ~~auditing~~ functional safety audit activities;
- the degree of independence between the persons, departments, organizations or other units carrying out the work and those carrying out the functional safety auditing activities;
- the recording and follow-up activities.

5.2.6.2.4 Management of change procedures shall be in place to initiate, document, review, implement and approve changes to the SIS other than replacement in kind (i.e., like for like, an exact duplicate of an element or an approved substitution that does not require modification to the SIS as installed).

5.2.6.2.5 Management of change procedures shall be in place that identifies changes that will affect the requirements on the SIS (e.g., re-design of a BPCS, changes to manning in a certain area).

5.2.7 SIS configuration management

5.2.7.1 ~~Requirements~~

5.2.7.1 Procedures for configuration management of the SIS during any SIS ~~and software~~ safety life-cycle phase shall be available.

NOTE In particular, the following ~~should~~ **can** be specified:

- the stage at which formal configuration ~~control~~ **management** is to be implemented;
- the procedures to be used for uniquely identifying all ~~constituent parts of an item (hardware and software)~~ **components of a SIS or SIS-subsystem (e.g., devices, application programming)**;
- the procedures for preventing unauthorized ~~items~~ **devices** from entering service.

5.2.7.2 The SIS software, hardware and procedures used to develop and execute the application program shall be subject to configuration management and shall be maintained under revision control.

NOTE SIS software includes application program (e.g., in logic solvers); embedded software (e.g., sensors, logic solvers, final elements); utility software (tools).

6 Safety life-cycle requirements

6.1 Objectives

The objectives of Clause 6 are:

- to define the phases and establish the requirements of the **SIS** safety life-cycle activities;
- to **define and** organize the technical activities into a **SIS** safety life-cycle;
- to ensure that adequate planning exists (or is developed) that makes certain that the SIS ~~shall~~ meets the safety requirements.

NOTE 1 The overall approach of the IEC 61511 series is shown in Figure 7. It ~~should~~ **can** be stressed that this approach is for illustration and is only meant to indicate the typical **SIS** safety life-cycle activities from initial conception through decommissioning.

