IEC 61511-1

Edition 2.0 2016-02
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

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

IEC 61511-1:2016-02 RLV(en)

IEC Central Office
3, rue de Varembé
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 It also gives information on projects, replaced and withdrawn publications.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

CONTENTS

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.

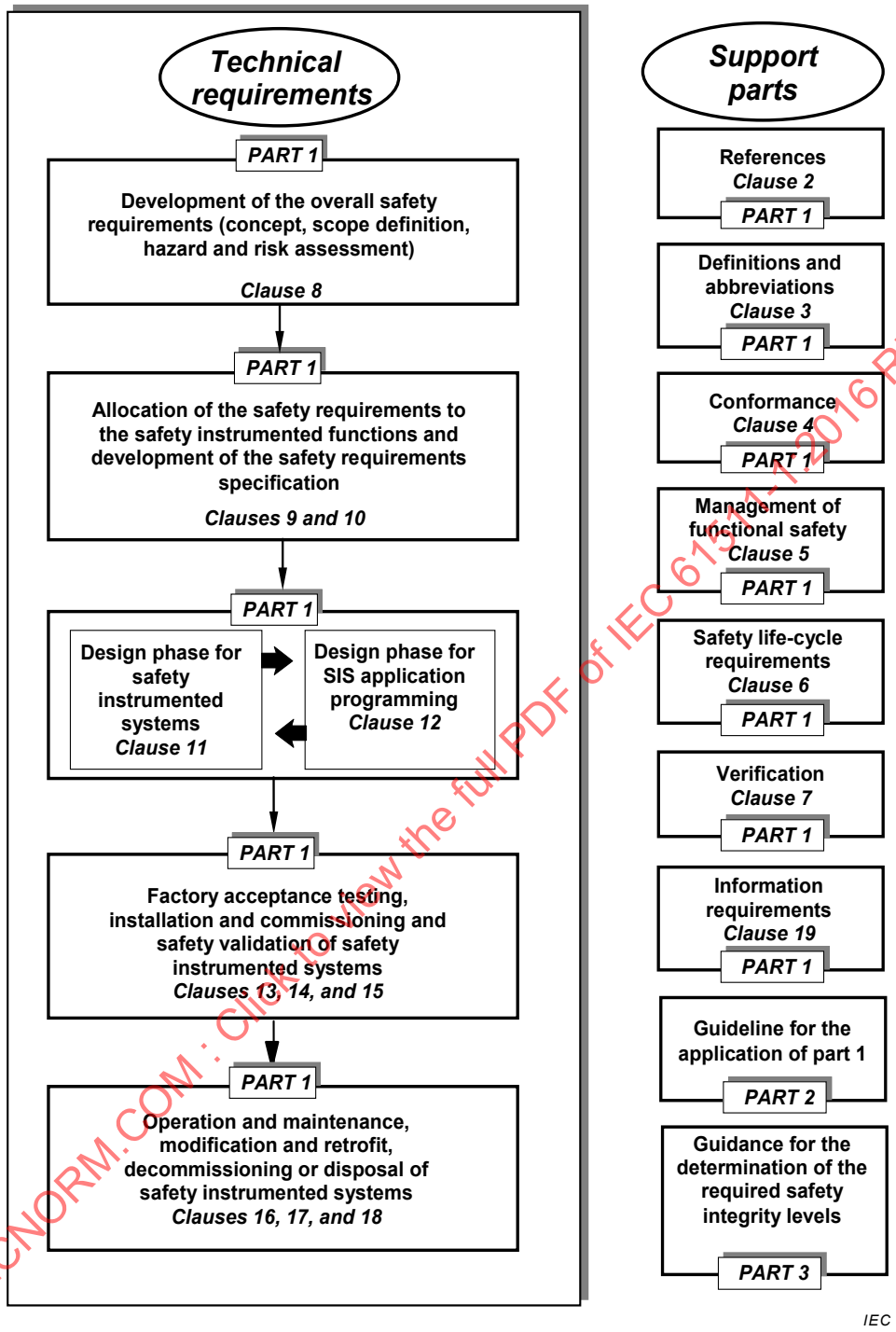


Figure 1 – Overall framework of the IEC 61511 series

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:

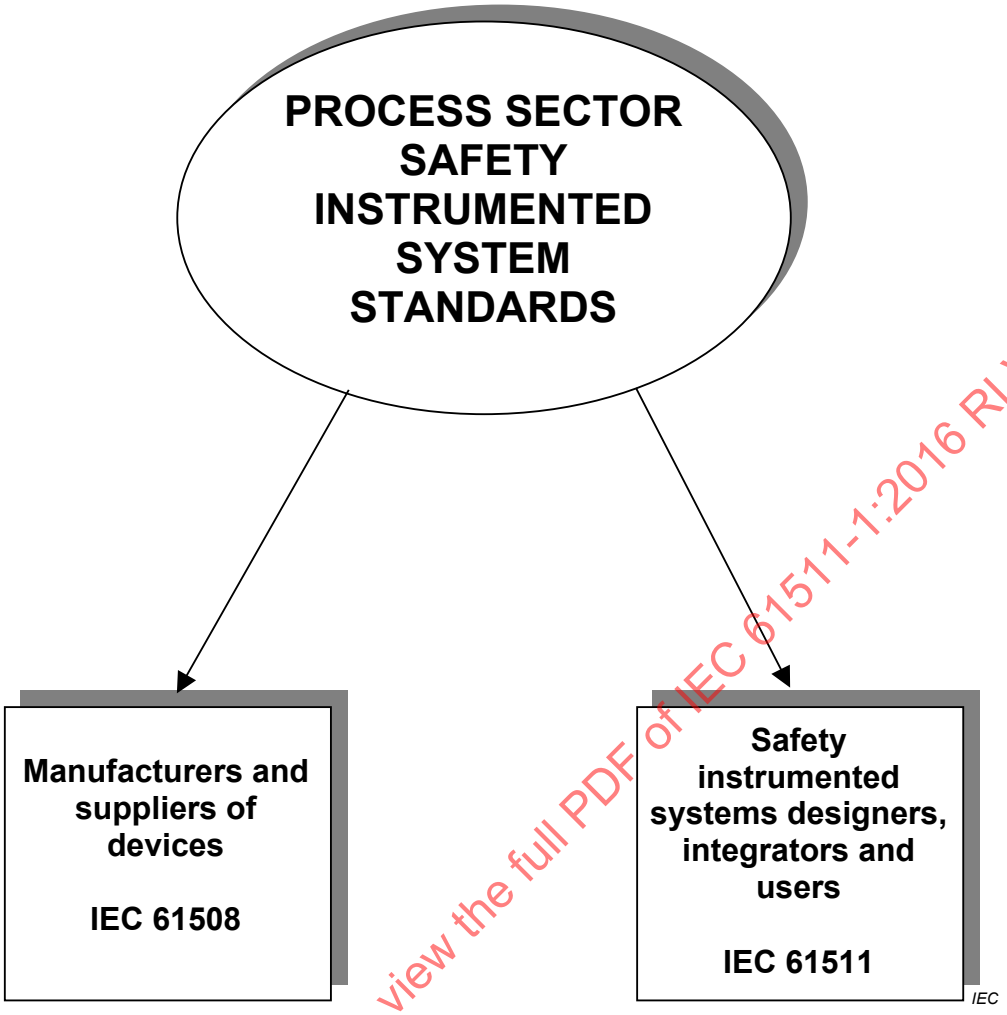


Figure 2 – Relationship between IEC 61511 and IEC 61508

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

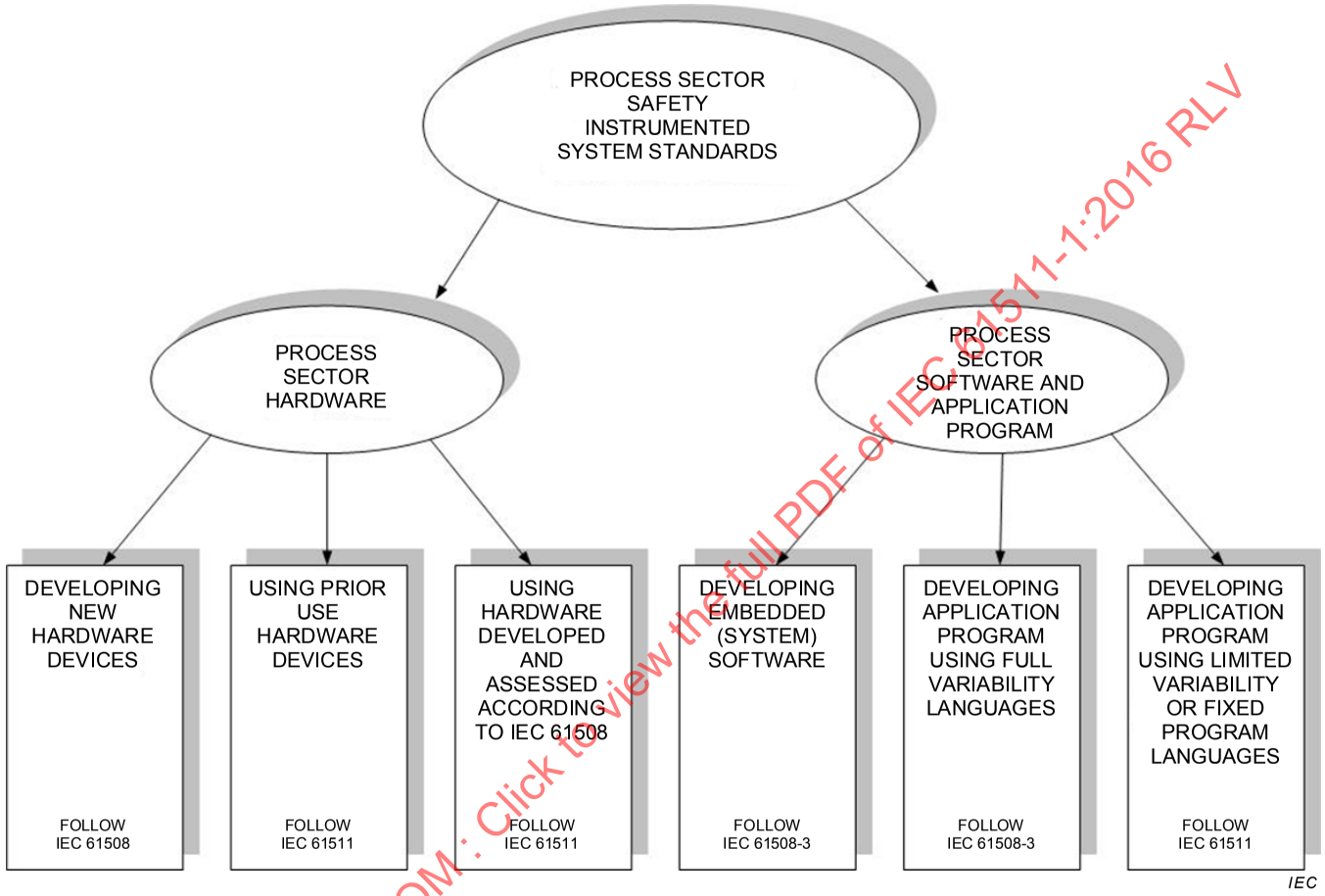
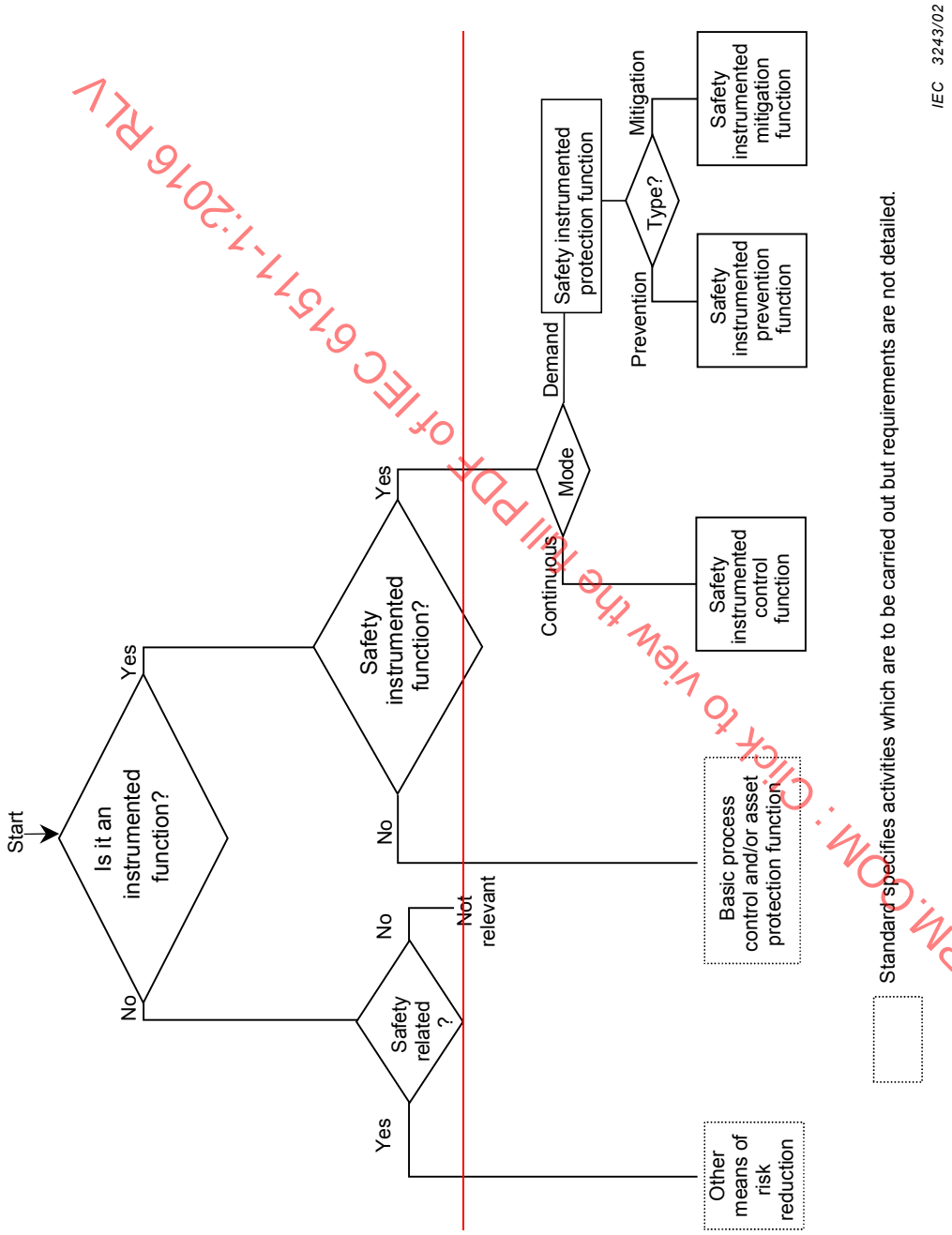


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508 ~~(see clause 1)~~

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.).



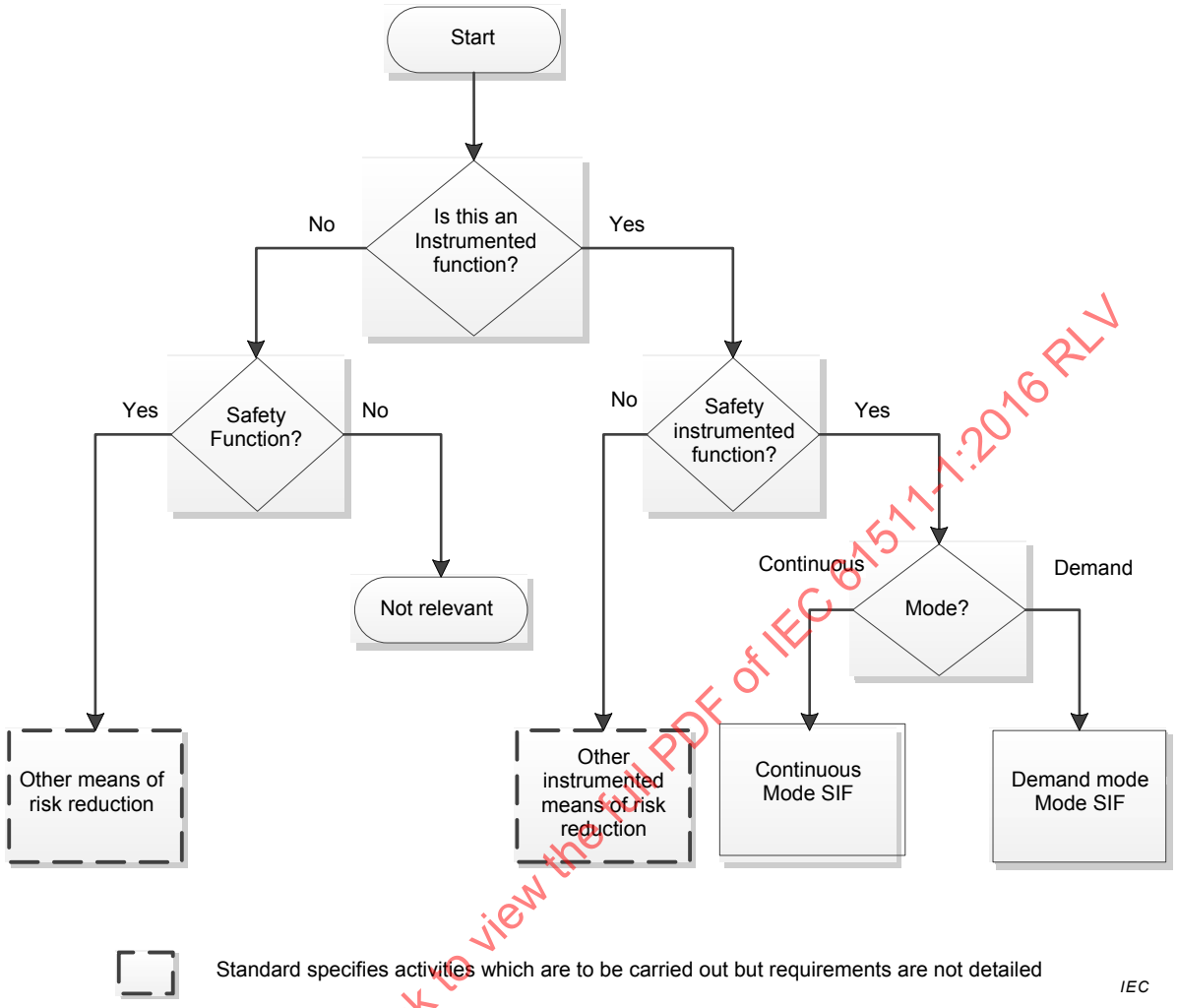


Figure 4 – Relationship between safety instrumented functions and other functions

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 an 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 and B) is greater than *P*(A) × *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 ($\lambda_{detected}$) and undetected failure rates ($\lambda_{undected}$) from the total failure rate ($\lambda_{total\ failure\ rate}$) as follows: $\lambda_{detected} = DC \times \lambda_{total\ failure\ rate}$ and $\lambda_{undected} = (1\text{-}DC) \times \lambda_{total\ failure\ rate}$.~~

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 DC = $\lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate. For a SIS subsystem with internal redundancy, DC is time dependant: $DC(t) = \lambda_{DD}(t)/\lambda_{DT}(t)$.

Note 3 to entry: When the 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:

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

3.2.16
diversity
different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical ~~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 IEV 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 IEV 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. [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 IEV 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 IEV 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 IEV 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., ~~CRTs~~ 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)

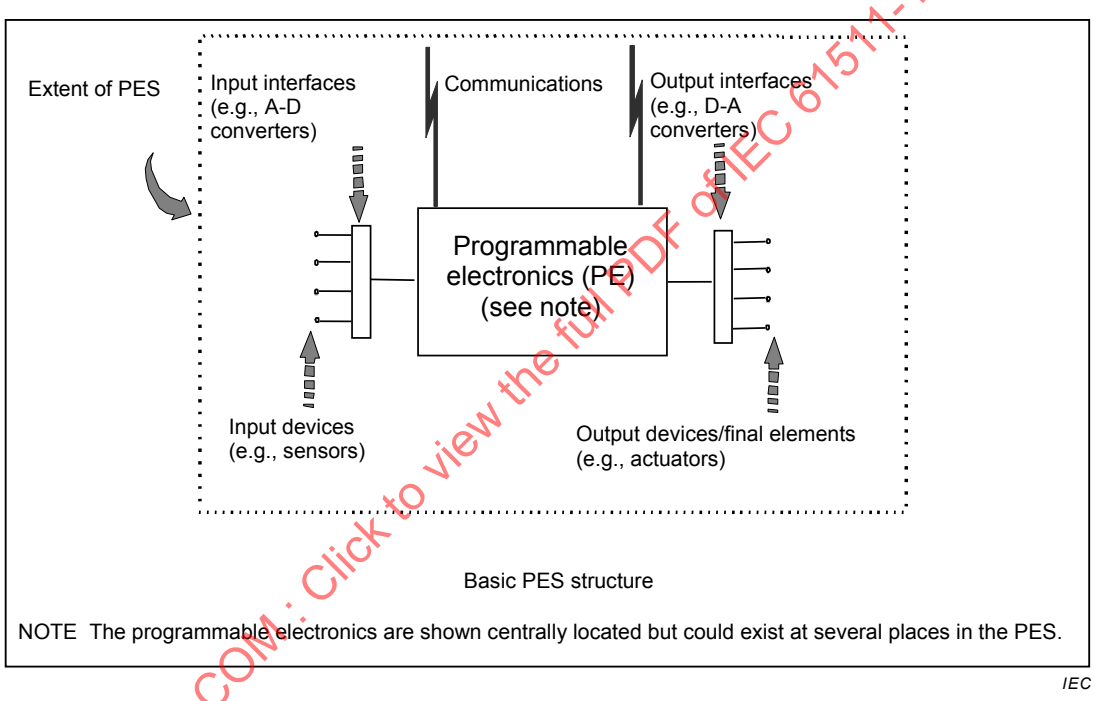


Figure ~~6~~ 5 – Programmable electronic system (PES): structure and terminology

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 IEV 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

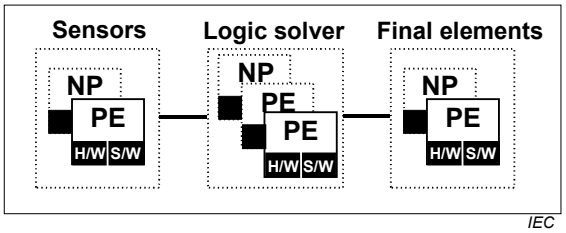


Figure ~~7~~ 6 – Example of SIS architectures comprising three SIS subsystems

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 cointaining, 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 IEV 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 IEV 191-04-19.~~

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
~~S/W~~	~~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 a~~n 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 ~~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.

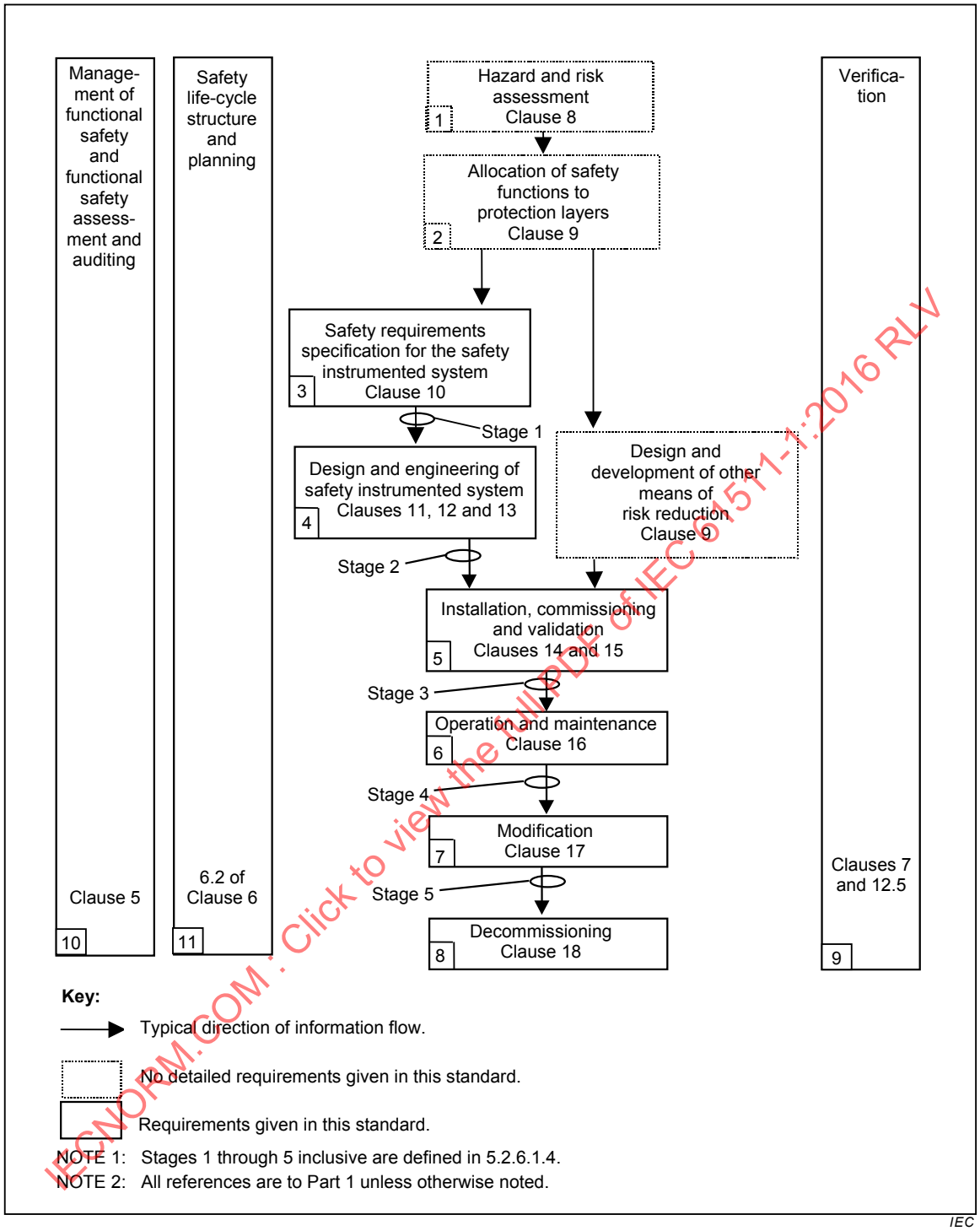


Figure ~~8~~ 7 – SIS safety life-cycle phases and FSA stages

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	Require-ments 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~~ 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, com-missioning and validation activities

Table 2 *(2 of 2)*

Safety life-cycle phase or activity		Objectives	Require-ments 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	Decommission-ing	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).

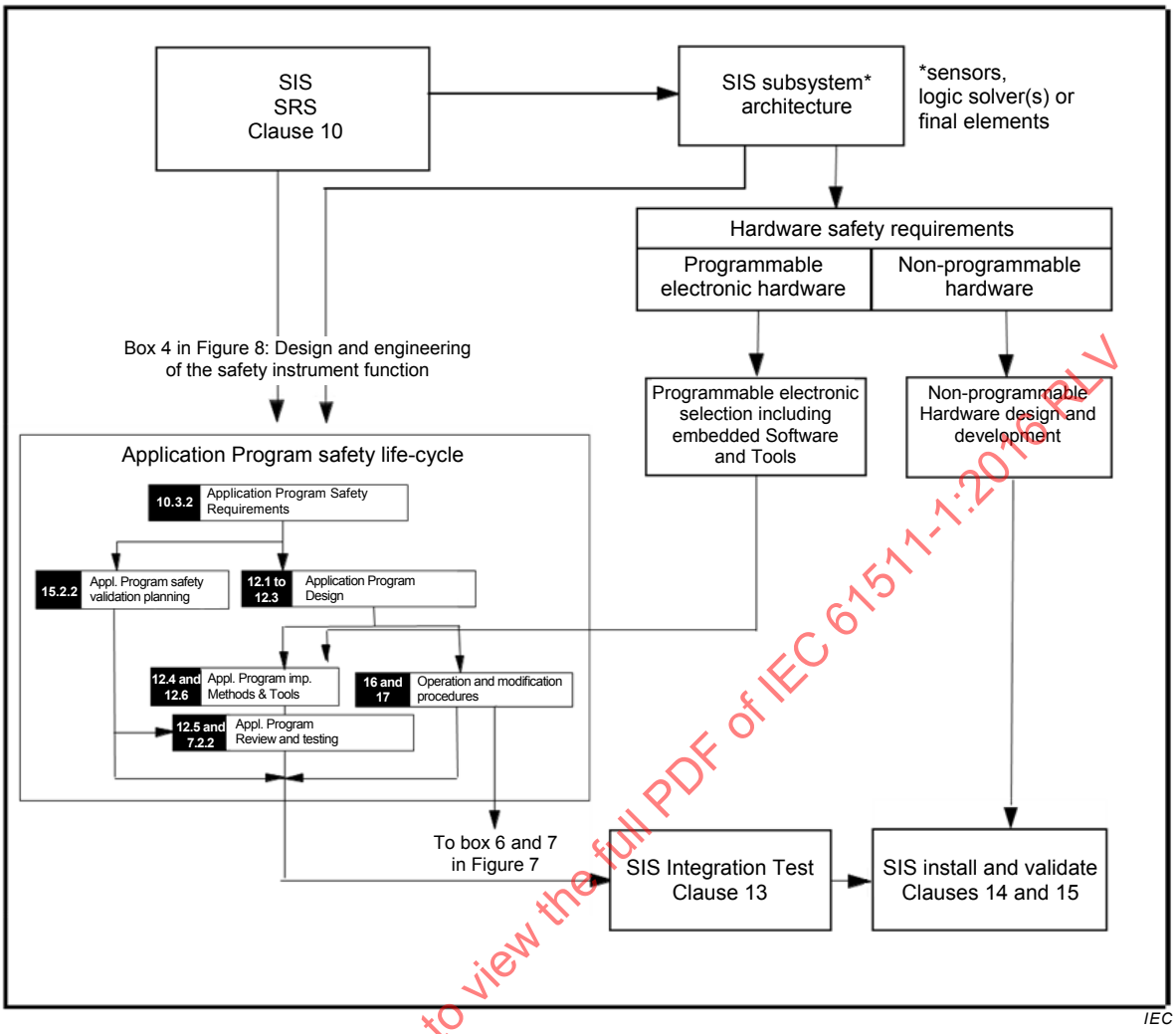


Figure ~~10~~ 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle

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

Safety life-cycle phase		Objectives	Require-ments Clause	Inputs	Outputs
Figure 8 box number	Title				
10.3.2	Application program safety requirements	To specify application program safety requirements for each SIS necessary to implement the required SIF. To specify the requirements for application program for each SIF allocated to that SIS.	10.3 11.5	SIS safety requirements. Safety manuals of the selected SIS. SIS architecture.	SIS application program safety requirements specification. Verification information.
15.2.2	Application program safety validation planning	To develop a plan for validating the application program.	15.2.2, 15.2.5	SIS application program safety requirements.	SIS safety validation planning. Verification information.
12.1 to 12.3	Application program development	Architecture. To create an application program architecture that fulfils the specified requirements for application program safety. To review and evaluate the requirements placed on the application program by the hardware architecture of the SIS. To specify the procedures for the development of the application program.	12.1 (also 10.3, 12.2)	SIS application program safety requirements. SIS hardware architecture design constraints.	Description of the architecture design, e.g., segregation of application program into related process sub-system and SIL, e.g., recognition of common application program modules such as pump or valve sequences. Application program architecture and sub-system integration test requirements. Verification information.
	Application program design	To develop the application program design. To identify a suitable set of configuration, library, management, and simulation and test tools, over the safety life-cycle of the application program.	12.3	SIS application program safety requirements. Description of the architecture design. Manuals of the SIS. Safety Manual of the selected SIS logic solver.	Application program design. Procedures for use during programming. Description of the standard (manufacturers) library functions to be used. Verification information.

Table 3 *(2 of 2)*

Safety life-cycle phase		Objectives	Require-ments Clause	Inputs	Outputs
Figure 8 box number	Title				
12.4 12.6	Application program implementation	Application development and application module development. To implement the application program that fulfils the specified requirements for application safety. To use appropriate support tools and programming languages.	12.4 12.3.4 12.6	Description of the design. List of manuals and procedures of the selected logic solver for use with the application program.	Application program (e.g., function block diagrams, ladder logic). Application program simulation and integration test. Special purpose application program safety requirements. Verification information.
12.5 7.2.2	Application program verification	To verify that the requirements for application program safety have been achieved. To show that all SIS application programs interact correctly to perform their intended functions and do not perform unintended functions.	12.5 7.2.2	Application program simulation and integration test requirements (structure based testing). Application program architecture integration test requirements.	Application program test results. Verified and tested application program system. Verification information.
13	SIS integration test	To integrate the application program onto the target logic solver, including interaction with a sample set of field devices and or simulator.	Clause 13	Application program and logic solver integration test requirements.	Application program and logic solver integration test results.

6.3.2 Methods, techniques and tools shall be applied for each life-cycle phase in accordance with 12.6.2.

6.3.3 Each phase of the SIS safety life-cycle for which safety planning has been carried out shall be verified (see Clause 7) and the results shall be available as described in Clause 19.

7 Verification

7.1 Objective

The objective of Clause 7 is to demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases (Figure 7) as identified by the verification planning.

7.2 Requirements

7.2.1 Verification planning shall be carried out throughout the SIS safety life-cycle and shall define all activities required for the appropriate phase (Figure 7) of the safety life-cycle, including the application program. Verification planning shall conform to the IEC 61511 series by ~~providing~~ addressing the following:

- the verification activities;

- the procedures, measures and techniques to be used for verification including implementation and resolution of resulting recommendations;
- when these activities will take place;
- the persons, departments and organizations responsible for these activities, including levels of independence;
- identification of items to be verified;
- identification of the information against which the verification is carried out;
- the adequacy of the outputs against the requirements for that phase;
- correctness of the data;
- how to handle non-conformances;
- tools and supporting analysis;
- the completeness of the SIS implementation and the traceability of the requirements;
- the readability and audit-ability of the documentation;
- the testability of the design.

7.2.2 Where the verification includes testing, the verification planning shall also address the following:

- the strategy for integration of application program and hardware and field devices, including the integration of sub-systems that shall comply with other standards (such as machinery or burner);
- test scope (describes the test set-up and what type of test to be performed including the hardware, application programming, and programming devices to be included);
- test cases and test data (these will be specific scenarios with the associated data);
- types of tests to be performed;
- test environment including tools, hardware, all software and required configuration;
- test criteria (e.g., pass/fail criteria) on which the results of the test will be evaluated;
- procedures for corrective action on failure during test;
- physical location(s) (e.g., factory or site);
- dependence on external functionality;
- appropriate personnel;
- management of change;
- non-conformances.

7.2.3 Non-safety functions integrated with safety functions shall be verified for non-interference with the safety functions.

7.2.4 Verification shall be performed according to the verification planning.

7.2.5 During testing, any modification shall be subjected to an impact analysis which shall determine all SIS components impacted and the necessary re-verification activities.

7.2.6 The results of the verification process shall be available (see Clause 19), including whether the objective and criteria of the tests have been met.

NOTE 1 Selection of techniques and measures for the verification process and the degree of independence depends upon a number of factors including degree of complexity, novelty of design, novelty of technology and required SIL.

NOTE 2 Examples of some verification activities include design reviews, use of tools and techniques including software verification tools and ~~CAD~~ computer based design analysis tools.

8 Process H&RA

8.1 Objectives

The objectives of the requirements of Clause 8 are 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;
- any requirements for risk reduction;
- the safety functions required to achieve the necessary risk reduction;
- if any of the safety functions are SIFs ~~(see Clause 9)~~.

NOTE 1 Clause 8 addresses process engineers, hazard and risk specialists, safety managers as well as instrument engineers. Its purpose is to recognize the multi-disciplinary approach typically required for the determination of SIF.

NOTE 2 Where reasonably practicable, processes ~~should~~ can be designed to be inherently safe. When this is not practicable, ~~risk reduction methods such as mechanical protection systems and safety instrumented systems may need to be added to the design~~ other layers of protection (see Figure 9) can be required. ~~These systems may act alone or in combination with each other.~~ In some applications, industry standards can specify the use of particular protection layers.

NOTE 3 ~~Typical risk reduction methods found in process plants are indicated in Figure 9 (no hierarchy implied).~~ The risk reduction can be accomplished using several layers of protection and the layers can be independent, sufficient, dependable and auditable.

8.2 Requirements

8.2.1 A H&RA shall be carried out on the materials, process and ~~its associated~~ equipment ~~(for example, BPCS)~~. It shall result in:

- a description of each identified hazardous event and the factors that contribute to it ~~(including human errors)~~;
- a description of the likelihood and consequence of each hazardous event;
- consideration of ~~conditions~~ process operating modes such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown;
- the determination of ~~requirements for~~ additional risk reduction necessary to achieve the required functional safety;
- a description of, or references to information on, the measures taken to reduce or remove hazards and risk;
- a detailed description of the assumptions made during the analysis of the risks including ~~probable~~ demand rates on the protection layers and ~~equipment failure rates~~ the average frequency of dangerous failures of the initiating sources, and of any credit taken for operational constraints or human intervention;
- ~~allocation of the safety functions to layers of protection (see Clause 9) taking account of potential reduction in effective protection due to common cause failure between the safety layers and between the safety layers and the BPCS (see note 1);~~
- identification of those safety function(s) applied as SIF(s) ~~(see Clause 9)~~.

  NOTE 1 In determining the safety integrity requirements, account ~~will need to~~ can be taken of the effects of common cause between systems that create demands and the protection ~~systems~~ layers that are designed to respond to those demands. An example of this would be where demands can arise through ~~control system~~ BPCS failure and the equipment used within the ~~protection systems~~ protective layers is similar or identical to the equipment used within the ~~control system~~ BPCS. In such cases, a demand caused by a failure of BPCS equipment ~~in the control system~~ may not be responded to effectively if a common cause has rendered similar equipment in the protection ~~system~~ layer to be ineffective. It may not be possible to recognize common cause problems during the initial hazard identification and risk analysis because at such an early stage the design of the protection ~~system~~ layers will not necessarily have been completed. In such cases, it ~~will~~ can be necessary to reconsider the safety integrity requirements and SIF once the design of the SIS and other protection layers

has been completed. In determining whether the overall design of process and protection layers meets requirements, common cause failures will ~~need to~~ be considered.

NOTE 2 Examples of techniques that can be used to establish the required SILs of SIFs are illustrated in IEC 61511-3:2016.

8.2.2 The average frequency of dangerous failures ~~rate~~ of a BPCS ~~(which does not conform to IEC 61511) that places a demand on a protection layer~~ as an initiating source shall not be assumed to be $<10^{-5}$ per hour.

8.2.3 The H&RA shall be recorded in such a way that the relationship between the above items is clear and traceable.

NOTE 1 The above requirements do not mandate that ~~risk and risk reduction targets~~ the safety integrity requirements have to be assigned as numerical values. ~~Graphical~~ Qualitative or semi-quantitative approaches (see IEC 61511-3:2016, Annexes C, D & E) can also be used.

NOTE 2 The ~~extent of risk reduction necessary should~~ safety integrity requirements vary depending on the application and national legal requirements. An accepted principle in many countries is that additional risk reduction measures ~~should~~ can be applied until the cost incurred becomes disproportionate to the ~~risk reduction~~ improvement in safety integrity achieved.

8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction;
- a description of, or references to information on, the measures taken to reduce or remove the threats.

NOTE 1 Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

NOTE 2 The information and control of boundary conditions needed for the security risk assessment are typically with owner/operating company of a facility, not with the supplier. Where this is the case, the obligation to comply with 8.2.4 can be with the owner/operating company of the facility.

NOTE 3 The SIS security risk assessment can be included in an overall process automation security risk assessment.

NOTE 4 The SIS security risk assessment can range in focus from an individual SIF to all SISs within a company.

9 Allocation of safety functions to protection layers

9.1 Objectives

The objectives of the requirements of Clause 9 are to

- allocate safety functions to protection layers;
- determine the required SIFs;
- determine for each SIF the associated safety integrity ~~level~~ requirements.

NOTE 1 Account ~~should~~ can be taken, during the process of allocation, of other industry standards or codes.

NOTE 2 The integrity requirements for each SIF might include the associated risk reduction, PFD, PFH or SIL.

9.2 Requirements of the allocation process

9.2.1 The allocation process shall result in

- the allocation of safety functions required to achieve the necessary risk reduction to specific protection layers ~~for the purpose of prevention, control or mitigation of hazards from the process and its associated equipment~~;
- the allocation of risk reduction ~~targets to safety instrumented functions~~ or average frequency of dangerous failure to each SIF.

NOTE Legislative requirements or other industry codes may ~~determine priorities in~~ influence the allocation process.

9.2.2 The required SIL shall be derived taking into account the required ~~risk reduction~~ PFD or PFH that is to be provided by the SIF.

NOTE Further guidance can be found in IEC 61511-3:2016.

9.2.3 For each SIF operating in demand mode, the required SIL shall be specified in accordance with either Table 4 or Table 5. ~~If Table 4 is used then neither the proof-test interval nor the demand rate shall be used in the determination of safety integrity level.~~

9.2.4 For each SIF operating in continuous mode ~~of operation~~, the required SIL shall be specified in accordance with Table 5.

Table ~~3~~ 4 – Safety integrity ~~levels~~ requirements: ~~probability of failure on demand~~ PFD_{avg}

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**~~Target average probability of failure on demand~~ PFD_{avg}**	**~~Target~~ Required risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	> 1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

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

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	**~~Target~~ Average frequency of dangerous failures ~~to perform the safety instrumented function~~ (failures per hour)**
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE 1 Further explanation of modes of operation can be found in 3.2.39.

NOTE 2 The SIL is defined numerically so as to provide an objective measure for comparison of alternate designs and solutions. However, it is recognized that, given the current state of knowledge, many systematic causes of failure can only be assessed qualitatively.

NOTE 3 The required average frequency of dangerous failures ~~per hour~~ for a continuous mode SIF is determined by considering the risk ~~(in terms of hazard rate)~~ caused by failure of the continuous mode SIF together with the failures ~~rate~~ of other ~~equipment~~ devices that lead to the same risk, taking into consideration ~~contributions from~~ the risk reduction provided by other protection layers.

~~NOTE 4 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).~~

9.2.5 In cases where the allocation process results in a risk reduction requirement of >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour for a single SIS or multiple SISs or SIS in conjunction with a BPCS protection layer, there shall be a reconsideration of the application (e.g., process, other protection layers) to determine if any of the risk parameters can be modified so that the risk reduction requirement of >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is avoided. The review shall consider whether:

– the process or vessels/pipe work can be modified to remove or reduce hazards at the source;

– additional safety-related systems or other risk reduction means, not based on instrumentation, can be introduced;

– the severity of the consequence can be reduced, e.g., reducing the amount of hazardous material;

– the likelihood of the specified consequence can be reduced e.g., reducing the likelihood of the initiating source of the hazardous event.

NOTE Applications which require the use of a single SIF with a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour need to be avoided because of the difficulty of achieving and maintaining such high levels of performance throughout the SIS safety life-cycle. Risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour can require high levels of competence and high levels of coverage for all factory acceptance testing, proof testing, verification, and validation activities.

9.2.6 If after further consideration of the application and confirmation that a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is still required, then consideration should be given to achieving the safety integrity requirement using a number of protection layers (e.g., SIS or BPCS) with lower risk reduction requirements. If the risk reduction is allocated to multiple protection layers then such protection layers shall be independent from each other or the lack of independence shall be assessed and shown to be sufficiently low compared to the risk reduction requirements. The following factors shall be considered during this assessment:

– common cause of failure of SIS and the cause of demand;

NOTE 1 The extent of the common cause can be assessed by considering the diversity of all devices where failure could cause a demand and all devices of the BPCS protection layer and/or the SIS used for risk reduction.

NOTE 2 An example of common cause between the SIS and the cause of demand is if loss of process control through sensor fault or failure can cause a demand and the sensor used for control is of the same type as the sensor used for the SIS.

– common cause of failure with other protection layers providing risk reduction;

NOTE 3 The extent of the common cause can be assessed by considering the diversity of all devices of the BPCS protection layer and/or the SIS used to achieve the risk reduction requirements.

NOTE 4 An example of common cause between SISs providing risk reduction is when two separate and independent SISs with diverse measurements and diverse logic solvers are used but the final actuation devices are two shut off valves of similar types or a single shut off valve actuated by both SISs.

– any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times;

NOTE 5 Even if the protective layers are diverse then synchronous proof testing will reduce the overall risk reduction achieved and this can be a significant factor impeding achievement of the necessary risk reduction for the hazardous event.

NOTE 6 When high levels of risk reduction are required and proof tests are desynchronised according to Note 5 then the dominant factor is normally common cause failure even if multiple independent protection layers are used to reduce risk. Dependency within and between protection layers providing risk reduction for the same hazardous event can be assessed and shown to be sufficiently low.

9.2.7 If a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is to be implemented, whether allocated to a single SIS or multiple SIS or SIS in conjunction with a BPCS protection layer, then a further risk assessment shall be carried out using a quantitative methodology to confirm that the safety integrity requirements are

achieved. The methodology shall take into consideration dependency and common cause failures between the SIS and:

– any other protection layer whose failure would place a demand on it;
– any other SIS reducing the likelihood of the hazardous event;
– any other risk reduction means that reduce the likelihood of the hazardous event (e.g., safety alarms).

9.2.8 If the risk reduction required for a hazardous event is allocated to multiple SIFs in a single SIS, then the SIS shall meet the overall risk reduction requirement.

9.2.9 The results of the allocation process shall be recorded so that the SIFs are described in terms of the functional needs of the process, e.g., the actions to be taken, set points, reaction times, activation delays, fault treatment, valve closure requirements, and in terms of the risk reduction requirements.

NOTE This description can be in an unambiguous logical form and can be referred to as the process requirements specification or the safety description. The description can make the intent and the approach used in the allocation process clear. The process requirements specification is used as input information for the SRS covered in Clause 10 and can be sufficiently detailed to ensure adequate specification of the SIS and its devices. For example, the description can include the set-points for sensors, the process safety time available for response, and the valve closure requirements.

~~**9.3 Additional requirements for safety integrity level 4**~~

~~**9.3.1** No safety instrumented function with a safety integrity level higher than that associated with SIL 4 shall be allocated to a safety instrumented system. Applications which require the use of a single safety instrumented function of safety integrity level 4 are rare in the process industry. Such applications shall be avoided where reasonably practicable because of the difficulty of achieving and maintaining such high levels of performance throughout the safety life cycle. Where such systems are specified they will require high levels of competence from all those involved throughout the safety life cycle.~~

~~If the analysis results in a safety integrity level of 4 being assigned to a safety instrumented function, consideration shall be given to changing the process design in such a way that it becomes more inherently safe or adding additional layers of protection. These enhancements could perhaps then reduce safety integrity level requirements for the safety instrumented function.~~

~~**9.3.2** A safety instrumented function of safety integrity level 4 shall be permitted only if the criteria in either a), or both b) and c) below are met.~~

~~a) There has been an explicit demonstration, by a combination of appropriate analytical methods and testing, of the target safety integrity failure measure having been met.~~

~~b) There has been extensive operating experience of the components used as part of the safety instrumented function.~~

~~NOTE Such experience should have been gained in a similar environment and, as a minimum, components should have been used in a system of comparable complexity level.~~

~~c) There is sufficient hardware failure data, obtained from components used as part of the safety instrumented function, to allow sufficient confidence in the hardware safety integrity target failure measure that is to be claimed.~~

~~NOTE The data should be relevant to the proposed environment, application and complexity level.~~

9.3 Requirements on the basic process control system as a protection layer

9.3.1 The basic process control system may be ~~identified~~ claimed as a protection layer as shown in Figure 9.

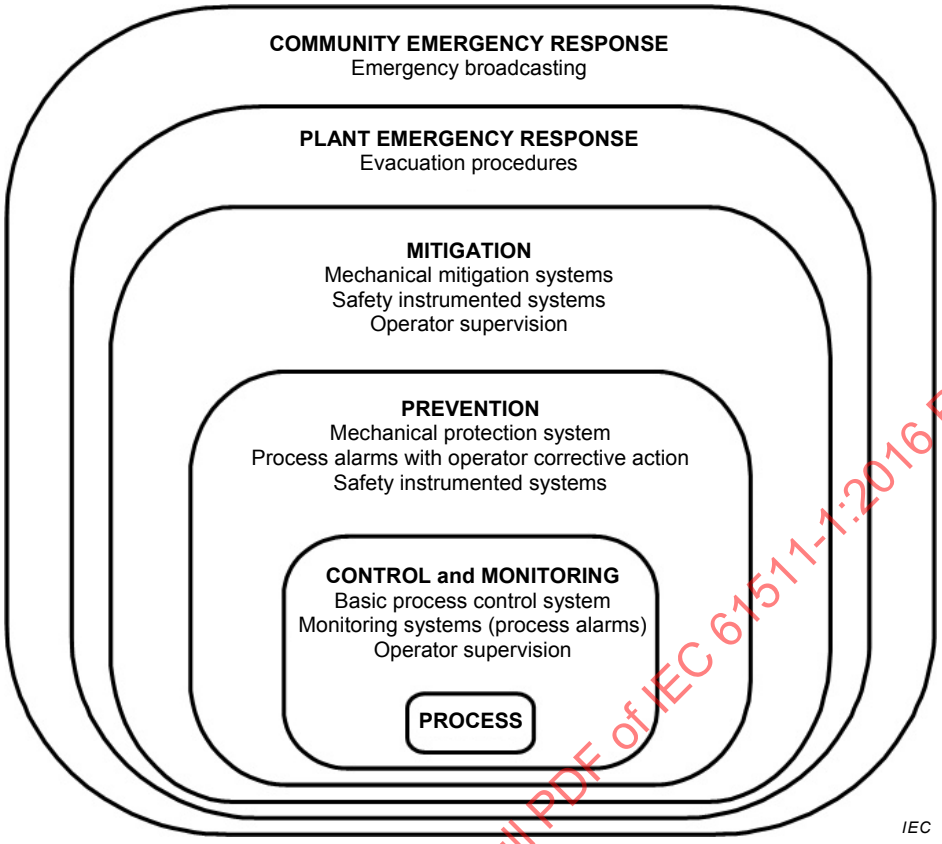


Figure 5 – Typical protection layers and risk reduction ~~methods found in process plants~~ means

9.3.2 The risk reduction ~~factor~~ claimed for a BPCS ~~(which does not conform to IEC 61511 or IEC 61508) used as a~~ protection layer shall be ≤10.

NOTE ~~When considering how much risk reduction credit to be given to a BPCS,~~ Consideration ~~should~~ can be given to the fact that a ~~part of the~~ BPCS may also be an initiating source for ~~an event~~ the demand on the protection layer.

9.3.3 If the risk reduction claimed for a BPCS protection layer is > 10, then the BPCS shall be designed and managed to the requirements within the IEC 61511 series.

9.3.4 If it is not intended that the BPCS conform to the IEC 61511 series, then:

- no more than one BPCS protection layer shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is the initiating source for the demand on the protection layer; or
- no more than two BPCS protection layers shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is not the initiating source of the demand.

NOTE The identified BPCS protection layer can consist of one BPCS as the initiating source for the demand (see 8.2.2) and a second independent BPCS protection layer (see 9.3.2 and 9.3.3) or up to two independent BPCS protection layers when the initiating source is not related to BPCS failure.

9.3.5 When 9.3.4 applies, each BPCS protection layer shall be independent and separate from the initiating source and from each other to the extent that the claimed risk reduction of each BPCS protection layer is not compromised.

NOTE 1 The assessment of separation and independence can consider what is necessary to achieve the risk reduction, e.g., the central processing units (CPU), input/output modules, relays, field devices, application programming, networks, program database, engineering tools, human machine interface, by-pass tools and other devices.

NOTE 2 A hot backup controller is not considered to be independent of the primary controller because it is subject to common cause failure (for example, hot backup controllers have components that are common to both the primary and the backup controller, such as the backplane, firmware, diagnostics, transfer mechanisms and undetected dangerous failures).

9.4 Requirements for preventing common cause, common mode and dependent failures

9.4.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between:

- protection layers ~~and between~~;
- protection layers and the BPCS.

are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.

NOTE A definition of dependent failure is provided in 3.2.12.

9.4.2 The assessment shall consider the following:

- independence between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS ~~(for example, can plugging of relief valves cause the same problems as plugging of sensors in a SIS?)~~.

NOTE 1 Common causes from the process can be addressed. Plugging of relief valves may cause the same problems as plugging of sensors in a SIS.

NOTE 2 Independence and physical separation can be addressed. A Human Machine Interface, SIS/BPCS networks or bypass means can cause common cause failure.

10 SIS safety requirements specification (SRS)

10.1 Objective

The objective of Clause 10 is to specify the requirements for the SIS, including any application programs and the architecture of the SIS.

10.2 General requirements

The safety requirements shall be derived from the allocation of SIF and from those requirements identified during ~~safety planning~~ H&RA.

~~NOTE~~ The SIS requirements ~~should~~ shall be expressed and structured in such a way that they are

- clear, precise, verifiable, maintainable and feasible;
- written to aid comprehension and interpretation by those who ~~are likely to~~ will utilise the information at any phase of the safety life-cycle.

10.3 SIS safety requirements

10.3.1 Addresses issues that shall be considered when developing the SIS safety requirements.

10.3.2 These requirements shall be sufficient to design the SIS and shall include ~~the following~~ a description of the intent and approach applied during the development of the SIS safety requirements as applicable:

- a description of all the SIF necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative);
- a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);
- requirements to identify and take account of common cause failures;
- a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated;
- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system);
- the assumed sources of demand and demand rate on each SIF;
- requirements relating to proof test intervals;
- requirements relating to proof test implementation;
- response time requirements for ~~the SIS~~ each SIF to bring the process to a safe state within the process safety time;

  NOTE See IEC 61511-2:2016 for further discussion of process safety time.
- the required SIL and mode of operation (demand/continuous) for each SIF;
- a description of SIS process measurements, range, accuracy and their trip points;
- a description of ~~SIS~~ SIF process output actions and the criteria for successful operation e.g., ~~requirements for tight shut-off~~ leakage rate for valves;
- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives for each SIF;
- requirements for manual shutdown for each SIF;
- requirements relating to energize or de-energize to trip for each SIF;
- requirements for resetting ~~the SIS~~ each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element resets after trips);
- maximum allowable spurious trip rate for each SIF;
- failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shut-down);
- any specific requirements related to the procedures for starting up and restarting the SIS;
- all interfaces between the SIS and any other system (including the BPCS and operators);
- a description of the modes of operation of the plant and ~~identification of the safety instrumented functions required to operate~~ requirements relating to SIF operation within each mode;
- the application ~~software~~ program safety requirements as listed in 10.3.2;
- requirements for ~~overrides/inhibits/~~ bypasses including written procedures to be applied during the bypassed state which describe how ~~they~~ the bypasses will be administratively controlled and then subsequently cleared;
- the specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS~~. Any such action shall be determined~~, taking into account of all relevant human factors;
- the mean repair time which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints;

- identification of the dangerous combinations of output states of the SIS that need to be avoided;
- identification of the extremes of all environment conditions that are likely to be encountered by the SIS ~~shall be identified~~ during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;
- identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIFs may be required to support these process operating modes;
- definition of the requirements for any SIF necessary to survive a major accident event, e.g., time required for a valve to remain operational in the event of a fire.

~~NOTE Non-safety instrumented functions may be carried out by the SIS to ensure orderly shutdown or faster start-up. These should be separated from the safety instrumented functions.~~

~~**10.3.2** The software safety requirements specification shall be derived from the safety requirements specification and the chosen architecture of the SIS.~~

10.3.3 The application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS. The application program safety requirements may be located in the SRS or in a separate document (e.g., application program requirements specification). The input to the application program safety requirements for each SIS subsystem shall include:

a) the specified safety requirements of each SIF, including sensor voting, etc.;

b) the requirements resulting from the SIS architecture and the safety manual such as limitations and constraints of the hardware and embedded software;

c) any requirements of safety planning arising from 5.2.4.

10.3.4 The application program safety requirements shall be specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS.

10.3.5 The application program safety requirements specification shall be sufficiently detailed to allow the design and implementation to achieve the required functional safety and to allow a functional safety assessment to be carried out. The following shall be considered:

- the SIFs supported by the application program and their SIL;
- real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a specified time period;
- program sequencing and time delays if applicable;
- equipment and operator interfaces and their operability;
- all relevant modes of operation of the process as specified in the SRS;
- action to be taken on bad process variable such as sensor value out of range, excessive range of change, frozen value, detected open circuit, detected short circuit;
- functions enabling proof testing and automated diagnostics tests of external devices (e.g., sensors and final elements) performed in the application program;
- application program self-monitoring (e.g., application driven watch-dogs and data range validation);
- monitoring of other devices within the SIS (e.g., sensors and final elements);

- any requirements related to periodic testing of SIF when the process is operational;
- references to the input documents (e.g., specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS);
- the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;
- process dangerous states (for example closure of two isolation gas valves at the same time that could lead to pressure fluctuations thus leading to a dangerous state) generated by the application program shall be identified and avoided;
- definitions of process variable validation criteria for each SIF.

10.3.6 The application program safety requirements specification shall be expressed and structured in such a way that they:

- describe the intent and approach underpinning the application program safety requirements;
- are clear and understandable to those who will utilize the document at any phase of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by all users (e.g., plant operators, maintenance personnel, application programmers);
- are verifiable, testable, modifiable;
- are traceable back through all deliverables including the detailed design documents, the SRS and the H&RA that identifies the required SIF and SIL.

11 SIS design and engineering

11.1 Objective

The objective of the requirements of Clause 11 is to design one or multiple SIS to provide the SIF and meet the specified ~~safety~~ integrity ~~level(s)~~ requirements (e.g., SIL, associated risk reduction, PFD and /or PFH).

11.2 General requirements

11.2.1 The design of the SIS shall be in accordance with the SIS safety requirements specifications, taking into account all the requirements of Clause 11.

11.2.2 Where the SIS is to implement both ~~safety~~ SIFs and non-SIFs then all the hardware, embedded software and application program that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL of any of the SIFs it can impact.

~~NOTE 1 Wherever practicable, the safety instrumented functions should be separated from the non-safety instrumented functions.~~

~~NOTE 2 Adequate independence means that neither the failure of any non-safety functions nor the programming access to the non-safety software functions is capable of causing a dangerous failure of the safety instrumented functions.~~

11.2.3 Where the SIS is to implement SIF of different SIL, then the shared or common hardware and embedded software and application program shall conform to the highest SIL ~~unless it can be shown that the safety instrumented functions of lower safety integrity level cannot negatively affect the safety instrumented functions of higher safety integrity levels~~.

NOTE Embedded software or application programs of different SIL could coexist in the same device provided it can be demonstrated that the SIF of lower SIL cannot negatively affect the SIF of the higher SIL.

11.2.4 If it is intended not to qualify the BPCS to the IEC 61511 series, then the ~~basic process control system~~ SIS shall be designed to be separate and independent from the BPCS to the extent that the ~~functional~~ safety integrity of the SIS is not compromised.

NOTE 1 Operating information ~~may~~ can be exchanged but ~~should~~ not compromise the functional safety of the SIS.

NOTE 2 Devices of the SIS ~~may~~ can also be used for functions of the BPCS if it can be demonstrated that a failure of the BPCS does not compromise the SIF of the SIS.

11.2.5 Requirements for operability, maintainability, diagnostics, inspection and testability shall be addressed during the design of the SIS in order to ~~facilitate implementation of human factor requirements in the design (for example, by-pass facilities to allow on-line testing and alarm when in bypass)~~ reduce the likelihood of dangerous failures.

~~NOTE The maintenance and test facilities should be designed to minimize as far as practicable the likelihood of dangerous failures arising from their use.~~

11.2.6 The design of the SIS shall take into account human capabilities and limitations and be suitable for the tasks assigned to operators and maintenance staff. The design of ~~all human-machine~~ operator interfaces shall follow good human factors practice and shall accommodate the likely level of training ~~or awareness~~ that operators should receive.

NOTE 1 For example, human factor studies may be necessary if operation requires data entry of limits or other operator input on a regular basis.

11.2.7 The SIS shall be designed in such a way that once it has placed the process in a safe state, the process shall remain in the safe state until a reset has been initiated unless otherwise directed by the SRS.

11.2.8 Manual means (e.g., emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the SRS.

11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependency between the SIS and BPCS, and the SIS and other protection layers.

11.2.10 A device used ~~to perform part of a safety instrumented function~~ by the BPCS shall not be used ~~for basic process control purposes,~~ by the SIS where a failure of that device ~~results in a failure of the basic process control function which causes~~ may result in both a demand on the SIF and a dangerous failure of the SIF, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand on the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared ~~component~~ device because if the shared ~~component~~ device fails, a demand will be created immediately to which the SIS may not be capable of responding. For that reason, additional analysis ~~will~~ can be necessary in these cases to ensure that the dangerous failure rates of the shared ~~equipment is~~ devices are sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.

11.2.11 For ~~subsystems~~ any SIS device that on loss of ~~power~~ utility(e.g., electrical power, air, hydraulics or pneumatic supply) does not fail to the safe state, ~~all of the following requirements~~ loss of utility and SIS circuit integrity shall be detected and alarmed (e.g., end-of-line monitoring, supply pressure measurement, hydraulic or pneumatic pressure monitoring) and action taken according to 11.3.

- ~~power supply integrity is ensured using supplemental power supply (for example, battery back-up, uninterruptible power supplies);~~
- ~~loss of power to the subsystem is detected.~~

NOTE 1 Utility integrity can be improved through using a supplementary supply (e.g., battery back-up, uninterruptible power supplies, air reservoir, hydraulic accumulator, second gas supply).

NOTE 2 The loss of a utility is likely to affect multiple SIFs and, possibly, multiple SISs. Hence common cause failure of multiple SIFs can be considered.

11.2.12 The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

NOTE Guidance related to SIS security is provided in ISA TR84.00.09 and IEC 62443-2-1:2010.

11.2.13 A safety manual covering operation, maintenance, fault detection and constraints associated with the SIS shall be available covering the intended configurations of the devices and the intended operating environment.

11.2.14 All communications used to implement a SIF shall be established using techniques appropriate for safety applications to meet the required SIL.

11.3 Requirements for system behaviour on detection of a fault

~~**11.3.1** The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem which can tolerate a single hardware fault shall result in either~~

~~a) a specified action to achieve or maintain a safe state (see note); or~~

~~b) continued safe operation of the process whilst the faulty part is repaired. If the repair of the faulty part is not completed within the mean time to restoration (MTTR) assumed in the calculation of the probability of random hardware failure, then a specified action shall take place to achieve or maintain a safe state (see note).~~

~~Where the above actions depend on an operator taking specific actions in response to an alarm (for example, opening or closing a valve), then the alarm shall be considered part of the safety instrumented system (i.e., independent of the BPCS).~~

~~Where the above actions depend on an operator notifying maintenance to repair a faulty system in response to diagnostic alarm, this diagnostic alarm may be a part of the BPCS but shall be subject to appropriate proof testing and management of change along with the rest of the SIS.~~

~~NOTE The specified action (fault reaction) required to achieve or maintain a safe state should be specified in the safety requirements (see 10.3). It may consist, for example, of the safe shutdown of the process or of that part of the process which relies, for risk reduction, on the faulty subsystem or other specified mitigation planning.~~

~~**11.3.2** The detection of a dangerous fault (by diagnostic test, proof tests or by any other means) in any subsystem having no redundancy and on which a safety instrumented function is entirely dependent (see note 1) shall, in the case that the subsystem is used only by safety instrumented function(s) operation in the demand mode, result in either~~

~~a) a specified action to achieve or maintain a safe state; or~~

~~b) the repair of the faulty subsystem within the mean-time-to-restoration (MTTR) period assumed in the calculation of the probability of random hardware failure. During this time the continuing safety of the process shall be ensured by additional measures and constraints. The risk reduction provided by these measures and constraints shall be at least equal to the risk reduction provided by the safety instrumented system in the absence of any faults. The additional measures and constraints shall be specified in the SIS operation and maintenance procedures. If the repair is not undertaken within the specified mean time to restoration (MTTR) then a specified action shall be performed to achieve or maintain a safe state (see note 2).~~

~~Where the above actions depend on an operator taking specific actions in response to an alarm (for example, opening or closing a valve), then the alarm shall be considered part of the safety instrumented system (i.e., independent of the BPCS).~~

~~Where the above actions depend on an operator notifying maintenance to repair a faulty system in response to a diagnostic alarm, this diagnostic alarm may be a part of BPCS but~~

~~shall be subject to appropriate proof testing and management of change along with the rest of the SIS.~~

~~NOTE 1 A safety instrumented function is considered to be entirely dependent on a subsystem if a failure of this subsystem results in a failure of the safety instrumented function in the safety instrumented system under consideration, and the safety instrumented function has not also been allocated to another protection layer (see Clause 9).~~

~~NOTE 2 The specified action (fault reaction) required to achieve or maintain a safe state should be specified in the safety requirements (see 10.3). It may consist, for example, of the safe shutdown of the process, or that part of the process which relies, for risk reduction, on the faulty subsystem or on other specified mitigation planning.~~

~~**11.3.3** The detection of a dangerous fault (by diagnostic test, proof tests or by any other means) in any subsystem having no redundancy and on which a safety instrumented function is entirely dependent (see note 1) shall, in the case of a subsystem which is implementing any safety instrumented function(s) operating in the continuous mode (see note 2), result in a specified action to achieve or maintain a safe state.~~

~~The specified action (fault reaction) required to achieve or maintain a safe state shall be specified in the safety requirements specification. It may consist, for example, of the safe shutdown of the process, or that part of the process which relies, for risk reduction, on the faulty subsystem, or other specified mitigation planning. The total time to detect the fault and to perform the action shall be less than the time for the hazardous event to occur.~~

~~Where the above actions depend on an operator taking specific actions in response to an alarm (for example, opening or closing a valve), then the alarm shall be considered part of the safety instrumented system (i.e., independent of the BPCS).~~

~~Where the above actions depend on an operator notifying maintenance to repair a faulty system in response to a diagnostic alarm, this diagnostic alarm may be a part of the BPCS but shall be subject to appropriate proof testing and management of change along with the rest of the SIS.~~

~~NOTE 1 A safety instrumented function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety instrumented function in the safety instrumented system under consideration, and the safety instrumented function has not also been allocated to another protection layer.~~

~~NOTE 2 When there is a possibility that some combination of output states of a subsystem can directly cause a hazardous event then it should be necessary to regard the detection of dangerous faults in the subsystem as a safety instrumented function operating in the continuous mode.~~

11.3.1 When a dangerous fault in a SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation. If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken. Where the compensating measures depend on an operator taking specific action in response to an alarm (e.g., opening or closing a valve) then the alarm shall be considered part of the SIS.

NOTE 1 The specified action (fault reaction) required to achieve or maintain a safe state of the process can be specified in the SRS (see 10.3.1). It can consist of the safe shutdown of the process or of that part of the process which relies on the faulty SIS for risk reduction.

NOTE 2 The compensating measures required for continued safe operations can depend on safety integrity requirements, the tolerable risk associated with the hazardous event, the hardware fault tolerance of the SIS, the anticipated MRT and the availability of any other layers of protection. In some cases it can be adequate to ensure action is taken to ensure repair of the dangerous failure within the assumed MPRT in the calculation of the PFDavg but in other cases it can be judged necessary to provide other measures to compensate for the reduced risk reduction until the SIS is fully restored. See also 16.2.3.

11.3.2 Where any dangerous fault in an SIS is brought to the attention of an operator by an alarm then the alarm shall be subject to appropriate proof testing and management of change.

11.4 Requirements for Hardware fault tolerance

11.4.1 For safety instrumented functions, the sensors, logic solvers and final elements shall have a minimum hardware fault tolerance.

NOTE 1 Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.

NOTE 2 The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in SIF design that may result due to the number of assumptions made in the design of the SIF, along with uncertainty in the failure rate of components or subsystems used in various process applications.

NOTE 3 It is important to note that the hardware fault tolerance requirements represent the minimum component or subsystem redundancy. Depending on the application, component failure rate and proof testing interval, additional redundancy may be required to satisfy the SIL of the SIF according to 11.9.

11.4.2 For PE logic solvers, the minimum hardware fault tolerance shall be as shown in Table 5.

Table 5 – Minimum hardware fault tolerance of PE logic solvers

SIL	Minimum hardware fault tolerance		
	SFF < 60 %	SFF 60 % to 90 %	SFF > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

11.4.3 For all subsystems (for example sensors, final elements and non-PE logic solvers) except PE logic solvers the minimum hardware fault tolerance shall be as shown in Table 6 provided that the dominant failure mode is to the safe state or dangerous failures are detected (see 11.3), otherwise the fault tolerance shall be increased by one.

NOTE To establish whether the dominant failure mode is to the safe state it is necessary to consider each of the following:

- the process connection of the device;
- use of diagnostic information of the device to validate the process signal;
- use of inherent fail safe behaviour of the device (for example, live zero signal, loss of power results in a safe state).

11.4.4 For all subsystems (for example, sensor, final elements and non-PE logic solvers) excluding PE logic solvers the minimum fault tolerance specified in Table 6 may be reduced by one if the devices used comply with all of the following:

- the hardware of the device is selected on the basis of prior use (see 11.5.3);
- the device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction;
- the adjustment of the process-related parameters of the device is protected, for example, jumper, password;
- the function has an SIL requirement of less than 4.

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

~~SIL~~	~~Minimum hardware fault tolerance (see 11.4.3 and 11.4.4)~~
~~1~~	~~0~~
~~2~~	~~1~~
~~3~~	~~2~~
~~4~~	~~Special requirements apply (see IEC 61508)~~

~~**11.4.5** Alternative fault tolerance requirements may be used providing an assessment is made in accordance to the requirements of IEC 61508-2, Tables 2 and 3.~~

11.4.1 The SIS shall have a minimum HFT with respect to each SIF it implements.

NOTE This does not exclude the possibility that the HFT may be reduced below the minimum requirement at certain times during operation of the system following the occurrence of faults.

11.4.2 When the SIS can be split into independent SIS subsystems (e.g. sensors, logic solvers and final elements), then the HFT can be assigned at the SIS subsystem level.

11.4.3 The HFT of the SIS or its SIS subsystems shall be in accordance with;

- 11.4.5 to 11.4.9 of clause 11 or,
- the requirements of 7.4.4.2 (route 1H) of IEC 61508-2:2010 or,
- the requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.

NOTE The route developed in IEC 61511 is derived from route 2_H of IEC 61508-2:2010.

11.4.4 When determining the achieved HFT, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements. Any such fault exclusions shall be justified and documented.

NOTE Further information about fault exclusion can be found in ISO13849-1:2006 and ISO13849-2:2012.

11.4.5 The minimum HFT for a SIS (or its SIS subsystems) implementing a SIF of a specified SIL shall be in accordance with Table 6 and if appropriate 11.4.6 and 11.4.7.

NOTE The HFT requirements in Table 6 represent the minimum system or, where relevant, the SIS subsystem redundancy. Depending on the application, device failure rate and proof-testing interval, additional redundancy can be required to satisfy the failure measure for the SIL of the SIF according to 11.9.

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

11.4.6 For a SIS or SIS subsystem that does not use FVL or LVL programmable devices and if the minimum HFT as specified in Table 6, would result in additional failures and lead to decreased overall process safety, then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.

NOTE Fault tolerance is the preferred solution to achieve the required confidence that a robust architecture has been achieved. When 11.4.6 applies, the purpose of the justification is to demonstrate that the proposed alternative architecture provides an equivalent or better solution. This may vary depending on the application and/or the technology in use; examples include: back-up arrangements (e.g., analytical redundancy, replacing a failed sensor output by physical calculation results from other sensors outputs); using more reliable items of the same technology (if available); changing for a more reliable technology; decreasing common cause failure impact by using diversified technology; increasing the design margins; constraining the environmental conditions (e.g. for electronic components); decreasing the reliability uncertainty by gathering more field feedback or expert judgment.

11.4.7 If a fault tolerance equal to zero results from applying 11.4.6, the justification required by 11.4.6 shall provide evidence that the related dangerous failure modes can be excluded, in accordance with 11.4.4 including consideration of the potential for systematic failures.

11.4.8 FVL and LVL programmable devices shall have diagnostic coverages not less than 60 %.

11.4.9 Reliability data used in the calculation of the failure measure shall be determined by an upper bound statistical confidence limit of no less then 70 %.

11.5 Requirements for selection of ~~components and subsystems~~ devices

11.5.1 Objectives

The objectives of the requirements of 11.5 are to:

- specify the requirements for the selection of ~~components or subsystems~~ devices which are to be used as part of the SIS;
- specify the requirements to enable a ~~component or subsystem~~ device to be integrated in the architecture of a SIS;
- specify acceptance criteria for ~~components and subsystems~~ devices in terms of associated SIF and safety integrity requirements.

11.5.2 General requirements

11.5.2.1 ~~Components and subsystems~~ Devices selected for use as part of a SIS ~~for~~ with a specified SIL ~~1 to SIL 3 applications~~ shall ~~either~~ be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010~~, as appropriate, or else they shall be in accordance with 11.4~~ and/or 11.5.3 through 11.5.6, as appropriate.

NOTE Devices assessed against IEC 61508-2:2010 and IEC 61508-3:2010 can be applied in accordance with the requirements for systematic capability in IEC 61508-2:2010.

11.5.2.2 ~~Components and subsystems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate.~~ All devices shall be suitable for the operating environment as determined through consideration of the manufacturer's documentation, the constraints within the SRS and the reliability parameters assumed in respect of 11.9. Suitability of the selected devices shall always be considered in the context of the operating environment.

NOTE Devices may exhibit different failure rates dependent on the operating environment and mode of operation. Failure rate data available from manufacturers may not be valid in all applications. For example, the failure rate and failure mode distribution can be different for a valve that is frequently exercised versus one that stands still for long periods of time.

~~**11.5.2.3** The suitability of the selected components and subsystems shall be demonstrated through consideration of~~

- ~~manufacturer hardware and embedded software documentation;~~
- ~~if applicable, appropriate application language and tool selection (see 12.4.4).~~

~~**11.5.2.4** The components and subsystems shall be consistent with the SIS safety requirements specifications.~~

~~NOTE For the selection of components and subsystems, all the other applicable aspects of this standard still apply, including architectural constraints, hardware integrity, behaviour on detection of a fault and application software.~~

11.5.3 Requirements for the selection of ~~components and subsystems~~ devices based on prior use

11.5.3.1 Appropriate evidence shall be available that the ~~components and subsystems~~ devices are suitable for use in the SIS.

NOTE 1 ~~In the case of field elements, there may be extensive operating experience either in safety or non-safety applications. This can be used as a basis for the evidence.~~ The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 2 Level of detail of the evidence ~~should~~ can be in accordance with the complexity of the considered ~~component or subsystem~~ device ~~and with the probability of failure necessary to achieve the required safety integrity level of the safety instrumented function(s)~~.

NOTE 3 A prior use evaluation involves gathering documented information concerning the device performance in a similar operating environment. Prior use demonstrates the functionality and integrity of the installed device, including the process interfaces, full device boundary, communications, and utilities. The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 4 Prior use data can contribute to a database for the calculation of hardware failure rates as described in 11.9.3.

11.5.3.2 The evidence of suitability shall include the following:

- consideration of the manufacturer's quality, management and configuration management systems;
- adequate identification and specification of the ~~components or subsystems~~ devices;
- demonstration of the performance of the ~~components or subsystems~~ devices in similar operating ~~profiles and physical~~ environments;

  NOTE 1 In the case of field devices (e.g., sensors and final elements) fulfilling a given ~~function~~ specification, ~~this function~~ the behaviour of the device in the operating environment is usually identical in safety and non-safety applications~~, which means that the device will be performing in a similar way in both type of applications~~. Therefore, ~~consideration of the performance of such devices in non-safety applications should also be deemed~~ evidence of the performance of similar devices in non-safety applications can also be used to satisfy this requirement.

- the volume of the operating experience.

  NOTE 2 For field devices, information relating to operating experience is mainly recorded in the user's list of equipment approved for use in their facilities, based on an extensive history of successful performance in safety and non-safety applications, and on the elimination of equipment not performing in a satisfactory manner. The list of field devices ~~may~~ can be used to support claims of experience in operation, provided that:

  – the list is updated and monitored regularly;

  – field devices are only added when sufficient operating experience has been obtained;

  – field devices are removed when they show a history of not performing in a satisfactory manner;

  – the ~~process application~~ operating environment is included in the list where relevant.

  NOTE 3 Device performance is highly affected by the operating environment. It is generally recommended that selection of devices can be based on adequate performance of an installed sufficient number of devices in multiple installations for a sufficient operating time. The gained experience can allow time to reveal early failures, such as those related to specification, handling, installation, and commissioning.

  NOTE 4 The amount of operational experience to gain credible statistical reliability data is typically much higher compared to the operational experience necessary to get evidence of prior use.

11.5.3.3 All devices selected on the basis of prior use shall be identified by a specified revision number and shall be under the control of a management of change procedure. In the

case of a change being made to the device, the continued validity of the evidence of prior use shall be justified by evaluating the significance of the change made.

11.5.4 Requirements for selection of FPL programmable ~~components and subsystems~~ devices (e.g., field devices) based on prior use

11.5.4.1 For SIL 1, SIL 2, and SIL 3, the requirements of 11.5.2 and 11.5.3 apply, together with the following subclauses.

11.5.4.2 All configuration options of the device possibly influencing safety shall be identified and considered. It is important to check that wherever specific settings are not defined that the default settings of the device are confirmed to be appropriate. Unused features of the ~~components and subsystems~~ devices shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required SIF.

11.5.4.3 For the specific configuration and ~~operational profile~~ operating environment of the ~~hardware and software~~ device, the evidence of suitability shall consider:

- characteristics of input and output signals;
- modes of use;
- functions and configurations used;
- ~~previous~~ prior use in similar ~~applications and physical~~ operating environments.

11.5.4.4 In addition, for SIL 3 applications, an ~~formal~~ assessment ~~(in accordance with 5.2.6.1)~~ of the FPL device shall be carried out to show that:

- the FPL device is both able to perform the required functions and that ~~the previous~~ prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;
- appropriate standards for hardware and software have been applied;
- the FPL device has been used or tested in configurations representative of the intended operational profiles.

~~**11.5.4.5** For SIL 3 applications, a safety manual including constraints for operation, maintenance and fault detection shall be available covering the typical configurations of the FPL device and the intended operational profiles.~~

11.5.5 Requirements for selection of LVL programmable ~~components and subsystems (for example, logic solvers)~~ devices based on prior use

11.5.5.1 The following requirements ~~may only be applied~~ apply to PE ~~logic solvers~~ devices used in SISs which implement SIL 1 or SIL 2 SIFs.

11.5.5.2 The requirements of 11.5.4 apply.

11.5.5.3 Where there is any difference between the ~~operational profiles and physical environments of a component or subsystem~~ operating environment of a device as experienced previously, and the ~~operational profile and physical~~ operating environment of the ~~component or subsystem~~ device when used within the SIS, then any such differences shall be identified and there shall be an assessment based on analysis and testing, as appropriate, to show that the likelihood of systematic faults when used in the SIS is sufficiently low.

11.5.5.4 The operating experience considered necessary to justify the suitability shall be determined taking into account:

- the SIL of the SIF;

- the complexity and functionality of the ~~component or subsystem~~ devices.

~~NOTE See IEC 61511-2 for further guidance.~~

11.5.5.5 For SIL 1 or 2 applications, a safety configured PE logic solver may be used provided that all the following additional provisions are met:

- understanding of unsafe failure modes;
- use of techniques for safety configuration that address the identified failure modes;
- the embedded software has a good history of use for safety applications;
- protection against unauthorized or unintended modifications.

NOTE A safety configured PE logic solver is a general purpose industrial grade PE logic solver which is specifically configured by the OEM, a systems engineer or the end-user for use in safety applications.

11.5.5.6 A formal assessment ~~(in accordance with 5.2.6.1)~~ of any PE logic solver used in a SIL 2 application shall be carried out to show that:

- it is both able to perform the required functions and that ~~previous~~ prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;
- measures are implemented to detect faults during program execution and initiate appropriate ~~reaction~~ responses; these measures shall comprise all of the following:
  - program sequence monitoring;
  - protection of code against modifications or failure detection by on-line monitoring;
  - failure assertion or diverse programming;
  - range check of variables or plausibility check of values;
  - modular approach;
  - appropriate coding standards have been used for the embedded and utility software;
  - testing in typical configurations, with test cases representative of the intended operational profiles;
  - trusted verified software modules and components have been used;
  - the system has undergone dynamic analysis and testing;
  - the system does not use artificial intelligence or dynamic reconfiguration;
  - documented fault-insertion testing (negative testing) has been performed.

~~**11.5.5.7** For SIL 2 applications, a safety manual including constraints for operation, maintenance and fault detection shall be available covering the typical configurations of the PE logic solver and the intended operational profiles.~~

11.5.6 Requirements for selection of FVL programmable ~~components and subsystems (for example, logic solvers)~~ devices

When the applications are programmed using a FVL, the PE ~~logic solver~~ device shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010.

11.6 Field devices

11.6.1 Field devices shall be selected and installed to minimize failures that could result in inaccurate information due to conditions arising from the ~~process and environmental conditions~~ operating environment. Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, coking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse lines.

11.6.2 Energize to trip ~~discrete input/output~~ circuits shall apply ~~a method~~ means to ensure circuit and power supply integrity.

NOTE 1 An example of such ~~a method~~ means is an end-of-line monitor, where a pilot current is continuously monitored to ~~ensure~~ detect circuit continuity and where the pilot current is not of sufficient magnitude to affect proper I/O operation.

NOTE 2 Additional requirements for loss of power can be found in 11.2.11.

~~**11.6.3** Each individual field device shall have its own dedicated wiring to the system input/output, except in the following cases.~~

- ~~Multiple discrete sensors are connected in series to a single input and the sensors all monitor the same process condition (for example, motor overloads).~~
- ~~Multiple final elements are connected to a single output.~~

  ~~NOTE For two valves connected to one output, both valves are required to change state at the same time for all the safety instrumented functions that use the two valves.~~
- ~~A digital bus communication with overall safety performance that meets the integrity requirements of the SIF it services.~~

11.6.3 Smart sensors shall be write-protected to prevent inadvertent modification ~~from a remote location~~, unless appropriate safety review (e.g., H&RA) allows the use of read/write.

NOTE The review ~~should~~ can take into account human factors such as failure to follow procedures.

11.7 Interfaces

11.7.1 General

~~Human machine and communication~~ Interfaces to the SIS can include, but are not limited to:

- operator interface(s);
- maintenance/engineering interface(s);
- communication interface(s).

11.7.2 Operator interface requirements

11.7.2.1 Where the SIS operator interface is via the BPCS operator interface, account shall be taken of credible failures that may occur in the BPCS operator interface.

NOTE This can include preparing plans to enable an orderly safe shutdown in the event of total failure of the operational displays.

11.7.2.2 The design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while ~~the unit is running~~ hazards are present. If the design does require the use of operator actions, the design should include facilities for protection against operator error.

NOTE If the operator has to select a particular option, there ~~should~~ can be a ~~repeat~~ confirmation step.

11.7.2.3 Bypass switches or means shall be protected to prevent unauthorized use (e.g., by key locks or passwords in conjunction with effective management controls).

NOTE Consideration can be given to enforcing time limits on bypass operation and to limiting the number of bypasses that can be active at any one time.

11.7.2.4 The SIS status information that is critical to maintaining the ~~SIL~~ SIF shall be available as part of the operator interface. This information may include:

- where the process is in its sequence;
- indication that SIS protective action has occurred;

- indication that a protective function is bypassed;
- indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- status of sensors and final elements;
- the loss of energy where that energy loss impacts safety;
- the results of diagnostics;
- failure of environmental conditioning equipment which is necessary to support the SIS.

11.7.2.5 The SIS operator interface design (see 11.7.2.7) shall be such as to prevent changes to the SIS application ~~software~~ program.

11.7.2.6 ~~Where safety information needs to be transmitted from the BPCS to the SIS, systems should be used which can selectively allow writing from the BPCS to specific SIS variables.~~ Where information is transferred from the BPCS to the SIS, systems, equipment or procedures ~~should~~ shall be applied to confirm that the ~~proper selection~~ correct information has been ~~transmitted and received by the SIS~~ transferred and that the safety ~~functionality~~ integrity of the SIS is not compromised.

~~NOTE 1 If the options or bypasses are selected in the BPCS and downloaded to the SIS then failures in the BPCS may interfere with the ability of the SIS to operate on demand. If this can occur then the BPCS will become safety related.~~

~~NOTE 2 In batch processes an SIS may be used to select different set points or logic functions depending on the recipe being used. In these cases the operator interface may be used to make the required selection.~~

~~NOTE 3 Provision of incorrect information from the BPCS to the SIS shall not compromise safety.~~

NOTE The systems, equipment or procedures used can include control over selective writing from the BPCS to specific SIS variables.

11.7.2.7 The design of the SIS operator interface via the BPCS operator interface shall be such that provision of incorrect information or data from the BPCS to the SIS shall not compromise safety.

11.7.3 Maintenance/engineering interface requirements

11.7.3.1 The design of ~~PE~~ the SIS maintenance/engineering interface shall ensure that any failure of this interface shall not adversely affect the ability of the SIS to ~~bring~~ carry out the ~~process to a safe state~~ required SIFs. This may require disconnecting of maintenance/engineering interfaces, such as programming panels, during normal SIS operation.

11.7.3.2 The maintenance/engineering interface shall provide the following functions with access security protection to each:

- SIS mode of operation, program, data, means of disabling alarm communication, test, bypass, maintenance;
- SIS diagnostic, voting and fault handling services;
- add, delete, or modify application ~~software~~ program;
- data necessary to troubleshoot the SIS;
- where bypasses are required they should be installed such that alarms and manual shutdown facilities are not disabled.

~~NOTE Software issues apply only to SIS using PE technology.~~

11.7.3.3 The maintenance/engineering interface shall not be used as the operator interface.

11.7.3.4 Enabling and disabling the read-write access shall be carried out only by a configuration ~~or programming~~ management process using the maintenance/engineering interface with appropriate documentation and security measures such as authentication and user secure channels.

11.7.4 Communication interface requirements

11.7.4.1 The design of any SIS communication interface shall ensure that any failure of the communication interface shall not adversely affect the ability of the SIS to ~~bring the process to~~ achieve or maintain a safe state of the process.

11.7.4.2 When the SIS ~~shall be~~ is able to communicate with the BPCS and peripherals ~~with no impact on the SIF~~, the communication interface, BPCS, or peripherals shall not adversely impact any of the SIFs within the SIS.

11.7.4.3 The communication interface shall be sufficiently robust to withstand electro-magnetic interference including power surges without causing a dangerous failure of the ~~SIF~~ SIS.

11.7.4.4 The communication interface shall be suitable for communication between devices referenced to different electrical ground potentials.

NOTE An alternate medium (e.g., fibre optics) ~~may~~ can be required.

11.8 Maintenance or testing design requirements

11.8.1 The design shall allow for testing of the SIS either end-to-end or in ~~parts~~ segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.

NOTE The term “end-to-end” means from process fluid at sensor end to process fluid at actuation end.

11.8.2 When on-line proof testing is required, test facilities shall be an integral part of the SIS design ~~to test for undetected failures~~.

11.8.3 When test ~~and/~~ or bypass facilities are included in the SIS, they shall conform with the following:

- The SIS shall be designed in accordance with the maintenance and testing requirements defined in the SRS;
- The operator shall be alerted to the bypass of any portion of the SIS via an alarm ~~and/~~ or operating procedure.

11.8.4 The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.

11.8.5 Compensating measures that ensure continued safe operation shall be provided in accordance with 11.3 when the SIS is in bypass (repair or testing).

11.8.6 Forcing of inputs and outputs in PE SIS shall not be used as a part of application ~~software~~ program(s), operating procedure(s) and maintenance (except as noted below).

Forcing of inputs and outputs without taking the SIS out of service shall not be allowed unless supplemented by procedures and access security. Any such forcing shall be announced or set off an alarm, as appropriate.

11.9 ~~SIF probability of failure~~ Quantification of random failure

11.9.1 The ~~probability of~~ calculated failure ~~on demand~~ measure of each SIF shall be equal to, or ~~less~~ better than, the target failure measure related to the SIL as specified in the SRS. This shall be ~~verified~~ determined by calculation.

~~NOTE 1 In the case of safety instrumented functions operating in the demand mode of operation, the target failure measure should be expressed in terms of the average probability of failure to perform its design function on demand, as determined by the safety integrity level of the safety instrumented function (see Table 3).~~

~~NOTE 2 In the case of a safety instrumented function operating in the continuous mode of operation, the target failure measure should be expressed in terms of the frequency of a dangerous failure per hour, as determined by the safety integrity level of the safety instrumented function (see Table 4).~~

~~NOTE 3 It is necessary to quantify the probability of failure separately for each safety instrumented function because different component failure modes could apply and the architecture of the SIS (in terms of redundancy) may also vary.~~

~~NOTE 4 The target failure measure may be a specified value of average probability of failure on demand or dangerous failure rate derived from a quantitative analysis or the specified range associated with the SIL if it has been determined by qualitative methods.~~

NOTE In complex applications, the hazardous event frequency can be used as an alternative to the target failure measures (e.g., where different demand causes have different safety integrity requirements or where non-independent SISs act in sequence).

11.9.2 The calculated ~~probability of~~ failure measure of each SIF due to ~~hardware~~ random failures shall take into account all contributing factors including the following:

a) the architecture of the SIS and of its SIS subsystems where relevant as they relate to each SIF under consideration;

b) the estimated failure rate related to each ~~subsystem~~ failure mode, due to random hardware ~~faults~~ failures, ~~in any modes~~ which would ~~cause~~ contribute to a dangerous failure of the SIS but which are detected by diagnostic tests;

c) the estimated failure rate related to each ~~subsystem~~ failure mode, due to random hardware ~~faults~~ failures, ~~in any modes~~ which would ~~cause~~ contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests but which are detected by proof tests;

~~NOTE The estimated rates of failure of a subsystem can be determined by a quantified failure mode analysis of the design using component or subsystem failure data from a recognized industry source or from experience of the previous use of the subsystem in the same environment as for the intended application, and in which the experience is sufficient to demonstrate the claimed mean time to failure on a statistical basis to a single-sided lower confidence limit of at least 70 %.~~

d) the estimated failure rate related to each failure mode, due to random hardware failure, which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests and undetected by proof tests;

e) the susceptibility of the SIS to failures caused by the proof tests themselves;

f) the susceptibility of the SIS to common cause failures;

g) the diagnostic coverage of any periodic diagnostic tests ~~(determined according to IEC 61511-2)~~, the associated diagnostic test interval and the ~~reliability for~~ probability of failure of the diagnostic facilities;

~~f) the intervals at which proof tests are undertaken;~~

h) the coverage of any periodic proof tests, the associated proof test procedure and the reliability for the proof test facilities and procedure;

i) the repair times for detected failures and the state of the SIS during repairs (on line or off line);

j) the estimated dangerous failure rate of any communication process in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);

k) the estimated ~~rate of dangerous failure of any human~~ likelihood that operator response ~~in any modes which~~ would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);

~~j) the susceptibility to EMC disturbances (for example, according to IEC 61326-1);~~

~~k) the susceptibility to climatic and mechanical conditions (for example, according to IEC 60654-1 and IEC 60654-3).~~

l) the reliability of any utility necessary for the SIS.

NOTE 1 Several modelling ~~methods~~ approaches are available and the most appropriate ~~method~~ approach is a matter for the analyst and ~~should~~ can depend on the circumstances. Available ~~methods~~ means include (see IEC 61508-6:2010, annex B)

~~– simulation;~~

– cause consequence analysis;

– reliability block diagrams;

– fault-tree analysis;

– Markov models;

– Petri nets models.

The probabilistic calculations can be performed analytically or by numerical simulation (e.g., Monte Carlo simulation).

~~NOTE 2 The diagnostic test interval and the subsequent time for repair together constitute the mean time for restoration (see IEV 191-13-08) which should be considered in the reliability model.~~

11.9.3 The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified and shall be based on field feedback from similar devices used in a similar operating environment.

NOTE 1 This includes user collected data, vendor/provider/user data derived from data collected on devices, data from general field feedback reliability databases, etc. In some cases, engineering judgement can be used to assess missing reliability data or evaluate the impact on reliability data collected in a different operating environment.

NOTE 2 The lack of reliability data reflective of the operating environment is a recurrent shortcoming of probabilistic calculations. End-users can organize relevant device reliability data collections in accordance with IEC 60300-3-2:2004 or ISO 14224:2006 to improve the implementation of the IEC 61511 series.

NOTE 3 Vendor data based on returns can be restricted to a population where there is full knowledge of the operational environment and fully recorded in accordance with IEC 60300-3-2:2004 or ISO 14224:2006. The user can also record the operational environment for the SIF and be able to demonstrate that the vendor's operational environment data matches the environment of the SIF.

11.9.4 The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.

NOTE 1 The reliability data uncertainties can be evaluated according to the amount of field feedback (less field feedback results in more uncertainty) or/and exercise of expert judgement. Published standards (IEC 60605-4), Bayesian approaches, engineering judgement techniques, etc. can be used to estimate the reliability data uncertainties.

NOTE 2 The following techniques can be used for calculating the failure measures (more information can be found in IEC 61511-2:2016):

– use of an upper bound confidence of 70 % for each input reliability parameter instead of its mean in order to obtain conservative point estimations of the failure measures, or;

– use the probabilistic distributions functions of input reliability parameters, perform Monte Carlo simulations to obtain an histogram representing the distribution of the failure measure and assess a conservative value from this distribution (e.g., that there is a 90 % confidence that the true failure measure is better than the value calculated).

11.9.5 If, for a particular design, the target failure measure for the relevant SIF is not achieved then:

a) identify the devices or parameters contributing most to the failure measure;

NOTE Fault tree cut-set analysis can be useful here.

b) evaluate the effect of possible improvement measures on the identified devices or parameters (e.g., more reliable devices, additional defences against common mode failures, increased diagnostic or proof test coverage, increased redundancy, reduced proof test interval, staggering tests, etc.);

c) select and implement improvement measures to establish the new result;

d) compare the new result to the target failure measure and repeat the steps a) to d) until the target failure measure is achieved in a conservative manner.

12 Requirements for application software, including selection criteria for utility software

This clause recognizes

– three types of software:

- application software;
- utility software, i.e., the software tools used to develop and verify the application software;
- embedded software, i.e., the software supplied as part of the PE;

– three types of software development language:

- fixed program languages (FPL);
- limited variability languages (LVL);
- full variability languages (FVL).

This standard is limited to application software developed using FPL or LVL. The following requirements are suitable for the development and modification of application software up to SIL 3. Therefore, this standard does not differentiate between SIL 1, 2 and 3.

The development and modification of application software using FPL or LVL up to SIL 3 shall comply with this standard. The development and modification of SIL4 application software shall comply with IEC 61508. The development and modification of application software using FVL shall comply with IEC 61508.

Utility software (together with the manufacturer safety manual which defines how the PE system can be safely applied) shall be selected and applied in conformance with the requirements of 12.4.4. The selection of embedded software shall comply with 11.5.

12.1 Application software safety life-cycle requirements

12.1.1 Objectives

12.1.1.1 The objectives of this clause are:

- to define the activities required to develop the application software for each programmed SIS subsystem;
- to define how to select, control, and apply the utility software used to develop the application software;
- to ensure that adequate planning exists so that the functional safety objectives allocated to the application software are met.

NOTE Figure 10 illustrates the scope of clause 12 within the application safety life cycle.

~~**12.1.2 Requirements**~~

~~**12.1.2.1** A safety life cycle for the development of application software which satisfies the requirements of this clause shall be specified during safety planning and integrated with the SIS safety life cycle.~~

~~**12.1.2.2** Each phase of the application software safety life cycle shall be defined in terms of its elementary activities, objectives, required input information and output results, verification requirements (see 12.7) and responsibilities (see Table 7 and Figure 11).~~

~~NOTE 1 Provided that the application software safety life cycle satisfies the requirements of Table 7, it is acceptable to tailor the depth, number and size of the phases of the V-model (see Figure 12) to take account of the safety integrity and the complexity of the project.~~

~~NOTE 2 The type of software language used (FPL, LVL or FVL) and the closeness of the language to the application functions may impact the scope of the V-model phases.~~

~~NOTE 3 The application software safety requirements specifications may be included as part of the SIS safety requirements specifications.~~

~~NOTE 4 The application software validation plan may be included as part of the overall SIS or SIS subsystem validation plan.~~

~~**12.1.2.3** The PE device that implements the application software shall be suitable for the safety integrity required by each SIF it services.~~

~~**12.1.2.4** Methods, techniques and tools shall be selected and applied for each life-cycle phase so as to~~

- ~~minimize the risk of introducing faults into the application software;~~
- ~~reveal and remove faults that already exist in the software;~~
- ~~ensure that the faults remaining in the software will not lead to unacceptable results;~~
- ~~ensure that the software can be maintained throughout the lifetime of the SIS;~~
- ~~demonstrate that the software has the required quality.~~

~~NOTE The selection of methods and techniques should depend upon the specific circumstances. The factors in this decision are likely to include~~

- ~~amount of software;~~
- ~~degree of complexity;~~
- ~~safety integrity level of the SIS;~~
- ~~consequence in the event of failure;~~
- ~~degree of standardization of design elements.~~

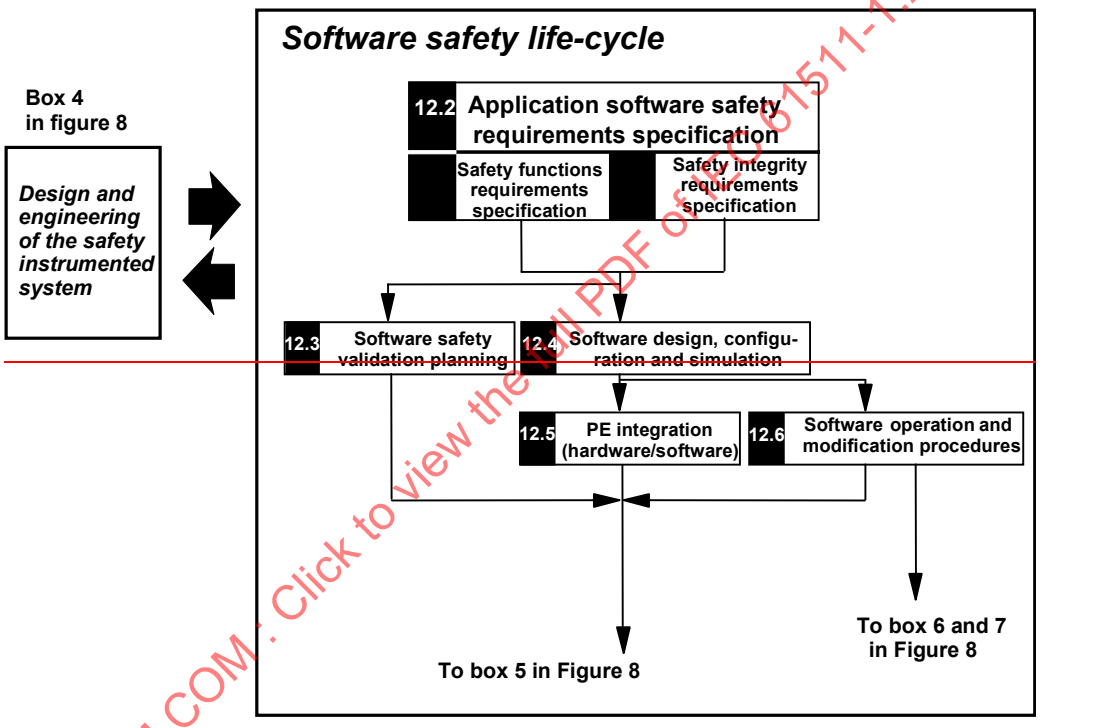
~~**12.1.2.5** Each phase of the application software safety life cycle shall be verified (see 12.7) and the results shall be available (see Clause 19).~~

~~**12.1.2.6** If at any stage of the application software safety life cycle, a change is required pertaining to an earlier life-cycle phase, then that earlier safety life-cycle phase and the following phases shall be re-examined and, if changes are required, repeated and re-verified.~~

~~**12.1.2.7** Application software, the SIS hardware and embedded software and utility software (tools) shall be subject to configuration management (see 5.2.7).~~

~~**12.1.2.8** Test planning shall be carried out. The following issues should be addressed:~~

- ~~the policy for integration of software and hardware;~~
- ~~test cases and test data;~~
- ~~types of tests to be performed;~~
- ~~test environment including tools, support software and configuration description;~~
- ~~test criteria on which the completion of the test will be judged;~~
- ~~physical location(s) (for example, factory or site);~~
- ~~dependence on external functionality;~~
- ~~appropriate personnel;~~
- ~~nonconformances.~~



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

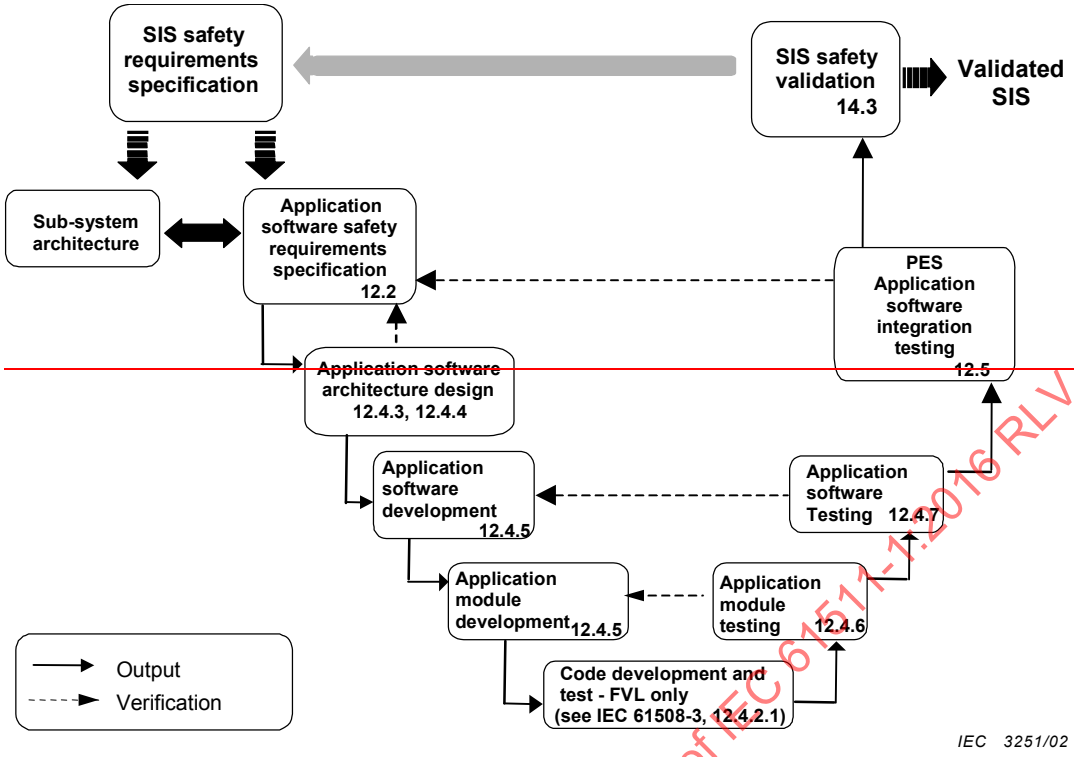


Figure 12 – Software development life cycle (the V-model)

Table 7 – Application software safety life-cycle: overview

Safety life-cycle phase		Objectives	Require-ments clause	Information required	Required results
Figure 11 box number	Title				
12.2	Application software safety requirements specification	To specify the requirements for the software safety instrumented functions for each SIS function necessary to implement the required safety instrumented functions To specify the requirements for software safety integrity for each safety instrumented function allocated to that SIS	12.2.2	SIS safety requirements specification Safety manuals of the selected SIS SIS architecture	SIS application software safety requirements specification Verification information
12.3	Application software safety validation planning	To develop a plan for validating the application software	12.3.2	SIS application software safety requirements specification	SIS application software safety validation plan Verification information
12.4	Application software design and development	Architecture To create a software architecture that fulfils the specified requirements for software safety To review and evaluate the requirements placed on the software by the hardware architecture of the SIS	12.4.3	SIS application software safety requirements specification SIS hardware architecture design manuals	Description of the architecture design, for example, segregation of application S/W into related process sub-system and SIL(s), for example, recognition of common application S/W modules such as pump or valve sequences Application software architecture and sub-system integration test specification Verification information
	Application software design, and development	Support tools and programming languages To identify a suitable set of configuration, library, management, and simulation and test tools, over the whole safety life cycle of the software (utility software) To specify the procedures for development of the application software	12.4.4	SIS application software safety requirements specification Description of the architecture design Manuals of the SIS Safety manual of the selected SIS logic solver	List of procedures for use of utility software Verification information

Safety life-cycle phase		Objectives	Require-ments clause	Information required	Required results
Figure 11 box number	Title				
12.4	Application software design, and development	Application software development and application module development To implement the application software that fulfils the specified requirements for application safety	12.4.5	Description of the architecture design List of manuals and procedures of the selected PES for use of utility software	1) Application software program (for example, function block diagrams, ladder logic) 2) Application program simulation and integration test 3) Special purpose application software safety requirements specification 4) Verification information
12.4	Application program development using full variability languages	Program development and test – FVL only To implement full variability language that fulfils the specified requirements for software safety	12.4.6 and 12.4.7	Special purpose application software safety requirements specification	Refer to IEC 61508-3
12.4	Application software design and development	Application software testing 1) To verify that the requirements for software safety have been achieved 2) To show that all appli-cation program subsystems and systems interact correctly to perform their intended functions and do not perform unintended functions Can be merged with the next phase (12.5) subject to satisfactory test coverage	12.4.6, 12.4.7, 12.7	Application program simulation and integration test specification (structure based testing) Software architecture integration test specification	1) Software test results 2) Verified and tested software system 3) Verification information
12.5	Program-mable elec-tronics integration (hardware and soft-ware)	To integrate the software onto the target programmable electronic hardware	12.5.2	Software and hardware integration test specification	Software and hardware integration test results Verified software and hardware
12.3	SIS safety validation	Validate that the SIS, including the safety application software, meets the safety requirements	12.3	Software and SIS safety validation plans	Software and SIS validation results

12.2 Application software safety requirements specification

NOTE This phase is box 12.2 of Figure 11.

12.2.1 Objective

12.2.1.1 The objective of this clause is to provide requirements for the specification of the application software safety requirements for each programmable SIS subsystem necessary to implement the required safety instrumented function(s) consistent with the architecture of the SIS.

NOTE See Figure 13 for hardware and software architectural relationship.

Programmable SIS subsystem architecture		
Hardware architecture	**Software architecture** (s/w architecture consists of embedded s/w and applications s/w)	
Generic and application specific features in hardware	**Embedded software**	**Application software**
Examples include – **diagnostic tests** – **redundant processors** – **dual I/O cards**	**Examples include** – **communications drivers** – **fault handling** – **executive software**	**Examples include** – **input/output functions** – **derived functions (for example sensor checking if not provided as a service of the embedded software)**

IEC 3252/02

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

12.2.2 Requirements

12.2.2.1 An application software safety requirements specification shall be developed.

NOTE 1 An SIS usually consists of three architectural subsystems: sensors, logic solver and final elements. Furthermore, subsystems could have redundant devices to achieve the required integrity level.

NOTE 2 An SIS hardware architecture with redundant sensors may place additional requirements on the SIS logic solver (for example, implementation of 1oo2 logic).

NOTE 3 The SIS subsystem software safety requirements that have already been specified in the requirements for the SIS (see Clause 10) need not be repeated.

NOTE 4 A software safety requirements specification is required to identify the minimum capabilities of the PE software functionality and also to constrain the selection of any functionality which would result in an unsafe condition.

12.2.2.2 The input to the specification of the software safety requirements for each SIS subsystem shall include

a) the specified safety requirements of the SIF;

b) the requirements resulting from the SIS architecture; and

c) any requirements of safety planning (see Clause 5).

NOTE 1 This information should be made available to the application software developer.

NOTE 2 This requirement does not mean that there should be no iteration between the developer of the SIS architecture, the organization responsible for configuration of the devices and the developer of the application software. As the application software safety requirements and the possible application software architecture (see 12.4.3) become more precise, there may be an impact on the SIS hardware architecture and, for this reason, close cooperation between the SIS architecture developer, the SIS subsystem supplier and the application software developer is essential (see Figure 5).

12.2.2.3 The specification of the requirements for application software safety shall be sufficiently detailed to allow the design and implementation to achieve the required safety integrity and to allow an assessment of functional safety to be carried out. The following shall be considered:

- the functions supported by the application software;
- capacity and response time performance;
- equipment and operator interfaces and their operability;
- all relevant modes of operation of the process as specified in the SIS safety requirement specification;

- action to be taken on bad process variable such as sensor value out of range, detected open circuit, detected short circuit;
- proof tests and diagnostic tests of external devices (for example, sensors and final elements);
- software self-monitoring (for example, includes application driven watch-dogs and data range validation);
- monitoring of other devices within the SIS (for example, sensors and final elements);
- enabling periodic testing of safety instrumented functions when the process is operational;
- references to the input documents (for example, specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS).

12.2.2.4 The application software developer shall review the information in the specification to ensure that the requirements are unambiguous, consistent and understandable. Any deficiencies in the specified safety requirements shall be identified to the SIS subsystem developer.

12.2.2.5 The specified requirements for software safety should be expressed and structured in such a way that they

- are clear to those who will utilize the document at any stage of the SIS safety life cycle; this includes the use of terminology and descriptions which are unambiguous and understood by plant operators and maintainers as well as the application programmers;
- are verifiable, testable, modifiable;
- are traceable back to the specification of the safety requirements of the SIS.

12.2.2.6 The application software safety requirements specification shall provide information allowing proper equipment selection. The following shall be considered:

- functions that enable the process to achieve or maintain a safe state;
- functions related to the detection, annunciation and management of faults in subsystems of the SIS;
- functions related to the periodic testing of safety instrumented functions on-line;
- functions related to the periodic testing of safety instrumented functions off-line;
- functions that allow the SIS to be safely modified;
- interfaces to non-safety related functions;
- capacity and response time performance;
- the safety integrity levels for each of the above functions.

NOTE 1 Dependent on the properties of the selected SIS subsystem some of these functions may be part of the system software.

NOTE 2 Interfaces include both off-line and on-line modification facilities.

12.3 Application software safety validation planning

NOTE This phase is box 12.3 of Figure 11.

12.3.1 Objective

12.3.1.1 The objective of the requirements of this clause is to ensure that suitable application software validation planning is carried out.

~~**12.3.2 Requirements**~~

~~**12.3.2.1** Application software validation planning shall be carried out in accordance with Clause 15.~~

~~**12.4 Application software design and development**~~

~~NOTE This phase is box 12.4 of Figure 11.~~

~~**12.4.1 Objectives**~~

~~**12.4.1.1** The first objective of the requirements of this clause is to create an application software architecture that is consistent with the hardware architecture and that fulfils the specified requirements for software safety (see 12.2).~~

~~**12.4.1.2** The second objective of the requirements of this clause is to review and evaluate the requirements placed on the software by the hardware and embedded software architecture of the SIS. These include side-effects of the SIS hardware/software behaviour, the application specific configuration of SIS hardware, the inherent fault tolerance of the SIS and the interaction of the SIS hardware and embedded software architecture with the application software for safety.~~

~~**12.4.1.3** The third objective of the requirements of this clause is to select a suitable set of tools (including utility software) to develop the application software.~~

~~**12.4.1.4** The fourth objective of the requirements of this clause is to design and implement or select application software that fulfils the specified requirements for software safety (see 12.2) that is analysable, verifiable and capable of being safely modified.~~

~~**12.4.1.5** The fifth objective of the requirements of this clause is to verify that the requirements for software safety (in terms of the required software safety instrumented functions) have been achieved.~~

~~**12.4.2 General requirements**~~

~~**12.4.2.1** The development, test, verification and validation of the full variability language application program shall be in accordance with IEC 61508-3.~~

~~**12.4.2.2** The design method shall be consistent with the development tools and restrictions given for the applied SIS subsystem.~~

~~NOTE Restrictions on the application of the SIS subsystem necessary to ensure compliance with IEC 61511 should be defined in the equipment safety manual.~~

~~**12.4.2.3** The selected design method and application language (LVL or FPL) should possess features that facilitate~~

~~a) abstraction, modularity and other features which control complexity; wherever possible, the software should be based on well-proven software modules that may include user library functions and well-defined rules for linking the software modules;~~

~~b) expression of~~

- ~~functionality, ideally as a logical description or as algorithmic functions;~~
- ~~information flow between modular elements of the application functions;~~
- ~~sequencing requirements;~~
- ~~assurance that safety instrumented functions always operate within the defined time constraints;~~
- ~~freedom from indeterminate behaviour;~~

— assurance that internal data items are not erroneously duplicated, all used data types are defined and appropriate action occurs when data is out of range or bad;

— design assumptions and their dependencies.

c) comprehension by developers and others who need to understand the design, both from an application functional understanding and from a knowledge of the constraints of the technology;

d) verification and validation, including coverage of the application software code, functional coverage of the integrated application, the interface with the SIS and its application specific hardware configuration;

e) application software modification. Such features include modularity, traceability and documentation.

12.4.2.4 The design achieved shall

a) include data integrity checks and reasonableness checks;

NOTE For example, end-to-end checks in communications links, bounds checking on sensor inputs, bounds checking on data parameters and diverse execution of application functions.

b) be traceable to requirements;

c) be testable;

d) have the capacity for safe modification;

e) keep the complexity and size of SIF application software to a minimum.

12.4.2.5 Where the application software is to implement safety instrumented functions of different safety integrity levels or non safety functions, then all of the software shall be treated as belonging to the highest safety integrity level, unless independence between the safety instrumented functions of the different safety integrity levels can be shown in the design. The justification for independence shall be documented. Whether independence is claimed or not, the intended SIL of each SIF shall be identified.

NOTE 1 IEC 61511-2 provides guidance on how to design and develop the application software when both safety and non-safety instrumented functions are to be implemented in the SIS.

NOTE 2 IEC 61511-2 provides guidance on how to design and develop the application software when SIF of different SIL are to be implemented in the SIS.

12.4.2.6 If previously developed application software library functions are to be used as part of the design, their suitability in satisfying the specification of requirements for application software safety (see 12.2) shall be justified. Suitability shall be based upon

- compliance to IEC 61508-3 when using FVL; or
- compliance to IEC 61511 when using FPL or LVL; or
- evidence of satisfactory operation in a similar application which has been demonstrated to have similar functionality or having been subject to the same verification and validation procedures as would be expected for any newly developed software (see 11.5.4 and 11.5.5).

NOTE The justification may be developed during safety planning (see Clause 6).

12.4.2.7 As a minimum, the following information shall be contained in the application program documentation or related documentation:

a) legal entity (for example company, author(s));

b) description;

c) traceability to application functional requirements;

d) logic conventions used;

e) standard library functions used;

f) inputs and outputs; and

g) configuration management including a history of changes.

12.4.3 Requirements for application software architecture

12.4.3.1 The design of the application software architecture shall be based on the required SIS safety specification within the constraints of the system architecture of the SIS. It shall comply with the requirements of the selected subsystem design, its tool set and safety manual.

NOTE 1 The software architecture defines the major components and subsystems of system and application software, how they are interconnected, and how the required attributes, particularly safety integrity, are achieved. Examples of system software modules include operating systems, databases, communication subsystems. Examples of application software modules include application functions which are replicated throughout the plant.

NOTE 2 The application software architecture should also be determined by the underlying architecture of the SIS subsystem provided by the supplier.

12.4.3.2 The description of the application software architecture design shall

a) provide a comprehensive description of the internal structure and of the operation of the SIS subsystem and of its components;

b) include the specification of all identified components, and the description of connections and interactions between identified components (software and hardware);

c) identify the software modules included in the SIS subsystem but not used in any SIF;

d) describe the order of the logical processing of data with respect to the input/output sub-systems and the logic solver functionality, including any limitations imposed by scan times;

e) identify all non-SIF and ensure they cannot affect the proper operation of any SIF.

NOTE It is of particular importance that the architecture documentation is up to date and complete with respect to the SIS subsystem.

12.4.3.3 The set of methods and techniques used to develop the application software should be identified and the rationale for their choice should be justified.

NOTE These methods and techniques should aim at ensuring

– the predictability of the behaviour of the SIS subsystem;

– the fault tolerance (consistent with the hardware) and fault avoidance, including redundancy and diversity.

12.4.3.4 The methods and techniques used in the design of the application software should be consistent with any constraints identified in the SIS subsystem safety manual.

12.4.3.5 The features used for maintaining the safety integrity of all data shall be described and justified. Such data may include plant input-output data, communications data, operation data, maintenance data and internal database data.

NOTE There will be iteration between the hardware and software architecture (see Figure 11) and there is therefore a need to discuss with the hardware developer such issues as the test specification for the integration of the programmable electronics hardware and the software (see 12.5).

12.4.4 Requirements for support tools, user manual and application languages

12.4.4.1 A suitable set of tools, including a sub-set of the application programming language, configuration management, simulation, test harness tools, and, when applicable, automatic test coverage measurement tools, shall be selected.

12.4.4.2 The availability of suitable tools (not necessarily those used during initial system development) to supply the relevant services over the whole lifetime of the SIS should be considered.

NOTE The selection of development tools should depend on the nature of the application software development activities, embedded software and the software architecture (see 12.4.3).

12.4.4.3 A suitable set of procedures for use of the tools should be identified, taking into account safety manual constraints, known weaknesses likely to introduce faults into the application software and any limitations on the coverage of earlier verification and validation.

12.4.4.4 The application language selected shall

- be implemented using a translator/compiler that has been assessed to establish its fitness for purpose;
- be completely and unambiguously defined or restricted to unambiguously defined features;
- match the characteristics of the application;
- contain features that facilitate the detection of programming mistakes; and
- support features that match the design method.

12.4.4.5 When 12.4.4.4 cannot be satisfied, then a justification for the language used shall be documented during application software architecture design description (see 12.4.3). The justification shall detail the fitness for purpose of the language, and any additional measures which address any identified shortcomings of the language.

12.4.4.6 The procedures for use of the application language should specify good programming practice, proscribe unsafe generic software features (for example, undefined language features, unstructured designs), identify checks to detect faults in the configuration and specify procedures for documentation of the application program.

12.4.4.7 The safety manual shall address the following items as appropriate:

a) use of diagnostics to perform safe functions;

b) list of certified/verified safety libraries;

c) mandatory test and system shutdown logic;

d) use of watchdogs;

e) requirements for, and limitations of, tools and programming languages;

f) safety integrity levels for which the device or system is suitable .

12.4.4.8 The suitability of the tools shall be verified.

12.4.5 Requirements for application software development

12.4.5.1 The following information shall be available prior to the start of detailed application software design:

a) the specification of software safety requirements (see 12.2);

b) the description of the application software architecture design (see 12.4.3) including identification of the application logic and fault tolerant functionality, a list of input and output data, the generic software modules and support tools to be used and the procedures for programming the application software.

12.4.5.2 The application software should be produced in a structured way to achieve

- modularity of functionality;
- testability of functionality (including fault tolerant features) and of internal structure;
- the capacity for safe modification;
- traceability to, and explanation of, application functions and associated constraints.

NOTE Wherever possible proven software modules should be used.

12.4.5.3 The design of each application module shall address robustness including

- plausibility checks of each input variable including any global variables used to provide input data;
- full definition of input and output interfaces;
- system configuration checks including the existence and accessibility of expected hardware and software modules.

12.4.5.4 The design of each application software module and the structural tests to be applied to each application software module shall be specified.

12.4.5.5 The application software should

- be readable, understandable and testable;
- satisfy the relevant design principles;
- satisfy the relevant requirements specified during safety planning (see 5.2.4).

12.4.5.6 The application software shall be reviewed to ensure conformance to the specified design, the design principles, and the requirements of safety validation planning.

NOTE Application software review includes such techniques as software inspections, walk-throughs, and formal analysis. It should be used in conjunction with simulation and testing to provide assurance that the application software satisfies its associated specification.

12.4.6 Requirements for application software module testing

NOTE Testing that the application software module correctly satisfies its specification is a verification activity (see also 12.7). It is the combination of review and structural testing that provides assurance that an application software module satisfies its associated specification, i.e., it is verified.

12.4.6.1 The configuration of each input point through the processing logic to the output point shall be checked through review, simulation and testing techniques to confirm that the I/O data is mapped to the correct application logic.

12.4.6.2 Each application software module shall be checked through review, simulation and testing techniques to determine that the intended function is correctly executed and unintended functions are not executed.

The tests shall be suitable for the specific module being tested and the following shall be considered:

- exercising all parts of the application model;
- exercising data boundaries;
- timing effects due to the sequence of execution;
- proper sequence implementation.

12.4.6.3 The results of the application software module testing shall be available.

12.4.7 Requirements for application software integration testing

NOTE Testing that the software is correctly integrated is a verification activity (see also 12.7).

12.4.7.1 The application software tests shall show that all application software modules and components/subsystems interact correctly with each other and with the underlying embedded software to perform their intended function.

NOTE Tests should also be carried out to confirm that the software does not perform unintended functions that jeopardize its safety requirements.

12.4.7.2 The results of application software integration testing shall be available and shall state

a) the test results; and

b) whether the objectives and criteria of the test specification have been met.

If there is a failure, the reasons for the failure shall be reported.

12.4.7.3 During application software integration, any modification to the software shall be subject to a safety impact analysis that shall determine:

a) all software modules impacted; and

b) the necessary re-design and re-verification activities (see 12.6).

12.5 Integration of the application software with the SIS subsystem

NOTE This phase is box 12.5 of Figure 11.

12.5.1 Objective

12.5.1.1 The objective of this clause is to demonstrate that the application software meets its software safety requirements specification when running on the hardware and embedded software used in the SIS subsystem.

NOTE Depending on the nature of the application, these activities may be combined with 12.4.7.

12.5.2 Requirements

12.5.2.1 Integration tests shall be specified as early in the software safety life cycle as possible to ensure the compatibility of the application software with the hardware and embedded software platform such that the functional and performance safety requirements can be met.

NOTE 1 The scope of the tests may be reduced based on previous experience.

NOTE 2 The following should be addressed:

– the division of the application software into manageable integration sets;

– test cases and test data;

– types of tests to be performed;

– test environment, tools, configuration and programs;

– test criteria on which the completion of the test will be judged; and

– procedures for corrective action on failure during test.

12.5.2.2 During testing, any modification or change shall be subject to a safety impact analysis which shall determine

a) all software modules impacted; and

b) the necessary re-verification activities (see 12.7).

12.5.2.3 The following test information shall be available:

a) configuration items under test;

b) configuration items supporting test (tools and external functionality);

c) personnel involved;

d) test cases and test scripts;

e) the test results;

f) whether the objective and criteria of the tests have been met; and

g) if there is a failure, the reasons for the failure, the analysis of the failure and the records of correction including re-test and re-verification (see 12.5.2.2).

12.6 FPL and LVL software modification procedures

NOTE Modification applies primarily to changes occurring during the operational phase of the software.

12.6.1 Objective

12.6.1.1 The objective of the requirements of this clause is to ensure that the software continues to meet the software safety requirements specification after modifications.

12.6.2 Modification requirements

12.6.2.1 Modifications shall be carried out in accordance with 5.2.6.2.2, 5.2.7 and Clause 17 with the following additional requirements.

a) Prior to modification an analysis of the effects of the modification on the safety of the process and on the software design status shall be carried out and used to direct the modification.

b) Safety planning for the modification and re-verification shall be available.

c) Modifications and re-verifications shall be carried out in accordance with the planning.

d) The planning for conditions required during modification and testing shall be considered.

e) All documentation affected by the modification shall be updated.

f) Details of all SIS modification activities shall be available (for example, a log).

12.7 Application software verification

12.7.1 Objectives

12.7.1.1 The first objective of this clause is to demonstrate that the information is satisfactory.

12.7.1.2 The second objective of this clause is to demonstrate that the output results satisfy the defined requirements at each phase of the application software safety life cycle.

12.7.2 Requirements

12.7.2.1 Verification planning shall be carried out for each phase of the application software life cycle in accordance with Clause 7.

12.7.2.2 The results of each phase shall be verified for

a) the adequacy of the outputs from the particular life-cycle phase against the requirements for that phase;

b) the adequacy of the review, inspection and/or testing coverage of the outputs;

c) compatibility between outputs generated at different life-cycle phases;

d) correctness of the data.

12.7.2.3 Verification should also address

a) testability;

b) readability;

c) traceability.

NOTE 1 Data format in the application program should be verified for

– completeness;

– self-consistency;

– protection against unauthorized alteration;

– consistency with the functional requirements.

NOTE 2 Application data should be verified for

– consistency with the data structures;

– completeness;

– compatibility with the underlying system software (for example, sequence of execution, run-time);

– correct data values;

– operation within a known safe boundary.

NOTE 3 Modifiable parameters should be verified for protection against

– invalid of undefined initial values;

– erroneous values;

– unauthorized changes;

– data corruption.

NOTE 4 Communications, process interfaces and associated software should be verified for

– failure detection;

– protection against message corruption, and

– data validation.

12.7.2.4 Non safety functions and process interfaces integrated with safety related signals and functions should be verified for

- non-interference with the safety functions;
- protection against interference with the safety functions in the case of malfunction of the non-safety functions.

12 SIS application program development

12.1 Objective

The objective of Clause 12 is to define the requirements for the development of the application program.

12.2 General requirements

12.2.1 The application program of the SIS shall be in accordance with the application program safety requirements (see 10.3.3) and all the requirements of this clause for all SIL up to and including SIL 3.

12.2.2 The application programmer shall review the information in the SRS and the application program safety requirements to ensure that the requirements are comprehensive, unambiguous, understandable and consistent. Any deficiencies in the application program safety requirements shall be identified and resolved, and if changes are made to the application program safety requirements, an impact analysis shall be carried out.

12.2.3 The IEC 61511 series addresses programming in Limited Variability Languages (LVL) and the use of devices using Fixed Program Languages (FPL). The IEC 61511 series does not address Full Variability Language (FVL) and the IEC 61511 series does not address SIL 4 application programming. Where function blocks are written in FVL then these shall be developed and modified under IEC 61508-3:2010.

12.2.4 Where the application program of the SIS is to implement both safety and non-safety functions, then all of the application program shall be treated as part of the SIS and shall comply with this standard and in addition, it shall be shown through assessment and test that the non-safety functions cannot interfere with the safety functions.

12.2.5 The application program shall be designed in such a way as to ensure that once the SIS has placed the process in a safe state, the process remains in the safe state, including under loss of power conditions and on power restoration, until a reset has been initiated unless otherwise directed by the SRS.

NOTE 1 If the SIF does not have a reset then there can be a documented engineering argument as to why it is acceptable to reinitiate the process without requiring the safe delay a reset would impose.

NOTE 2 More information can be found in 11.2.7.

12.2.6 During SIS start-up (or power up) the application program shall ensure that safety outputs remain in the safe state (typically de-energized state) until a reset has been initiated unless otherwise directed by the SRS.

12.2.7 The application program shall be designed in such a way that all parts of the application program are executed on every application program scan unless there is a specific alternate requirement that is supported in the safety manual. Process safety time requirements shall be considered when establishing application program scanning requirements.

12.2.8 The SIS application program and data shall be subject to modification, revision control, version management, back-up and restoration procedures.

12.2.9 The application program specifies requirements for application programming for users and integrators of SISs. In particular, requirements for the following are specified:

- SIS safety life-cycle phases and activities that are to be applied during the design and development of the application program. These requirements include the application of measures and techniques, which are intended to avoid errors in the application program and to control failures which may occur;

- information relating to the application program validation to be passed to the organization carrying out the SIS integration;
- preparation of information and procedures concerning the application program needed by the user for the operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications of the application program.

12.3 Application program design

12.3.1 An application program design shall address all SIS logic including all process operating modes for each SIF.

12.3.2 The input to the application program design shall be the SRS including the application program requirements (see Clause 10), the SIS architecture (see Clause 11) and the means and tools for developing the application program design (see 12.6). The application program design shall be consistent with and traceable back to the SRS.

12.3.3 The application program design shall allow an assessment of functional safety to be carried out.

12.3.4 The application program design and its decomposition into modules if applicable, shall address how the requirements are to be implemented, including the following as appropriate:

- the functions that enable the process to achieve or maintain a safe state;
- the specification of all identified application program components, and the description of connections and interactions between identified components;
- the timing constraints associated with the application program functions and their implementation in program scan time(s);
- a detailed description of the standard library modules (function blocks) being used;
- a detailed description of the application specific modules (function blocks) being used;
- a description of the way memory allocation has been achieved;
- the list of global variables used and the way in which their integrity is protected;
- identification of all non-SIF and the interfaces to non-safety related parts of the application program, to ensure that they cannot affect the proper operation of any SIF;
- definition of input and output interfaces, including tag listings and the associated data types;
- details of the data exchanged between the SIS application program and the operator interfaces;
- details of the data exchanged between the SIS application program and the BPCS and peripherals such as printers, data storage, etc.;
- how external and internal diagnostic information will be processed and logged;
- detailed description of how the operation and maintenance interfaces are implemented, including the way in which alarms are prioritised, indicated and accepted;
- a detailed description of any application level diagnostics that may be implemented such as external watch dogs, application data integrity checking, sensor validation to meet the required SIL;
- system configuration checks including the existence and accessibility of expected hardware devices and software modules;
- how the complexity in the application program design is minimised e.g., through use of modular design and simple functionality;

- functions related to the detection, annunciation and management of faults in SIS subsystems;
- functions related to the periodic testing of SIF on-line;
- functions related to the periodic testing of SIF off-line;
- functions that allow maintenance of the SIS to be carried out safely;
- references to documents on which the application program design specification is based.

12.3.5 The application program design shall ensure:

- completeness with respect to the SRS and its intended purpose;
- correctness with respect to the SRS and its intended purpose;
- freedom from ambiguity, i.e., clear to those who will utilize the document at any stage of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by plant operators and system maintainers, as well as the application programmers;
- freedom from design faults.

12.4 Application program implementation

12.4.1 The application program development methodology shall comply with the development tools and restrictions given by the manufacturer of the SIS PE subsystem on which the application program shall be used.

12.4.2 The following information shall be contained in the application program or related documentation:

a) the application program originator;

b) a description of the purpose of the application program;

c) the versions of the safety manuals that were used;

d) identification of the dependency of each SIF on the parts (modules) of the application program;

e) traceability to the application program safety requirements specification;

f) identification of each SIF and its SIL;

g) identification and description of the symbols used, including logic conventions, standard library functions, application library functions;

h) identification of the SIS logic solver input and output signals;

i) where the overall SIS utilises communications, a description of the communications information flow;

NOTE An example would be where a SIF uses several logic solvers.

j) a description of the program structure, including a description of the order of the logical processing of data with respect to the input/output sub-systems and any limitations imposed by scan times;

k) If required by the SRS, the means by which:

- the correctness of field data is ensured, (e.g., comparison between analog sensors to improve the diagnostic coverage);
- the correctness of data sent over a communication link is ensured (e.g., when communicating from an HMI, before implementation of a command an ‘ack’ or 'acknowledge’ is transmitted);
- communications are made secure (e.g., cyber security measures);

l) version identification and a history of changes.

12.4.3 If previously developed application program library functions are to be used as part of the design, their suitability shall be justified and based upon:

- compliance to IEC 61508; if proven-in-use evaluation for FVL in compliance to IEC 61508-3:2010 is undertaken, the programmable devices on which the application program library functions execute shall also be evaluated as proven-in-use according to IEC 61508-2:2010; or
- compliance to IEC 61511 prior use requirements (see 11.5.4 or 11.5.5) when using FPL or LVL;
- in all cases, demonstrating that any unused functions do not adversely impact the application program.

12.4.4 The application program shall be produced in a structured way so as to achieve:

- modular decomposition of the functionality;
- keep the complexity of SIF application program to a minimum consistent with that of the complexity of the required SIF;
- testability of functionality (including fault tolerant features) and of the internal structure of the application program;
- traceability to, and explanation of, application functions and associated constraints;
- one to one mapping between the hardware architecture and application program architecture.

12.5 Requirements for application program verification (review and testing)

12.5.1 Verification planning shall be carried out in accordance with Clause 7.

12.5.2 The application program including its documentation shall be reviewed by a competent person not involved in the original development. The approach used for the review and the review results shall be documented.

12.5.3 The application program, including its decomposition into modules if appropriate, shall be verified through review, analysis, simulation and testing techniques using written procedures and test specifications, that shall be carried out to confirm that the application program functions meet the SRS and that unintended functions are not executed and that there are no unintended side effects with respect to the SIF. The following shall be addressed:

- conformance to the application program design specification, the defined means and procedures, and the requirements of safety validation and test planning;
- exercising of all parts of the application program;
- exercising a representative range of data conditions;
- testing for failure conditions (i.e., negative testing);
- timing and the sequence of execution;
- testing of communications to and from the SIS;

  NOTE Wherever feasible the communication overload condition can be verified and tested.
- integration of the off-line application program with the logic solver hardware and the underlying PE;
- internal data flow checks to confirm that the logic solver is not just apparently working, but is working as expected;
- when possible, integration of the application program and 3rd party devices.

12.5.4 The mapping of the I/O data to the application program, including data type and range, shall be verified.

12.5.5 During testing, modifications to the application program shall be subject to an impact analysis in order to determine:

- all application program parts impacted;
- the necessary re-design and re-verification activities.

12.5.6 The results of application program testing shall be documented and include:

- the versions of the application program and its supporting documentation being tested;
- the versions of supporting software and test tools;
- names of the person(s) who performed the tests and reviews and dates;
- descriptions of the tests, reviews and dates performed;
- the test results;
- whether the objective and criteria of the tests have been met;
- if there was a failure during the test, the reasons why the failure occurred, the analysis of the failure and the records of its correction and re-test requirements.

12.6 Requirements for application program methodology and tools

12.6.1 The application program development shall comply with the constraints in the applicable safety manual(s).

NOTE The safety manual(s) can be reviewed and, if required for a specific application, additional procedures for and/or constraints on the use of methodologies and tools can be implemented.

12.6.2 Methods, techniques and tools shall be selected and applied for each life-cycle phase so as to:

- minimize the risk of introducing faults into the application program;
- reveal and remove faults that already exist in the application program;
- ensure as far as is practicable that any faults remaining in the application program will not lead to unacceptable results;
- enhance the means of managing modifications of the application program throughout the lifetime of the SIS;
- provide evidence that the application program has the required quality.

13 Factory acceptance test (FAT)

~~NOTE This clause is informative.~~

13.1 Objective

The objective of Clause 13 is to test the ~~logic solver and associated software together~~ devices of the SIS to ensure that the requirements defined in the SRS are met.

NOTE 1 By testing the logic solver, associated software and hardware prior to ~~installing in a plant~~ installation, errors can be readily identified and corrected.

NOTE 2 The FAT is sometimes referred to as an integration test and can be part of the validation.

NOTE 3 Testing of field elements together with the logic solver can be recommended when there needs to be a high confidence in operation prior to final installation, e.g., subsea applications.

13.2 Recommendations

13.2.1 The need for a FAT ~~should~~ shall be specified during the ~~design phase of~~ safety planning for a project.

NOTE 1 Close co-operation between the logic solver supplier and design contractor ~~may~~ can be required in order to develop the integration tests.

NOTE 2 The activities follow the design and development phases and precede the installation and commissioning.

NOTE 3 The activities are applicable to the SIS subsystems with or without programmable electronics.

NOTE 4 It is usual for the FAT to take place in a factory environment prior to installation and commissioning in the plant.

13.2.2 The planning for a FAT ~~should~~ shall specify the following:

- Types of tests to be performed including black-box system functionality tests; performance tests; internal checks; performance tests; environmental tests; interface testing; testing in degraded or faulted ~~modes~~ condition; exception testing; testing for safe reaction in case of power failure (including restart after power restored); and application of the SIS maintenance and operating manuals;

  NOTE 1 Black-box functionality testing is a test design method that treats the system as a "black box", so it does not explicitly use knowledge of its internal structure. Black- box test design is usually described as focusing on testing function requirements. Synonyms for black box include behavioural, functional, opaque-box, and closed-box testing.

  NOTE 2 Performance tests determine whether the system meets timing, reliability and availability, integrity, safety targets and constraints.

  NOTE 3 Environmental tests include EMC, life-and stress-testing.

  NOTE 4 Internal data flow checks can be carried out to that the SIS is processing input data and generating output response as specified.

- Test cases, test description and test data;

  NOTE 5 Clarity in defining who is responsible for developing the test case and who is going to be responsible for carrying out the test and witnessing the test ~~is~~ can be very important.

- Dependence on other systems/interfaces;
- Test environment and tools;
- Logic solver, sensor and final element configuration;
- Test criteria on which the completion of the test shall be judged;
- Procedures for corrective action on failure of test;
- Test personnel competences;
- Physical location;
- Hazards posed by the testing especially dealing with stored energy;
- A clear diagram of the test-set up.
- Recording of tests conducted, data, results and observations whilst the tests are being conducted.

  NOTE 6 Tests that cannot be physically demonstrated are normally resolved by a formal ~~argument~~ line of reasoning as to why the SIS achieves the requirement, target or constraint.

13.2.3 The FAT ~~should~~ shall take place on a defined version of the logic solver.

13.2.4 The FAT ~~should~~ shall be conducted in accordance with the FAT planning. These tests ~~should~~ shall show that all the logic performs correctly.

13.2.5 For each test carried out the following ~~should~~ shall be addressed:

- the version of the test planning being used;
- the SIF and performance characteristic being tested;
- the detailed test procedures and test descriptions;
- a chronological record of the test activities;
- the tools, equipment and interfaces used.

13.2.6 The results of FAT ~~should~~ shall be documented, stating

- the test cases;
- the test results;
- whether the objectives and test criteria have been met.

If there is a failure during test, the reasons for the failure ~~should~~ shall be documented and analysed and the appropriate corrective action should be implemented.

13.2.7 During FAT, any modification or change ~~should~~ shall be subject to a safety analysis to determine:

- the extent of impact on each SIF;
- the extent of ~~re-test~~ testing and verification which ~~should~~ shall be defined and implemented.

NOTE Commissioning ~~may~~ can commence whilst corrective action is undertaken, depending on the results of the FAT.

14 SIS installation and commissioning

14.1 Objectives

The objectives of the requirements of Clause 14 are to:

- install the SIS according to the specifications and drawings;
- commission the SIS so that it is ready for final system validation.

NOTE The purpose of commissioning activities is to ensure that each of the SIS devices is individually ready to operate, as specified in the design phase.

14.2 Requirements

14.2.1 Installation and commissioning planning shall define all activities required for installation and commissioning. The planning shall provide the following:

- the installation and commissioning activities;
- the procedures, measures and techniques to be used for installation and commissioning;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities.

Installation and commissioning planning may be integrated in the overall project planning where appropriate.

14.2.2 All SIS ~~components~~ devices shall be properly installed according to the design and installation plan(s) ~~(see 14.2.1)~~.

14.2.3 The SIS shall be commissioned in accordance with planning in preparation for the final system validation. Commissioning activities shall include, but not be limited to, confirmation of the following:

- earthing (grounding) has been properly connected;
- energy sources have been properly connected and are operational;
- transportation stops and packing materials have been removed;
- no physical damage is present;
- all instruments have been properly calibrated and configured;

- all field devices are operational;
- logic solver and input/outputs are operational;
- the interfaces to other systems and peripherals are operational;
- all communications between remote SIS systems are operational.

14.2.4 Appropriate records of the commissioning of the SIS shall be produced, stating the ~~test~~ results of the activities and whether the objectives and criteria identified during the design phase have been met. If there is a failure, the reasons for the failure shall be recorded.

14.2.5 Where it has been established that the actual installation does not conform to the design information then the difference shall be evaluated by a competent person and ~~the likely~~ impact of the difference on safety shall be determined. If it is established that the difference has no impact on safety, then the design information shall be updated to "as-built" status. If the difference has a negative impact on safety, then the installation shall be modified to meet the design requirements.

15 SIS safety validation

15.1 Objective

The objective of the requirements of Clause 15 is to validate, through inspection and testing, that the installed and commissioned SIS and its associated SIF(s) achieve the requirements as stated in the SRS.

NOTE This is sometimes referred to as a site acceptance test (SAT).

15.2 Requirements

15.2.1 Validation planning of the SIS shall be carried out throughout the SIS safety life-cycle and shall define all activities and equipment required for validation. The following items shall be included:

- the validation activities including validation of the SIS with respect to the SRS including implementation and resolution of resulting recommendations;
- validation of all relevant process operating modes of the process and its associated equipment including:
  - preparation for use including setting and adjustment;
  - start-up, automatic, manual, semi-automatic, steady state of operation;
  - re-setting, shutdown, maintenance;
  - ~~reasonably foreseeable abnormal conditions, for example, those identified through the risk analysis phase~~ other modes identified in previous phases of the SIS safety life-cycle;
- the procedures, measures and techniques to be used for validation, including how validation activities can be performed, without putting the plant and process at risk of the hazardous events the SIS is to protect against;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities and the levels of independence for validation activities;
- reference to information against which validation shall be carried out (e.g., cause and effect chart);
- the equipment and facilities that needs to be installed or made available (e.g. isolation valves and leak detection equipment that will be needed for the testing of valves).

  NOTE Examples of validation activities include loop testing, logic testing, calibration procedures, simulation of application ~~software~~ program.

15.2.2 ~~Additional~~ Validation planning for the ~~safety~~ application ~~software~~ program shall include the following:

- identification of the ~~safety software~~ application program functions which needs to be validated for each process operating mode before commissioning begins;
- the technical strategy for the validation including (where relevant):
  - manual and automated techniques;
  - static and dynamic techniques;
  - analytical and statistical techniques.
- in accordance with the preceding bullet, the measures (techniques) and procedures that will be used for confirming that each SIF conforms with the specified safety requirements and the specified SIL;
- the required environment in which the validation activities are to take place (e.g., for tests this would include calibrated tools and equipment);
- the application program;
- the pass/fail criteria for accomplishing ~~software~~ validation including:
  - the required process and operator input signals with their sequences and their values;
  - the anticipated output signals with their sequences and their values;
  - other acceptance criteria, for example memory usage, timing and value tolerances.
- the policies and procedures for evaluating the results of the validation, particularly failures;

~~NOTE These requirements are based on the general requirements of 12.2.~~

- all documents (see Clause 19) are validated for accuracy, consistency and traceability of the SIF from inception during the H&RA through the final installed SIF.

15.2.3 Where measurement accuracy is required as part of the validation then instruments used for this function should be calibrated against a specification traceable to a standard within an uncertainty appropriate to the application. If such a calibration is not feasible, an alternative method shall be used and documented.

15.2.4 The validation of the SIS and its associated SIF(s) shall be carried out in accordance with the SIS validation planning. Validation activities shall include, but not be limited to, the following:

- confirmation that the SIS performs under normal and abnormal process operating modes (e.g., start-up, shutdown) as identified in the SRS;
- confirmation that adverse interaction of the BPCS and other connected systems do not affect the proper operation of the SIS;
- the SIS properly communicates (where required) with the BPCS or any other system or network, including during abnormal conditions such as a data overload;
- sensors, logic solver, and final elements perform in accordance with the SRS, including all redundant channels, including abnormal condition such as data overload;

  NOTE If a factory acceptance test (FAT) was performed on the logic solver as described in Clause 13, credit ~~may~~ can be taken for validation of the logic solver by the FAT. After all equipment is installed in the plant, full loop validation will test the logic solver functionality and its connections to other SIS subsystems.
- SIS design documentation is consistent with the installed system;
- confirmation that the SIF performs as specified on invalid process variable values (e.g., out of range);
- the proper shutdown sequence is activated;
- the SIS provides the proper annunciation and proper operation display;

- computations that are included in the SIS are correct for expected range of values but also at limits and over the limits;
- the SIS reset functions perform as defined in the SRS;
- bypass functions operate correctly;
- start-up overrides operate correctly;
- manual shutdown systems operate correctly;
- the proof-test ~~intervals are~~ policy documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- confirmation that the SIS performs as required on loss of utilities (e.g., electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the SIS returns to the desired state;
- confirmation that the EMC immunity, as specified in the SRS (see 10.3), has been achieved.

15.2.5 The ~~software~~ validation of the application program shall determine whether:

- all of the specified ~~software~~ application program safety requirements (see 10.3.2) are correctly performed;
- the ~~software~~ application program does not jeopardize the safety requirements under SIS fault conditions and in degraded modes of operation and for BPCS fault conditions for any interfaces between the SIS and BPCS;
- the application program does not jeopardize the safety requirements by executing ''unused'' software functionality, i.e., functionality not defined in the specification.

The information of the validation activities shall be available.

15.2.6 ~~Appropriate information of the results of the~~ The results from the validation plan activities shall represent and cover the entire SIS validation process. SIS validation documentation shall be produced which provides:

- the version of the SIS validation planning being used;
- the SIF(s) under test (or analysis), along with the specific reference to the requirement identified during the SIS validation planning;
- tools and equipment used, along with their calibration data;
- the results of each test;
- the version of the test specification used;
- the criteria for acceptance of the ~~integration~~ completed tests;
- the version of the SIS hardware, application program(s), and other software being tested;
- any discrepancy between expected and actual results and the resolution of that discrepancy;
- the analysis made and the decisions taken on whether to continue the test or to issue a change request, in the case where discrepancies occur.

15.2.7 ~~When discrepancies occur between expected and actual results,~~ The results shall be verified against the expected results. All discrepancies shall be analysed and the findings shall be available as part of the validation documentation. This shall include the analysis made and the decisions taken on whether to continue the validation or to issue a change request and to return to an earlier part of the development life-cycle.

15.2.8 After the SIS validation and prior to the identified hazards being present, the following activities shall be carried out:

- all bypass functions (e.g., PE logic solver and PE sensor forces, disabled alarms) shall be returned to their normal position;
- all process isolation valves shall be set according to the process start-up requirements and procedures;
- all test materials (e.g., fluids) shall be removed;
- all ~~forces shall be removed and if applicable all force enables~~ commissioning overrides and force permissives shall be removed.

16 SIS operation and maintenance

16.1 Objectives

The objectives of the requirements of Clause 16 are to ensure that:

- the required SIL of each SIF is maintained during operation and maintenance;
- the SIS is operated and maintained ~~so that the designed functional safety is maintained~~ in a way that sustains the required safety integrity.

16.2 Requirements

16.2.1 Operation and maintenance planning for the SIS shall be carried out. It shall provide the following:

- routine and abnormal operation activities;
- inspection, proof testing, preventive and breakdown maintenance activities;
- the procedures, measures and techniques to be used for operation and maintenance;
- the operational response to faults and failures identified by diagnostics, inspections or proof-tests;
- verification of ~~adherence~~ conformity to operations and maintenance procedures;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities;
- a SIS maintenance plan.

NOTE The SIS maintenance plan can state different maintenance features depending on the SIL level.

16.2.2 Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:

a) the routine ~~actions~~ methods and procedures which need to be carried out to maintain the "as designed" functional safety of the SIS~~, for example, adhering to proof-test intervals defined by the SIL determination~~;

b) the procedures used to ensure the quality and consistency of proof testing, and to ensure adequate validation is being performed after replacement of any device;

c) the ~~actions~~ measures and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (e.g., when a system needs to be bypassed for testing or maintenance, what additional ~~mitigation steps~~ risk reduction needs to be implemented);

d) the methods and procedures which are used to test the diagnostics;

e) the information which needs to be maintained on ~~system~~ SIS failure and the demand rates on the SIS;

f) procedures for collecting data related to the demand rate and SIS reliability parameters;

NOTE 1 Collection and analysis of failure data has many benefits including the potential to reduce maintenance costs if failures rates in operation are significantly lower than what were predicted during design. Implementation costs of new installations can also be reduced because new designs can be based on less conservative failure rates.

g) the information which needs to be maintained showing results of audits and tests on the SIS;

h) the maintenance procedures to be followed when faults or failures occur in the SIS, including:

- procedures for fault diagnostics and repair;
- procedures for revalidation;
- maintenance reporting requirements;
- procedures for tracking maintenance performance.

NOTE 2 Considerations include:

– procedures for reporting failures;

– procedures for analysing systematic failures;

– the actions to allow safe shutdown in the event of BPCS failure;

– ensuring that test equipment ~~used during normal maintenance activities~~ is properly calibrated and maintained.

16.2.3 Operation procedures shall be made available. Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.). The operator shall be provided with information on the procedures to be applied before and during bypass and what should be done before the removal of the bypass and the maximum time allowed to be in the bypass state. This information shall be reviewed on a regular basis.

NOTE The operating and maintenance procedures can include verification that bypasses are removed after proof testing.

16.2.4 Continued process operation with a SIS device in bypass shall only be permitted if a hazards analysis has determined that compensating measures are in place and that they provide adequate risk reduction. Operating procedures shall be developed accordingly.

16.2.5 Operation and maintenance shall proceed in accordance with the relevant procedures.

16.2.6 Operators shall be trained on the function and operation of the SIS in their area. This training shall ensure that they understand:

- how the SIS functions (trip points and the resulting action that is taken by the SIS);

NOTE 1 This can also include impact of an SIS action to remaining operational plant.

- the hazard the SIS is protecting against;
- the correct operation and management of all bypass/override switches and under what circumstances these bypasses are to be used;
- the operation of any manual shutdown switches and manual start-up activity and when these manual switches are to be activated;

NOTE 2 This ~~may~~ can include “system reset” and “system restart”.

- expectation on activation of any diagnostic alarms (e.g., what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS);
- the proper verification of the diagnostics.

16.2.7 The status of all bypasses shall be recorded in a bypass log. All bypasses need authorization and indication.

16.2.8 Maintenance personnel shall be trained as required to sustain full functional performance of the SIS (hardware and software) to ~~its targeted integrity~~ meet the target SIL of each SIF.

16.2.9 Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:

- the demand rate on each SIF (see 5.2.5.3);
- the actions taken following a demand on the system;
- the failures and failure modes of equipment forming part of the SIS ~~established during routine~~, including those identified during normal operation, inspection, testing or ~~actual~~ demand on a SIF;
- the cause of the demands;
- the cause and frequency of ~~false~~ spurious trips;
- the failure of equipment forming part of any compensating measures.

~~NOTE It is very important that ALL discrepancies between expected behaviour and actual behaviour are analysed. This should not be confused with monitoring demands encountered during normal operation.~~

16.2.10 The operation and maintenance procedures may require revision, if necessary, following:

- functional safety audits;
- tests on the SIS;
- experience from normal or abnormal operation and maintenance events.

16.2.11 Written proof-test procedures shall be developed for every SIF to reveal dangerous failures undetected by diagnostics. These written test procedures shall describe every step that is to be performed and shall include:

- the correct operation of each sensor and final element;
- correct logic action;
- correct alarms and indications.

NOTE The following methods ~~may~~ can be used to determine the undetected failures that need to be tested:

– examination of fault trees;
– failure mode and effect analysis;
– reliability centred maintenance.

16.2.12 SIS spare parts shall be identified and shall be made available to minimize the bypass duration due to unavailability of any replacement part for the SIS.

NOTE Replacements that are not in kind (like for like) can be managed as a modification to the SIS.

16.2.13 Persons responsible for operations and maintenance shall review the hazard and risk analysis, allocation and design to ensure the assumptions made are valid e.g. assumptions on occupancy and corrosion protection.

16.3 Proof testing and inspection

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure ~~(see 16.2.8)~~ to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.

NOTE 1 Particular attention can be made to identify failure causes that may lead to common cause failures.

NOTE 2 Functional test procedures can also emphasize the need to avoid introducing common cause failures.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).

NOTE Testing of the SIS can be performed either end-to-end or in segments (see 11.8.1).

16.3.1.3 The schedule for the proof tests shall be according to the SRS. The frequency of proof tests for a SIF shall be determined through PFD_{avg} or PFH calculation in accordance with 11.9 for the SIS as installed in the operating environment.

NOTE Different parts of the SIS ~~may~~ can require different test intervals, for example, the logic solver ~~may~~ can require a different test interval than the sensors or final elements.

16.3.1.4 Any deficiencies found during the proof testing shall be repaired in a safe and timely manner. A proof test shall be repeated after the repair is completed.

16.3.1.5 At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation~~, and software reliability~~.

NOTE The user can adjust the test frequency based on this data and an analysis of the original basis for test frequency.

16.3.1.6 Any change to the application ~~logic~~ program requires full validation and a proof test of any SIF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were ~~correctly implemented~~ designed per the updated safety requirements and correctly implemented.

16.3.1.7 Suitable management procedures shall be applied to review deferrals and prevent significant delay to proof testing.

16.3.2 Inspection

Each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (e.g., missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation).

NOTE These problems could indicate an increase in the frequency of faults.

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

a) description of the tests and inspections performed including identification of the test procedure used;

b) dates of the tests and inspections;

c) name of the person(s) who performed the tests and inspections;

d) serial number or other unique identifier of the system tested (e.g., loop number, tag number, equipment number, and SIF number);

e) results of the tests and inspection including the “as-found” condition, all faults found (including the failure mode) and the "as-left" condition.

17 SIS modification

17.1 Objectives

The objectives of the requirements of Clause 17 are:

- that modifications to any SIS are properly planned, reviewed, approved and documented prior to making the change;
- to ensure that the required safety integrity of the SIS is maintained despite of any changes made to the SIS.

NOTE Modifications to the BPCS, other equipment, process or operating conditions ~~should~~ can be reviewed to determine whether they are such that the nature or frequency of demands on the SIS will be affected. Those having an adverse effect ~~should~~ can be considered further to determine whether the level of risk reduction will still be sufficient.

17.2 Requirements

17.2.1 Prior to carrying out any modification to a SIS, procedures for authorizing and controlling changes shall be in place.

17.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and the hazards that may be affected.

17.2.3 Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification ~~will~~ could impact safety then there shall be a return to the first phase of the SIS safety life-cycle affected by the modification.

17.2.4 Safety planning for the modification and re-verification shall be available. Modifications and re-verifications shall be carried out in accordance with the planning.

17.2.5 All documentation affected by the modification shall be updated.

17.2.6 Modification activity shall not begin ~~without~~ until a FSA is completed in accordance with 5.2.6.1.9 and after proper authorisation.

17.2.7 Appropriate information shall be maintained for all changes to the SIS. The information shall include:

- a description of the modification or change;
- the reason for the change;
- identified hazards and SIFs which may be affected;
- an analysis of the impact of the modification activity on the SIS;
- all approvals required for the changes;
- tests used to verify that the change was properly implemented and the SIS performs as required;
- details of all SIS modification activities (e.g., a modification log);
- appropriate configuration history;
- tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.

17.2.8 Modification shall be performed with qualified personnel who have been properly trained. All affected and appropriate personnel should be notified of the change and trained with regard to the change.

18 SIS decommissioning

18.1 Objectives

The objectives of the requirements of Clause 18 are to ensure that:

- prior to decommissioning any SIS from active service, a proper review is conducted and required authorization is obtained;
- the required SIF(s) remain operational during decommissioning activities.

18.2 Requirements

18.2.1 Prior to carrying out any decommissioning of part or all of a SIS or SIF, procedures for authorizing and controlling changes shall be in place.

18.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and identifying the hazards that may be affected.

18.2.3 An analysis shall be carried out on the impact on functional safety as a result of the proposed decommissioning activity. The assessment shall include an update of the H&RA sufficient to determine ~~the the breadth and depth that subsequent safety life cycle phases shall need to be re-taken~~ the scope of impact to the SIS safety life cycle. The subsequent SIS safety life-cycle phases shall need to be re-evaluated. The assessment shall also consider:

- functional safety during the execution of the decommissioning activities;
- the impact of decommissioning the SIS on adjacent operating units and facility services.

18.2.4 The results of the impact analysis shall be used during safety planning to re-~~activate~~ implement the relevant requirements of the IEC 61511 series including re-verification and re-validation.

18.2.5 Decommissioning activities shall not begin without proper documentation and authorization.

19 Information and documentation requirements

19.1 Objectives

The objectives of the requirements of Clause 19 are to ensure that the necessary information is available and documented in order that:

- all phases of the SIS safety life-cycle can be effectively performed;
- ~~the necessary information is available and documented in order that~~ verification, validation and FSA activities can be effectively performed.

~~NOTE 1 For examples of documentation structure, see IEC 61508-1 Annex A and, for more details, IEC 61506.~~

~~NOTE 2 The documentation could be available in different forms (for example, on paper, film or any data medium to be presented on screens or displays).~~

19.2 Requirements

19.2.1 The documentation required by the IEC 61511 series shall be available to personnel implementing the requirements of the IEC 61511 series.

19.2.2 The documentation ~~should~~ shall:

- describe the installation, system or equipment and the use of it;
- be accurate and up to date;
- be easy to understand;
- suit the purpose for which it is intended;

- be available in an accessible, maintainable and editable form, so that appropriate and relevant documents can be readily and accurately identified, located, retrieved and revised.

NOTE Further details of the requirements for information are included in Clause 14 and Clause 15.

19.2.3 The documentation shall have unique identities so it shall be possible to reference the different parts.

19.2.4 The documentation shall have designations indicating the type of information.

19.2.5 The documentation shall be traceable to the functional and integrity requirements arising from this standard, including the H&RA.

19.2.6 The documentation shall have a revision index (for example, version numbers) to make it possible to identify different versions of the information.

19.2.7 The documentation shall be structured to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document.

NOTE The physical structure of the documentation ~~should~~ can vary depending upon a number of factors such as the size of the system, its complexity and the organizational requirements.

19.2.8 All relevant documentation shall be revised, amended, reviewed, approved and shall be under the control of an appropriate information control scheme.

19.2.9 Current documentation pertaining to the following shall be maintained:

a) the results of the H&RA and the related assumptions;

b) the equipment used for SIF together with its safety requirements;

c) the organization responsible for maintaining functional safety;

d) the procedures necessary to achieve and maintain functional safety of the SIS;

e) the modification information as defined in 17.2.5;

f) the safety manual(s);

g) design, implementation, test and validation.

NOTE Further details of the requirements for information are included in 12.4.2, Clauses 14 and 15 and in 16.3.3.

Bibliography

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at <http://www.electropedia.org/)

~~IEC 60050(191): 1990, *International Electrotechnical Vocabulary* http://www.electropedia.org/ *Chapter 191: Depend-ability and quality of service*~~

~~IEC 60050(351):1998, *International Electrotechnical Vocabulary – Part 351: Automatic control*~~

IEC 60300-3-2:2004, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60605-4:2001, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60617-12:1997, *Graphical symbols for diagrams – Part 12: Binary logic elements*[1]

IEC TS 61000-1-2:2008, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61131-3:~~1993~~ 2013, *Programmable controllers – Part 3: Programming language*

IEC 61131-6:2012, *Programmable controllers – Part 6: Functional Safety*

IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

~~IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General requirements*~~

IEC 61508-4:~~1998~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations*

IEC 61508-6:~~2000~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

IEC 61511-3:~~2003~~__, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443-2-1:2010, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

[1] Withdrawn.

IEC 62682:2014, *Management of alarms for the process industry*

ISO/IEC 2382 ~~(all parts)~~:2006, *Information technology – Vocabulary*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 90003:2014, *Software engineering – Part 3: Guidelines for the application of ISO 9001:2000 to computer software*

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

ISO 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

~~ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*~~

ISO 9000:~~2000~~ 2005, *Quality management systems – Fundamentals and vocabulary*

~~ISO 9000-3:1997, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software*~~

ISO 9001:2008, *Quality management systems – Requirements*

ISO TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

ISO 13849-1:2006, *Safety of machinery – Safety related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety related parts of control systems – Part 2: Validation*

ISO 14224:2006, *Petroleum, petrochemical and natural gas industries- Collection and exchange of reliability and maintenance of data for equipment*

ISA TR 84.00.04 Part 1:2015, *Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

ISA TR 84.00.09:2013, *Security Countermeasures Related to Safety Instrumented Systems (SIS)*

_____

IEC 61511-1

Edition 2.0 2016-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Sécurite fonctionnelle – Systèmes instrumentes de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

IEC 61511-1:2016-02(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 1: Framework, definitions, system, hardware and 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.

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.

INTRODUCTION

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

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

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

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

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

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

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

The IEC 61511 series on SIS for the process industry:

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

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

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

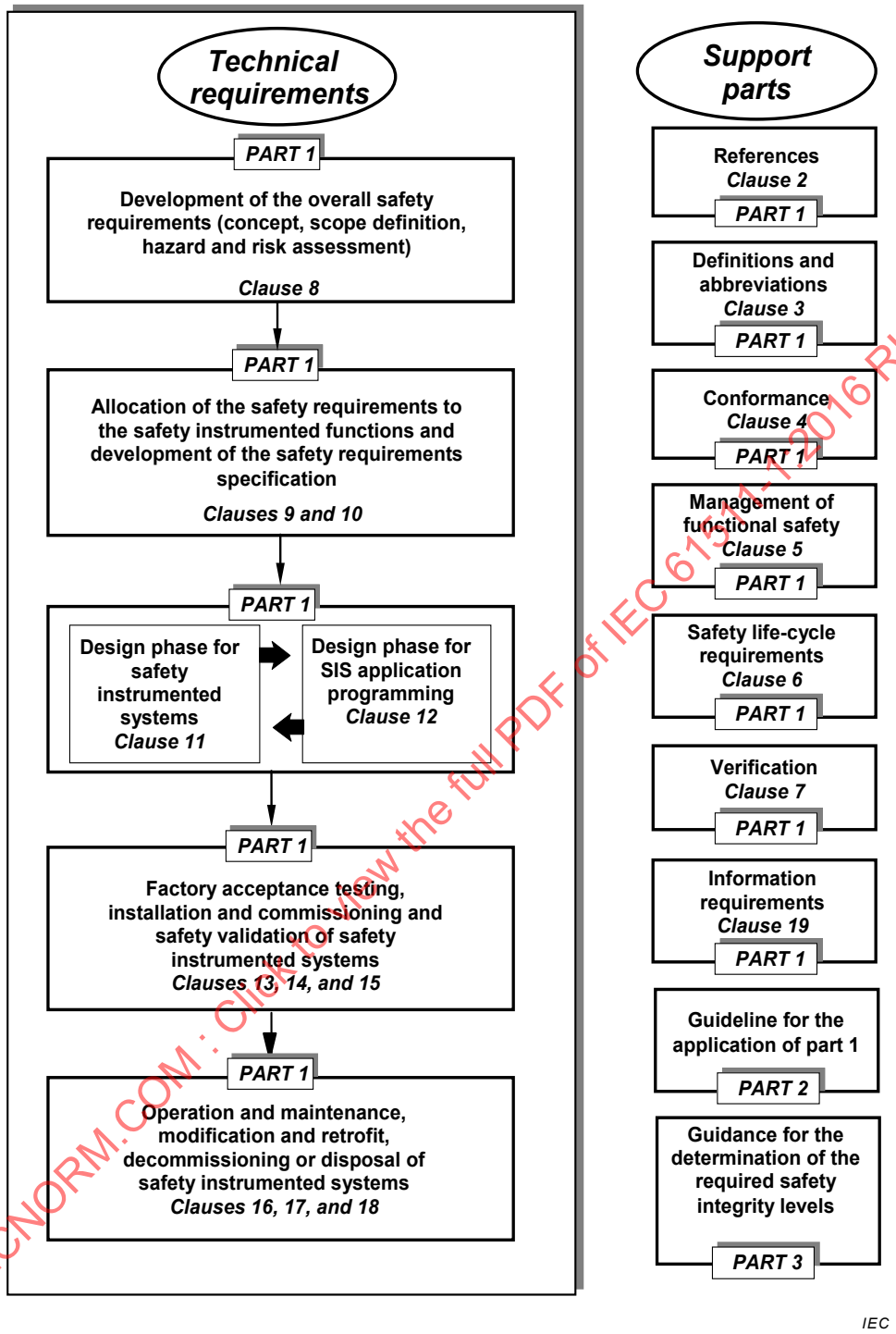


Figure 1 – Overall framework of the IEC 61511 series

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

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

1 Scope

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

In particular, IEC 61511-1:

a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (e.g., designers, suppliers, owner/operating company, contractor). This responsibility will be assigned to different parties according to safety planning, project planning and management, and national regulations;

b) applies when devices that meets the requirements of the IEC 61508 series published in 2010, or IEC 61511-1:2016 [11.5], is integrated into an overall system that is to be used for a process sector application. It does not apply to manufacturers wishing to claim that devices are suitable for use in SISs for the process sector (see IEC 61508-2:2010 and IEC 61508-3:2010);

c) defines the relationship between IEC 61511 and IEC 61508 (see Figures 2 and 3);

d) applies when application programs are developed for systems having limited variability language or when using fixed programming language devices, but does not apply to manufacturers, SIS designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3:2010);

e) applies to a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;

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

f) outlines the relationship between SIFs and other instrumented functions (see Figure 4);

g) results in the identification of the functional requirements and safety integrity requirements for the SIF taking into account the risk reduction achieved by other methods;

h) specifies life-cycle requirements for system architecture and hardware configuration, application programming, and system integration;

i) specifies requirements for application programming for users and integrators of SISs.

j) applies when functional safety is achieved using one or more SIFs for the protection of personnel, protection of the general public or protection of the environment;

k) may be applied in non-safety applications for example asset protection;

l) defines requirements for implementing SIFs as a part of the overall arrangements for achieving functional safety;

m) uses a SIS safety life-cycle (see Figure 7) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the SIS;

n) specifies that a H&RA is to be carried out to define the safety functional requirements and safety integrity levels (SIL) of each SIF;

NOTE 2 Figure 9 presents an overview of risk reduction means.

o) establishes numerical targets for average probability of failure on demand (in demand mode) and average frequency of dangerous failures (in demand mode or continuous mode) for each SIL;

p) specifies minimum requirements for hardware fault tolerance (HFT);

q) specifies measures and techniques required for achieving the specified SIL;

r) defines a maximum level of functional safety performance (SIL 4) which can be achieved for a SIF implemented according to IEC 61511-1;

s) defines a minimum level of functional safety performance (SIL 1) below which IEC 61511-1 does not apply;

t) provides a framework for establishing the SIL but does not specify the SIL required for specific applications (which should be established based on knowledge of the particular application and on the overall targeted risk reduction);

u) specifies requirements for all parts of the SIS from sensor to final element(s);

v) defines the information that is needed during the SIS safety life-cycle;

w) specifies that the design of the SIS takes into account human factors;

x) does not place any direct requirements on the individual operator or maintenance person:

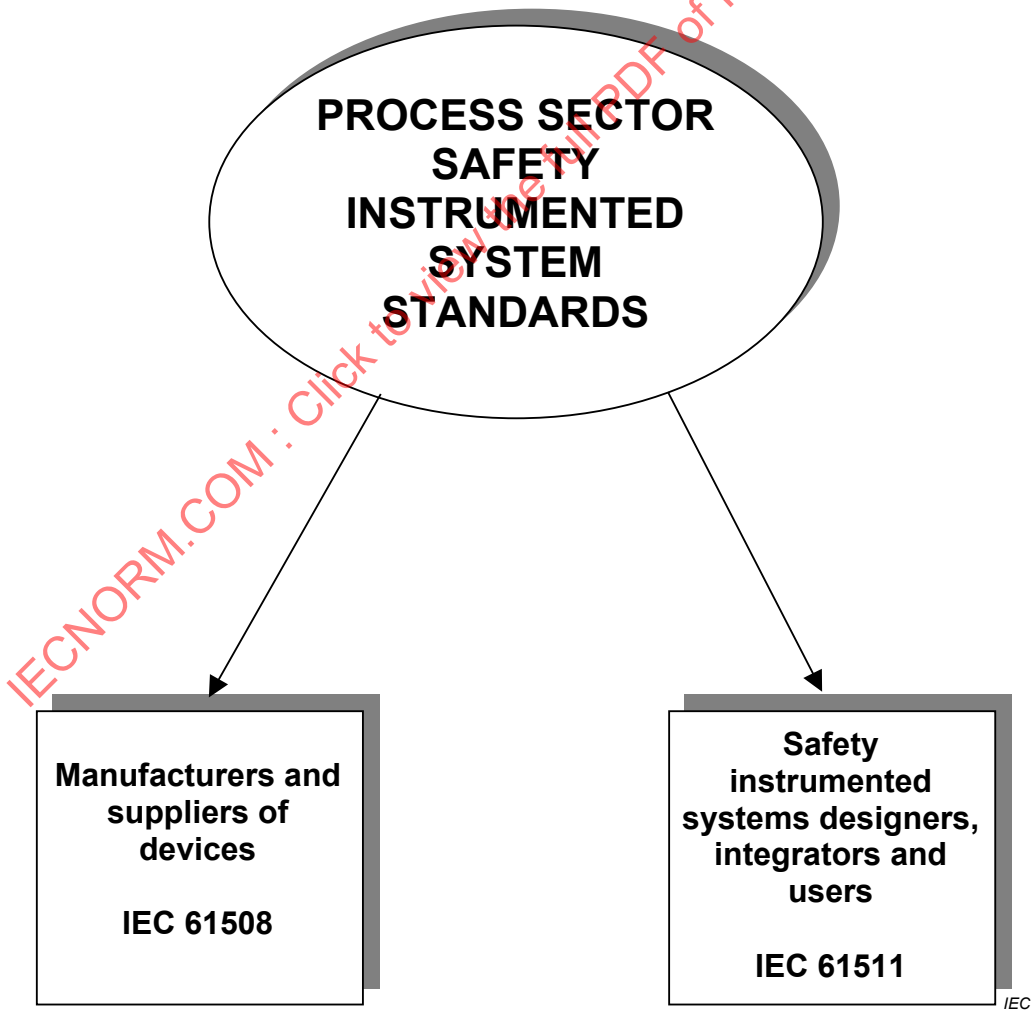


Figure 2 – Relationship between IEC 61511 and IEC 61508

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

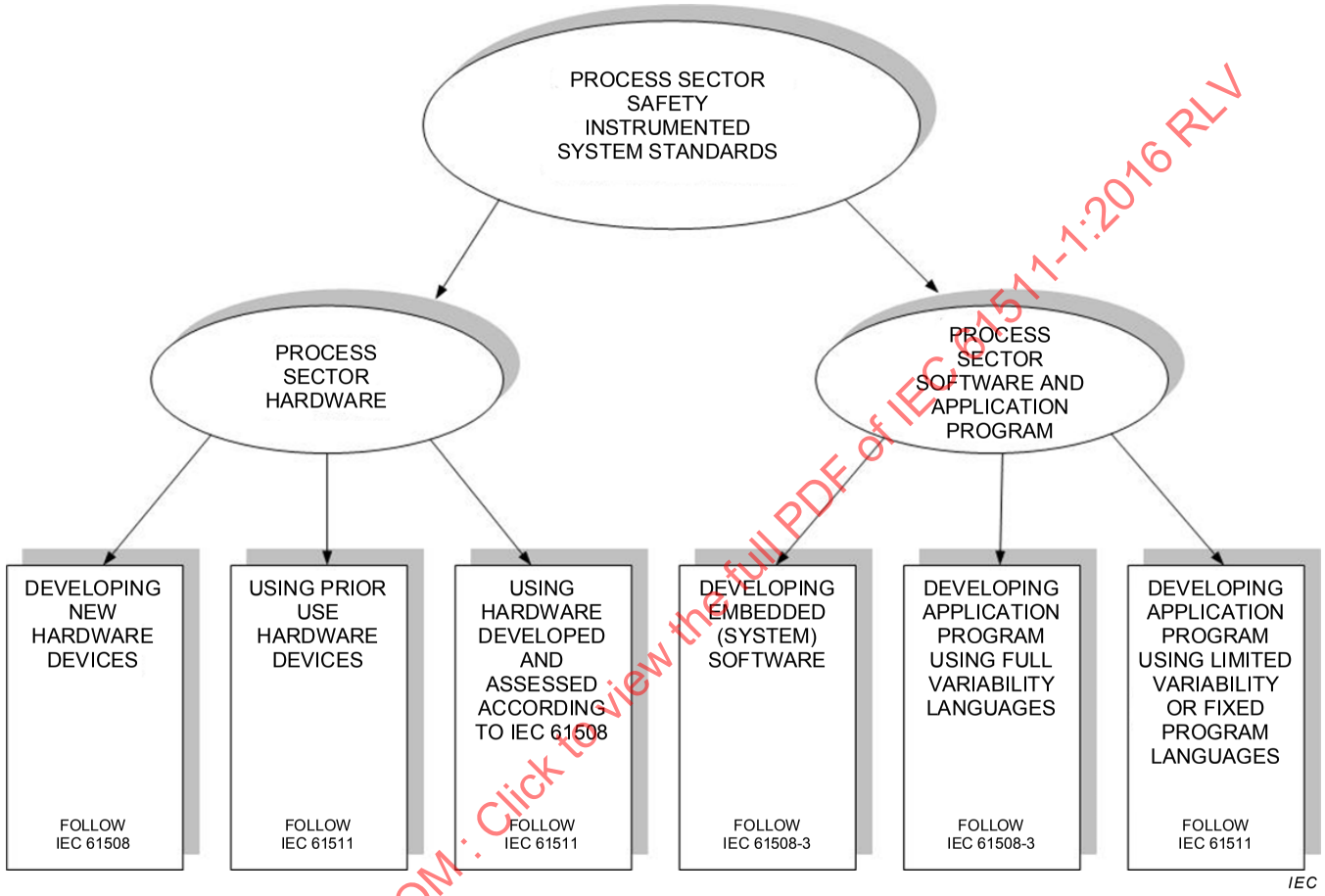


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

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.).

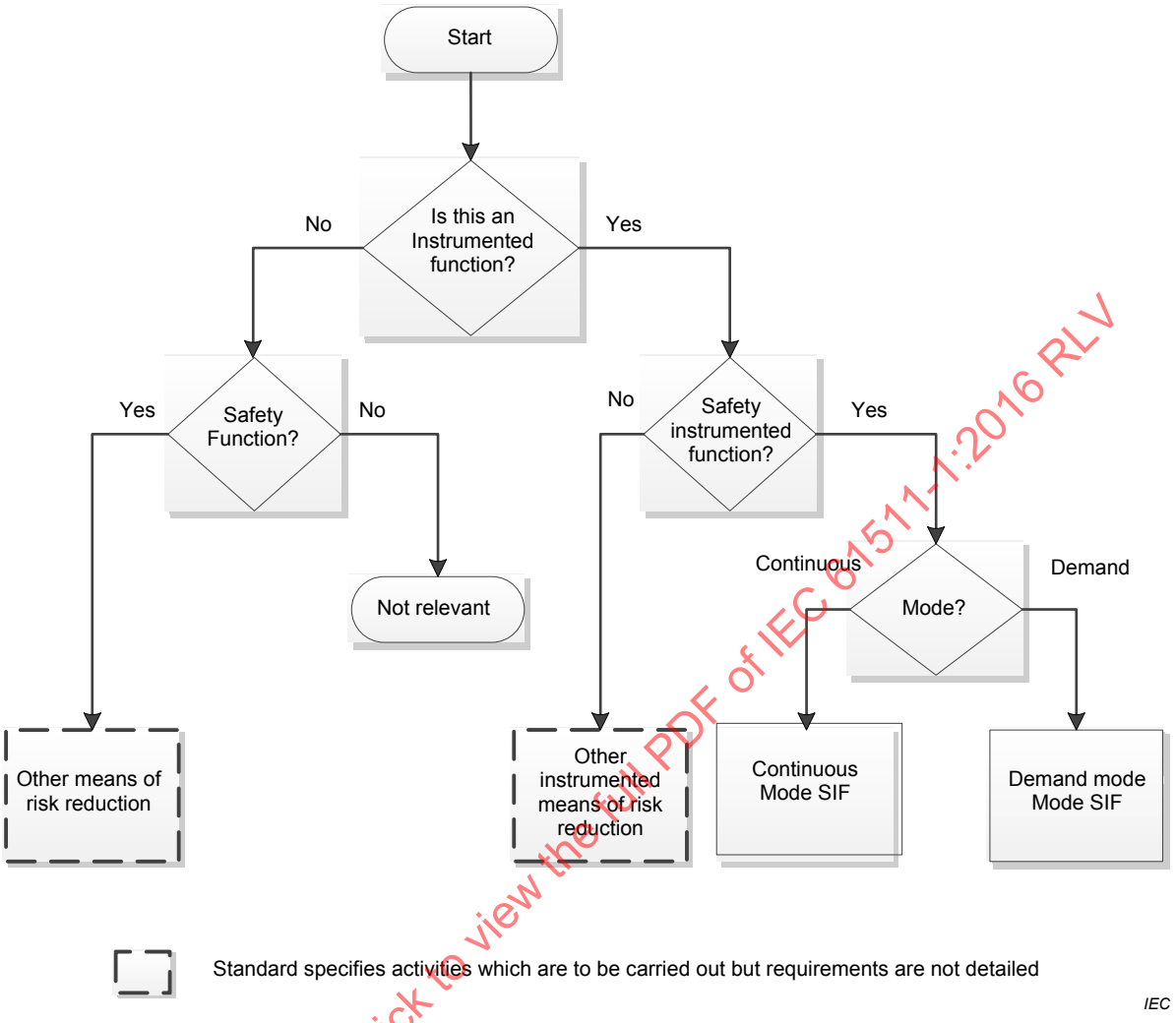


Figure 4 – Relationship between safety instrumented functions and other functions

2 Normative references

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

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

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

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

3 Terms, definitions and abbreviations

3.1 Terms

Terms are listed alphabetically in 3.2.

3.2 Terms and definitions

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

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

3.2.1
architecture
configuration
specific configuration of hardware and software components in a system

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

3.2.2
asset protection
function allocated to a system and designed for the purpose of preventing loss or damage to assets

3.2.3
basic process control system
BPCS
system which responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any SIF

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

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

3.2.4
bypass
action or facility to prevent all or parts of the SIS functionality from being executed

Note 1 to entry: Examples of bypassing include:

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

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

3.2.5
channel
device or group of devices that independently perform(s) a specified function

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

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

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

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

3.2.6
common cause

3.2.6.1
common cause failures, pl
concurrent failures of different devices, resulting from a single event, where these failures are not consequences of each other

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

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

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

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

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

3.2.6.2
common mode failures, pl
concurrent failures of different devices characterized by the same failure mode (i.e., identical faults)

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

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

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

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

3.2.7
compensating measure
temporary implementation of planned and documented methods for managing risks during any period of maintenance or process operation when it is known that the performance of the SIS is degraded

3.2.8
component
one of the parts of a system, SIS subsystem, or device performing a specified function

Note 1 to entry: Component may also include software.

3.2.9
configuration management
discipline of identifying the components and the arrangements of those components of an evolving system for the purposes of controlling changes to those components, and maintaining continuity of the system and traceability of any changes throughout the life-cycle

3.2.9.1
conservative approach
cautious way of doing analysis and calculations

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

3.2.10
control system
system which responds to input signals from the process and/or from an operator and generates output signals causing the process to operate in the desired manner

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

3.2.11
dangerous failure
failure which impedes or disables a given safety action

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

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

– a degraded SIF where the safety action is available but there is either a higher PFD (demand mode of operation) or a higher likelihood of initiating an 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 if the probability of occurrence of A and B, P(A and B), is greater than P(A) × P(B).

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

Note 3 to entry: Dependent failures include common cause.

3.2.13
detected
revealed
overt
relating to hardware and software failures or faults which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods

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

– Overt is used for failures or faults which announce themselves when they occur (e.g., due to the change of state). The repair of such failures can begin as soon as they have occurred.

– Detected is used for failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, operator intervention like physical inspection and manual tests). The repair of such failures can begin only after they have been revealed. See Note 2 for the specific use of this term in IEC 61511.

– Revealed is used for failures or faults that become evident due to being overt or as a result of being detected.

Note 2 to entry: 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
hardware, with or without software, capable of performing a specified function

Note 1 to entry: Examples are sensors, logic solvers, final elements, operator interfaces, 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
fraction of dangerous failures rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof tests

Note 1 to entry: Diagnostics coverage is typically applied to 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 dangerous failures of SIS devices or SIS subsystems. For example, the diagnostics coverage for the dangerous failures of a device is DC = $\lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate. For a SIS subsystem with internal redundancy, DC is time dependant: $DC(t) = \lambda_{DD}(t)/\lambda_{DT}(t)$.

Note 3 to entry: When the 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:

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

3.2.16
diversity
different means of performing a required function

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

3.2.17
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

3.2.18
failure
loss of ability to perform as required

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

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

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

Note 4 to entry: Failures are either random or systematic (see 3.2.61 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
inability to perform as required, due to an internal state

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

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

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

3.2.20
fault avoidance
use of techniques and procedures which aim to avoid the introduction of faults during any phase of the SIS safety life-cycle

3.2.20.1
fault exclusion
elimination from further consideration of faults due to improbable failure modes

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

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

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

3.2.21
fault tolerance
ability of a functional item to continue to perform a required function in the presence of faults or errors

3.2.22
final element
part of the BPCS or SIS that implements the physical action necessary to achieve or maintain a safe state

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

3.2.23
functional safety
part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers

3.2.24
functional safety assessment
FSA
investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers

3.2.25
functional safety audit
systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

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

3.2.26
hardware safety integrity
part of the safety integrity of the SIS relating to random hardware failures in a dangerous mode of failure

Note 1 to entry: The two failure measures that are relevant in this context are the average frequency of dangerous failure (continuous mode of operation) and the average probability of failure 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
injury or damage to the health of people, or damage to property or to the environment

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

3.2.27.1
harmful event
hazardous event which has caused harm

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

3.2.28
hazard
potential source of harm

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

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

3.2.28.1
hazardous event
event that can cause harm

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

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

3.2.28.2
hazardous situation
circumstance in which people, property or the environment are exposed to one or more hazards

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

3.2.29
human error
intended or unintended human action or inaction that produces an inappropriate result

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

Note 2 to entry: This excludes malicious action.

3.2.30
impact analysis
activity of determining the effect that a change to a function or component will have to other functions or components in the system as well as in other systems

3.2.31
independent organization
organization that is separate and distinct, by management and other resources, from the organizations responsible for the activities that take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation

3.2.32
independent person
person who is separate and distinct from the activities which take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation and does not have direct responsibility for those activities

3.2.33
input function
function which monitors the process and its associated equipment in order to provide input information for the logic solver

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

3.2.34
instrument
apparatus used in performing an action (typically found in instrumented systems)

3.2.34.1
instrumented system
system composed of sensors (e.g., pressure, flow, temperature transmitters), logic solvers (e.g., programmable controllers, distributed control systems, discrete controllers), and final elements (e.g., control valves, motor control circuits)

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

3.2.35
logic function
function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions)

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

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

3.2.36
logic solver
part of either a BPCS or SIS that performs one or more logic function(s)

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

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

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

3.2.36.1
safety configured PE logic solver
general purpose industrial grade PE logic solver which is specifically configured for use in safety applications

Note 1 to entry: Further guidance can be found in 11.5.

3.2.37
maintenance/engineering interface
hardware and software provided to allow proper SIS maintenance or modification

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

3.2.37.1
mean repair time
MRT
expected overall repair time

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

3.2.37.2
mean time to restoration
MTTR
expected time to achieve restoration

Note 1 to entry: MTTR encompasses:

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

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

3.2.37.3
maximum permitted repair time
MPRT
maximum duration allowed to repair a fault after it has been detected

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

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

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

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

3.2.38
mitigation
action that reduces the consequence(s) of a hazardous event

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

3.2.39
mode of operation (of a SIF)
way in which a SIF operates which may be either low demand mode, high demand mode or continuous mode

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

b) **high demand mode:** mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year.

c) **continuous mode:** mode of operation where the SIF retains the process in a safe state as part of normal operation.

3.2.39.1
demand mode SIF
SIF operating in low demand mode (3.2.39 a)) or high demand mode (3.2.39 b))

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

– if the failure is undetected and a demand occurs before the next proof test;

– if the failure is detected by the diagnostic tests but the related process and its associated equipment has not been moved to a safe state before a demand occurs.

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

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

3.2.39.2
continuous mode SIF
SIF operating in continuous mode (3.2.39 c))

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

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

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

3.2.40
module
self-contained part of a SIS application program (can be internal to a program or a set of programs) that performs a specified function (e.g., final element start/stop/test sequence, an application specific sequence within a SIF)

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

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

3.2.41
MooN
SIS, or part thereof, made up of "N" independent channels, which are so connected, that "M" channels are sufficient to perform the SIF

3.2.42
necessary risk reduction
risk reduction to be achieved by the SIS(s) and/or other protection layers to ensure that the tolerable risk is not exceeded

3.2.43
non-programmable system
(NP) system
system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software)

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

3.2.44
operating environment
conditions inherent to the installation of a device that potentially affects its functionality and safety integrity, such as:

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

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

3.2.45
operating mode
process operating mode
any planned state of process operation, including modes such as start-up after emergency shutdown, normal start-up, operation, and shutdown, temporary operations, and emergency operation and shutdown

3.2.46
operator interface
means by which information is communicated between a human operator and the SIS (e.g., display interfaces, indicating lights, push-buttons, horns, alarms)

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

3.2.47
output function
function which controls the process and its associated equipment according to output information from the logic function

3.2.48
performance
accomplishment of a given action or task measured against the specification and the IEC 61511 series

3.2.49
phase
period within the SIS safety life-cycle where activities described in the IEC 61511 series take place

3.2.50
prevention
action that reduces the likelihood of occurrence of a hazardous event

3.2.51
prior use
documented assessment by a user that a device is suitable for use in a SIS and can meet the required functional and safety integrity requirements, based on previous operating experience in similar operating environments

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

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

3.2.52
process risk
risk arising from the process conditions caused by abnormal events (including BPCS malfunction)

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

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

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

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

3.2.52.1
process safety time
time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed

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

3.2.53
programmable electronics
PE
item based on computer technology which may be comprised of hardware, software, and of input and/or output units

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

– smart sensors and final elements;

– programmable electronic logic solvers including:

– programmable controllers;
– programmable logic controllers;
– loop controllers.

3.2.54
programmable electronic system
PES
system for control, protection or monitoring based on one or more programmable electronic devices, including all 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)

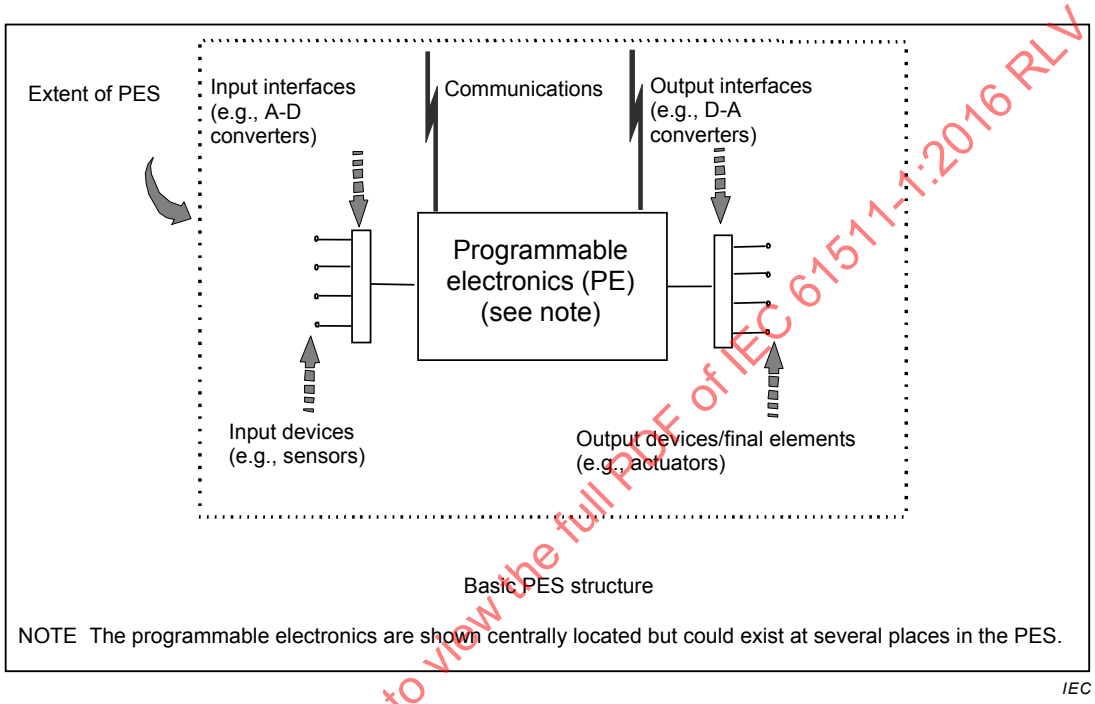


Figure 5 – Programmable electronic system (PES): structure and terminology

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 detect dangerous hidden faults in a SIS so that, if necessary, a repair can 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 can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical 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).

3.2.58
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 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: 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
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 devices and the addition of parity bits.

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

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

3.2.61
risk
combination of the probability of occurrence of harm and the severity of that harm

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 favours a given safety action

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.

3.2.63
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 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 risk which is not tolerable

Note 1 to entry: 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 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

3.2.66
safety instrumented function
SIF
safety 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

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

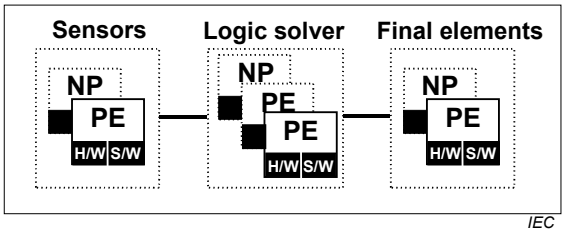


Figure 6 – Example of SIS architectures comprising three SIS subsystems

3.2.68
safety integrity
ability of the SIS to perform the required SIF as and when required

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 random hardware and systematic failures which lead to an unsafe state 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 frequency or the probability of failure on demand. However, safety integrity also depends on many systematic factors, which cannot be accurately quantified 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 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, pl
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 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
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, 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 and their associated safety integrity levels

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

3.2.73
sensor
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.

3.2.74
software
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 to entry: For examples of different types of software, see 3.2.75 and 3.2.76.

3.2.75
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

Note 1 to entry: Typical examples of device applications with FPL are: smart sensor (e.g., pressure transmitter without control algorithms), smart final element (e.g. valve without control algorithms), sequence of events recorder, 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 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 program
program specific to the user application containing, in general, logic sequences, permissives, limits and expressions that control the input, output, calculations, and decisions necessary to meet the SIS functional requirements

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
application program life-cycle
activities occurring during a period of time that starts when the application program is conceived and ends when the application program is permanently disused

Note 1 to entry: An 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.

3.2.78
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 devices, which interact according to a specification

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

Note 2 to entry: This definition deviates from the definition in IEC 61508 to reflect differences in process sector terminology.

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 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 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 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 include human error that originates in:

– the SRS;
– the design, manufacture, installation, operation or maintenance of the hardware;
– the design 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 SIS relating to systematic failures 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
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 relationship between the target failure measures and the SIL are given in Tables 4 and 5.

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
not detected or not revealed or not overt

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
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 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
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
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
LVL	Limited variability language
MooN	"M" out of "N" 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
pl	Plural
PLC	Programmable logic controller
SAT	Site acceptance test
SC	Systematic capability
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification

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

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

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.

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.

The following items 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 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) 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 reliability parameters of the SIS are in accordance with those assumed during the design;
- define the necessary corrective action to be taken if the failure rates are greater than what was assumed during design;

- compare the demand rate on the SIF during actual operation 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 a FSA team be appointed which includes the technical, application and operations expertise needed for the particular application.

5.2.6.1.2 The membership of the 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).

5.2.6.1.3 The following 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 methods by which the FSA will be revalidated after modifications.

NOTE When the FSA team is large, consideration 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 can be introduced as new hazards are identified, after modification and at periodic intervals during operation.

NOTE 2 Consideration 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 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 Prior to the hazards being present 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 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 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 can be addressed will depend upon their impact on the 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 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 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 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 Procedures for configuration management of the SIS during any SIS safety life-cycle phase shall be available.

NOTE In particular, the following can be specified:

– the stage at which formal configuration management is to be implemented;

– the procedures to be used for uniquely identifying all components of a SIS or SIS-subsystem (e.g., devices, application programming);

– the procedures for preventing unauthorized 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 meets the safety requirements.

NOTE 1 The overall approach of the IEC 61511 series is shown in Figure 7. It 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.

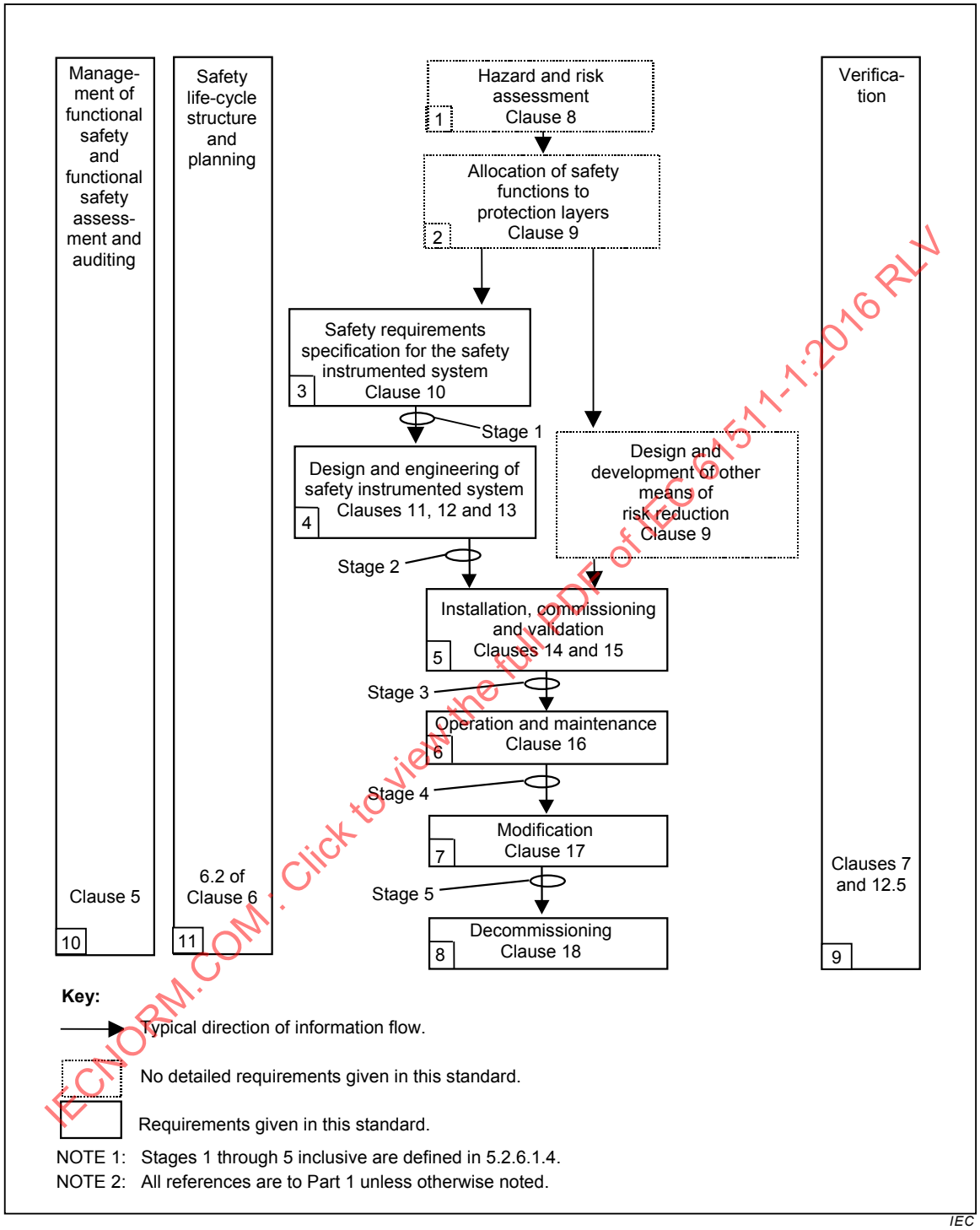


Figure 7 – SIS safety life-cycle phases and FSA stages

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	Require-ments 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
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	SIS safety requirements; 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 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 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 safety requirements. Results of SIS integration tests Results of the installation, com-missioning and validation activities

Table 2 *(2 of 2)*

Safety life-cycle phase or activity		Objectives	Require-ments 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	Decommission-ing	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).

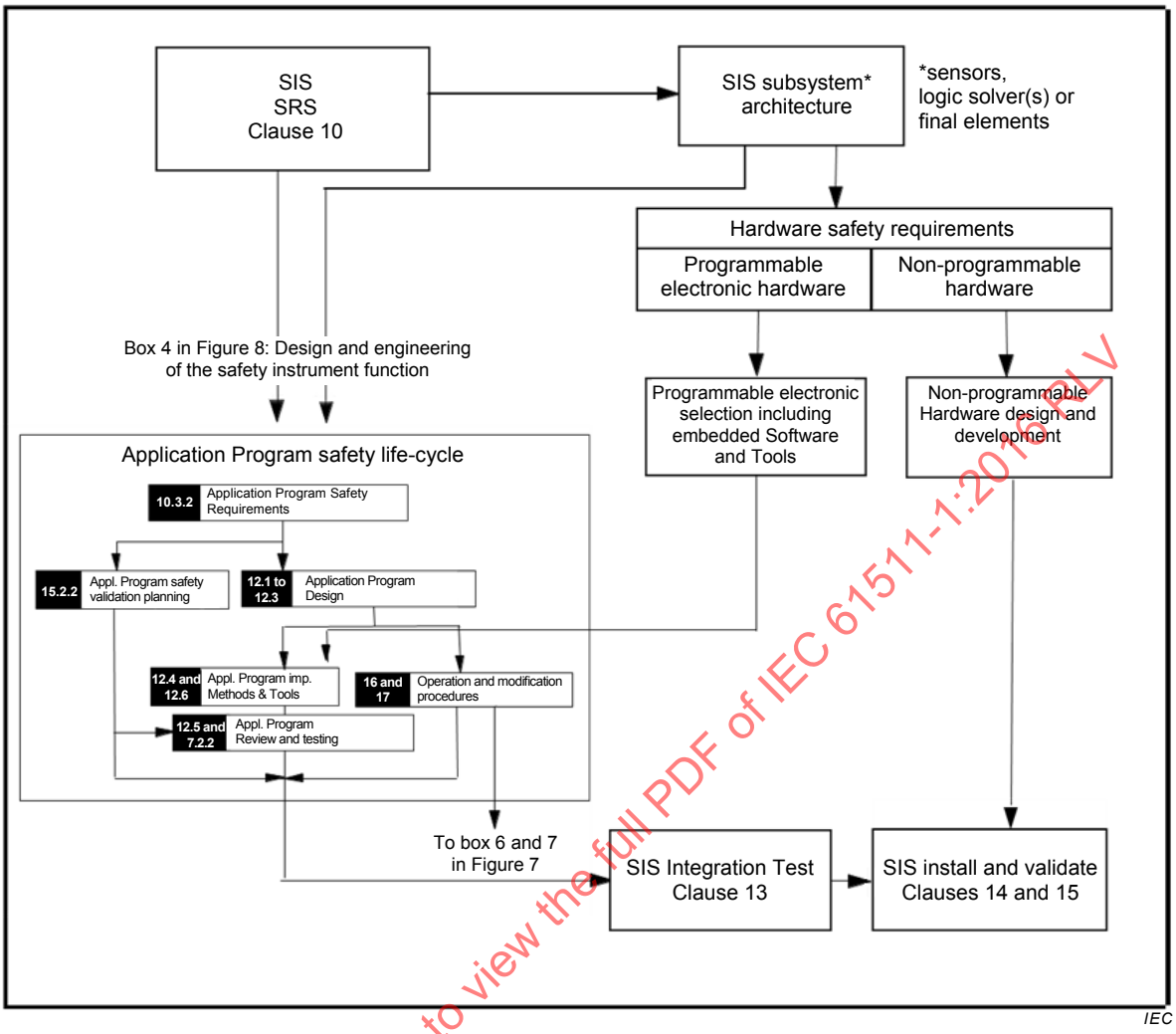


Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle

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

Safety life-cycle phase		Objectives	Require-ments Clause	Inputs	Outputs
Figure 8 box number	Title				
10.3.2	Application program safety requirements	To specify application program safety requirements for each SIS necessary to implement the required SIF. To specify the requirements for application program for each SIF allocated to that SIS.	10.3 11.5	SIS safety requirements. Safety manuals of the selected SIS. SIS architecture.	SIS application program safety requirements specification. Verification information.
15.2.2	Application program safety validation planning	To develop a plan for validating the application program.	15.2.2, 15.2.5	SIS application program safety requirements.	SIS safety validation planning. Verification information.
12.1 to 12.3	Application program development	Architecture. To create an application program architecture that fulfils the specified requirements for application program safety. To review and evaluate the requirements placed on the application program by the hardware architecture of the SIS. To specify the procedures for the development of the application program.	12.1 (also 10.3, 12.2)	SIS application program safety requirements. SIS hardware architecture design constraints.	Description of the architecture design, e.g., segregation of application program into related process sub-system and SIL, e.g., recognition of common application program modules such as pump or valve sequences. Application program architecture and sub-system integration test requirements. Verification information.
	Application program design	To develop the application program design. To identify a suitable set of configuration, library, management, and simulation and test tools, over the safety life-cycle of the application program.	12.3	SIS application program safety requirements. Description of the architecture design. Manuals of the SIS. Safety Manual of the selected SIS logic solver.	Application program design. Procedures for use during programming. Description of the standard (manufacturers) library functions to be used. Verification information.

Table 3 *(2 of 2)*

Safety life-cycle phase		Objectives	Require-ments Clause	Inputs	Outputs
Figure 8 box number	Title				
12.4 12.6	Application program implementation	Application development and application module development. To implement the application program that fulfils the specified requirements for application safety. To use appropriate support tools and programming languages.	12.4 12.3.4 12.6	Description of the design. List of manuals and procedures of the selected logic solver for use with the application program.	Application program (e.g., function block diagrams, ladder logic). Application program simulation and integration test. Special purpose application program safety requirements. Verification information.
12.5 7.2.2	Application program verification	To verify that the requirements for application program safety have been achieved. To show that all SIS application programs interact correctly to perform their intended functions and do not perform unintended functions.	12.5 7.2.2	Application program simulation and integration test requirements (structure based testing). Application program architecture integration test requirements.	Application program test results. Verified and tested application program system. Verification information.
13	SIS integration test	To integrate the application program onto the target logic solver, including interaction with a sample set of field devices and or simulator.	Clause 13	Application program and logic solver integration test requirements.	Application program and logic solver integration test results.

6.3.2 Methods, techniques and tools shall be applied for each life-cycle phase in accordance with 12.6.2.

6.3.3 Each phase of the SIS safety life-cycle for which safety planning has been carried out shall be verified (see Clause 7) and the results shall be available as described in Clause 19.

7 Verification

7.1 Objective

The objective of Clause 7 is to demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases (Figure 7) as identified by the verification planning.

7.2 Requirements

7.2.1 Verification planning shall be carried out throughout the SIS safety life-cycle and shall define all activities required for the appropriate phase (Figure 7) of the safety life-cycle, including the application program. Verification planning shall conform to the IEC 61511 series by addressing the following:

- the verification activities;

- the procedures, measures and techniques to be used for verification including implementation and resolution of resulting recommendations;
- when these activities will take place;
- the persons, departments and organizations responsible for these activities, including levels of independence;
- identification of items to be verified;
- identification of the information against which the verification is carried out;
- the adequacy of the outputs against the requirements for that phase;
- correctness of the data;
- how to handle non-conformances;
- tools and supporting analysis;
- the completeness of the SIS implementation and the traceability of the requirements;
- the readability and audit-ability of the documentation;
- the testability of the design.

7.2.2 Where the verification includes testing, the verification planning shall also address the following:

- the strategy for integration of application program and hardware and field devices, including the integration of sub-systems that shall comply with other standards (such as machinery or burner);
- test scope (describes the test set-up and what type of test to be performed including the hardware, application programming, and programming devices to be included);
- test cases and test data (these will be specific scenarios with the associated data);
- types of tests to be performed;
- test environment including tools, hardware, all software and required configuration;
- test criteria (e.g., pass/fail criteria) on which the results of the test will be evaluated;
- procedures for corrective action on failure during test;
- physical location(s) (e.g., factory or site);
- dependence on external functionality;
- appropriate personnel;
- management of change;
- non-conformances.

7.2.3 Non-safety functions integrated with safety functions shall be verified for non-interference with the safety functions.

7.2.4 Verification shall be performed according to the verification planning.

7.2.5 During testing, any modification shall be subjected to an impact analysis which shall determine all SIS components impacted and the necessary re-verification activities.

7.2.6 The results of the verification process shall be available (see Clause 19), including whether the objective and criteria of the tests have been met.

NOTE 1 Selection of techniques and measures for the verification process and the degree of independence depends upon a number of factors including degree of complexity, novelty of design, novelty of technology and required SIL.

NOTE 2 Examples of some verification activities include design reviews, use of tools and techniques including software verification tools and computer based design analysis tools.

8 Process H&RA

8.1 Objectives

The objectives of the requirements of Clause 8 are 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;
- any requirements for risk reduction;
- the safety functions required to achieve the necessary risk reduction;
- if any of the safety functions are SIFs.

NOTE 1 Clause 8 addresses process engineers, hazard and risk specialists, safety managers as well as instrument engineers. Its purpose is to recognize the multi-disciplinary approach typically required for the determination of SIF.

NOTE 2 Where reasonably practicable, processes can be designed to be inherently safe. When this is not practicable, other layers of protection (see Figure 9) can be required. In some applications, industry standards can specify the use of particular protection layers.

NOTE 3 The risk reduction can be accomplished using several layers of protection and the layers can be independent, sufficient, dependable and auditable.

8.2 Requirements

8.2.1 A H&RA shall be carried out on the materials, process and equipment. It shall result in:

- a description of each identified hazardous event and the factors that contribute to it;
- a description of the likelihood and consequence of each hazardous event;
- consideration of process operating modes such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown;
- the determination of additional risk reduction necessary to achieve the required functional safety;
- a description of, or references to information on, the measures taken to reduce or remove hazards and risk;
- a detailed description of the assumptions made during the analysis of the risks including demand rates on the protection layers and the average frequency of dangerous failures of the initiating sources, and of any credit taken for operational constraints or human intervention;
- identification of those safety function(s) applied as SIF(s).

NOTE 1 In determining the safety integrity requirements, account can be taken of the effects of common cause between systems that create demands and the protection layers that are designed to respond to those demands. An example of this would be where demands can arise through BPCS failure and the equipment used within the protective layers is similar or identical to the equipment used within the BPCS. In such cases, a demand caused by a failure of BPCS equipment may not be responded to effectively if a common cause has rendered similar equipment in the protection layer to be ineffective. It may not be possible to recognize common cause problems during the initial hazard identification and risk analysis because at such an early stage the design of the protection layers will not necessarily have been completed. In such cases, it can be necessary to reconsider the safety integrity requirements and SIF once the design of the SIS and other protection layers has been completed. In determining whether the overall design of process and protection layers meets requirements, common cause failures will be considered.

NOTE 2 Examples of techniques that can be used to establish the required SILs of SIFs are illustrated in IEC 61511-3:2016.

8.2.2 The average frequency of dangerous failures of a BPCS as an initiating source shall not be assumed to be $<10^{-5}$ per hour.

8.2.3 The H&RA shall be recorded in such a way that the relationship between the above items is clear and traceable.

NOTE 1 The above requirements do not mandate that the safety integrity requirements have to be assigned as numerical values. Qualitative or semi-quantitative approaches (see IEC 61511-3:2016, Annexes C, D & E) can also be used.

NOTE 2 The safety integrity requirements vary depending on the application and national legal requirements. An accepted principle in many countries is that additional risk reduction measures can be applied until the cost incurred becomes disproportionate to the improvement in safety integrity achieved.

8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction;
- a description of, or references to information on, the measures taken to reduce or remove the threats.

NOTE 1 Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

NOTE 2 The information and control of boundary conditions needed for the security risk assessment are typically with owner/operating company of a facility, not with the supplier. Where this is the case, the obligation to comply with 8.2.4 can be with the owner/operating company of the facility.

NOTE 3 The SIS security risk assessment can be included in an overall process automation security risk assessment.

NOTE 4 The SIS security risk assessment can range in focus from an individual SIF to all SISs within a company.

9 Allocation of safety functions to protection layers

9.1 Objectives

The objectives of the requirements of Clause 9 are to

- allocate safety functions to protection layers;
- determine the required SIFs;
- determine for each SIF the associated safety integrity requirements.

NOTE 1 Account can be taken, during the process of allocation, of other industry standards or codes.

NOTE 2 The integrity requirements for each SIF might include the associated risk reduction, PFD, PFH or SIL.

9.2 Requirements of the allocation process

9.2.1 The allocation process shall result in

- the allocation of safety functions required to achieve the necessary risk reduction to specific protection layers;
- the allocation of risk reduction or average frequency of dangerous failure to each SIF.

NOTE Legislative requirements or other industry codes may influence the allocation process.

9.2.2 The required SIL shall be derived taking into account the required PFD or PFH that is to be provided by the SIF.

NOTE Further guidance can be found in IEC 61511-3:2016.

9.2.3 For each SIF operating in demand mode, the required SIL shall be specified in accordance with either Table 4 or Table 5.

9.2.4 For each SIF operating in continuous mode, the required SIL shall be specified in accordance with Table 5.

Table 4 – Safety integrity requirements: PFD_{avg}

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**PFD_{avg}**	**Required risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	> 1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	**Average frequency of dangerous failures (failures per hour)**
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE 1 Further explanation of modes of operation can be found in 3.2.39.

NOTE 2 The SIL is defined numerically so as to provide an objective measure for comparison of alternate designs and solutions. However, it is recognized that, given the current state of knowledge, many systematic causes of failure can only be assessed qualitatively.

NOTE 3 The required average frequency of dangerous failures for a continuous mode SIF is determined by considering the risk caused by failure of the continuous mode SIF together with the failures of other devices that lead to the same risk, taking into consideration the risk reduction provided by other protection layers.

9.2.5 In cases where the allocation process results in a risk reduction requirement of >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour for a single SIS or multiple SISs or SIS in conjunction with a BPCS protection layer, there shall be a reconsideration of the application (e.g., process, other protection layers) to determine if any of the risk parameters can be modified so that the risk reduction requirement of >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is avoided. The review shall consider whether:

– the process or vessels/pipe work can be modified to remove or reduce hazards at the source;

– additional safety-related systems or other risk reduction means, not based on instrumentation, can be introduced;

– the severity of the consequence can be reduced, e.g., reducing the amount of hazardous material;

– the likelihood of the specified consequence can be reduced e.g., reducing the likelihood of the initiating source of the hazardous event.

NOTE Applications which require the use of a single SIF with a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour need to be avoided because of the difficulty of achieving and

maintaining such high levels of performance throughout the SIS safety life-cycle. Risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour can require high levels of competence and high levels of coverage for all factory acceptance testing, proof testing, verification, and validation activities.

9.2.6 If after further consideration of the application and confirmation that a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is still required, then consideration should be given to achieving the safety integrity requirement using a number of protection layers (e.g., SIS or BPCS) with lower risk reduction requirements. If the risk reduction is allocated to multiple protection layers then such protection layers shall be independent from each other or the lack of independence shall be assessed and shown to be sufficiently low compared to the risk reduction requirements. The following factors shall be considered during this assessment:

– common cause of failure of SIS and the cause of demand;

NOTE 1 The extent of the common