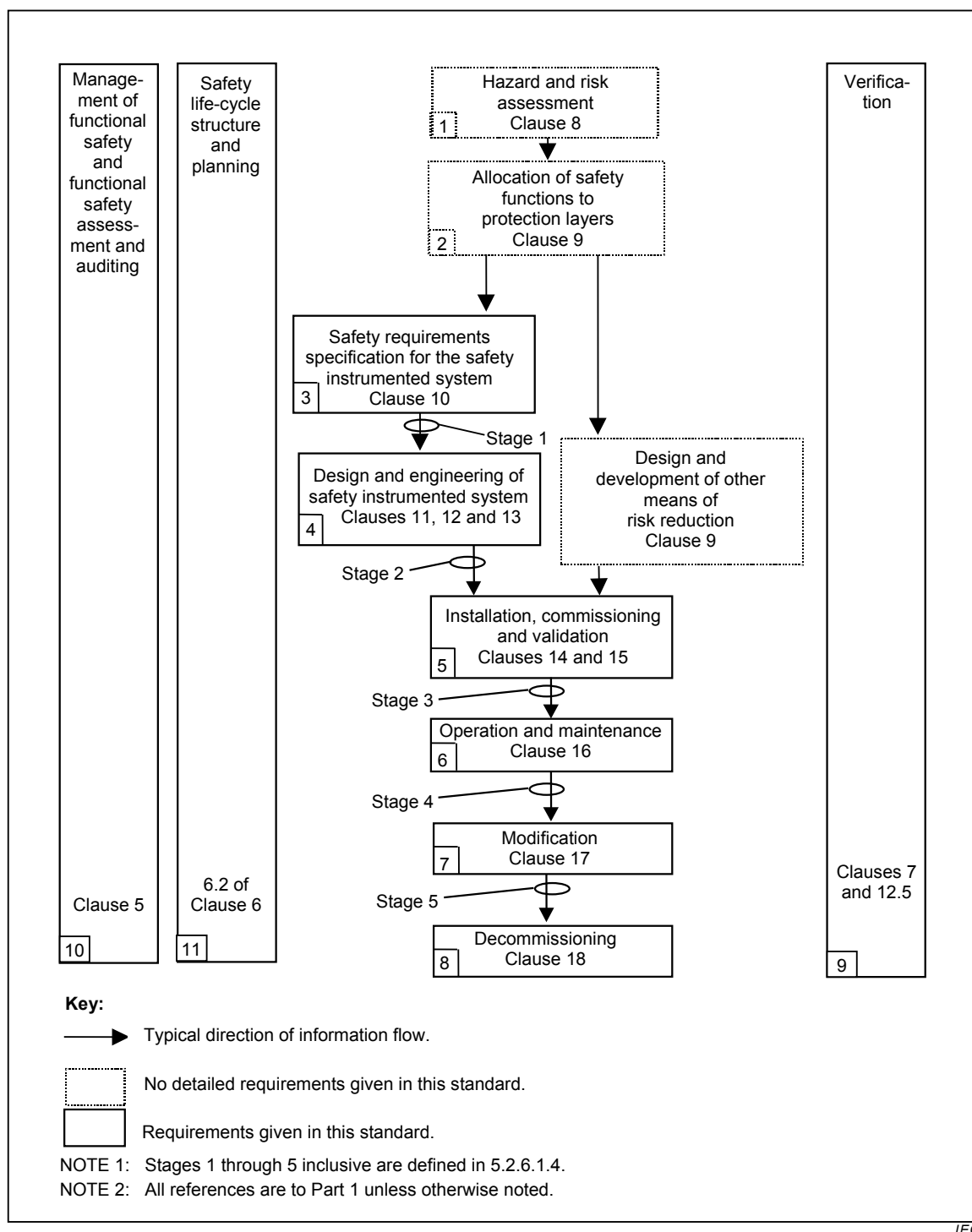


Figure-8 7 – SIS safety life-cycle phases and FSA stages

NOTE 2 Information in Figure 7 may flow from operation and maintenance back to the earlier life-cycle stages to reflect tracking of incidents and failures and to verify engineering assumptions.

6.2 Requirements

6.2.1 A SIS safety life-cycle incorporating the requirements of the IEC 61511 series shall be defined during safety planning. The safety life-cycle shall also address the application programming (see 6.3.1).

6.2.2 Each phase of the SIS safety life-cycle shall be defined in terms of its inputs, outputs and verification activities (see Table 2).

Table 2 – SIS safety life-cycle overview (1 of 2)

Safety life-cycle phase or activity		Objectives	Requirements Clause	Inputs	Outputs
Figure 7 box number	Title				
1	H&RA	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	Clause 8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL	Clause 9	A description of the required SIF and associated safety integrity requirements	Description of allocation of safety requirements ~~(see Clause 9)~~
3	SIS safety requirements specification	To specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety	Clause 10	Description of allocation of safety requirements ~~(see clause 9)~~	SIS safety requirements; ~~software~~ software application program safety requirements
4	SIS design and engineering	To design the SIS to meet the requirements for SIF and their associated safety integrity	Clauses 11, 12	SIS safety requirements ~~Software~~ Application program safety requirements	Design of the SIS hardware and application program in conformance with the SIS safety requirements; planning for the SIS integration test
5	SIS installation commissioning and validation	To integrate and test the SIS To validate that the SIS meets in all respects the requirements for safety in terms of the required SIF and ~~the required~~ their associated safety integrity	Clauses 14, 15	SIS design SIS integration test plan SIS safety requirements Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS ~~design~~ safety requirements . Results of SIS integration tests Results of the installation, commissioning and validation activities

Table 2 (2 of 2)

Safety life-cycle phase or activity		Objectives	Requirements Clause	Inputs	Outputs
Figure 7 box number	Title				
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	Clause 16	SIS safety requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	Clause 17	Revised SIS safety requirements	Results of SIS modification
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remains appropriate	Clause 18	As built safety requirements and process information	SIF placed out of service
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	Clause 7, 12.5	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase
10	SIS FSA	To investigate and arrive at a judgement on the functional safety achieved by the SIS	Clause 5	Planning for SIS FSA SIS safety requirement	Results of SIS FSA
11	Safety lifecycle structure and planning	To establish how the lifecycle steps are accomplished	6.2	Not applicable	Safety plan

6.2.3 For all **SIS** safety life-cycle phases, safety planning shall take place to define the **activities**, criteria, techniques, measures, procedures and **responsible organisation/people** to:

- ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both functional and safety integrity requirements;
- ensure proper installation and commissioning of the SIS;
- ensure the safety integrity of the SIF after installation;
- maintain the safety integrity during operation (e.g., proof testing, failure analysis);
- manage the process hazards during maintenance activities on the SIS.

6.2.4 If at any stage of the safety life-cycle, a change is required pertaining to an earlier life-cycle phase, then that earlier SIS safety life-cycle phase and the subsequent phases shall be re-examined, altered as required and re-verified.

6.3 Application program SIS safety life-cycle requirements

6.3.1 Each phase of the application program safety life-cycle (see Figure 8) shall be defined in terms of its elementary activities, objectives, required input information and output results and verification requirements (see Table 3).

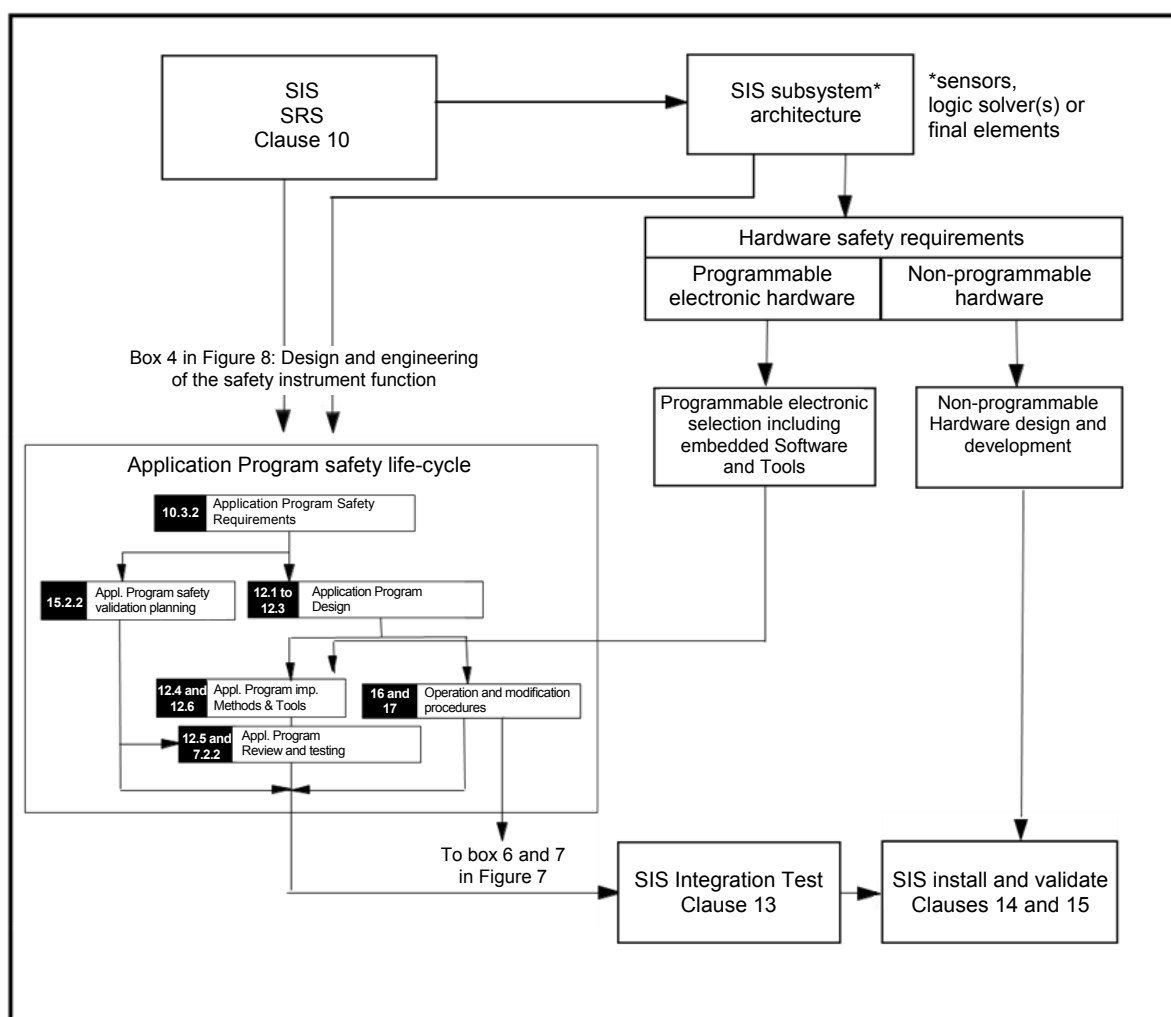


Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle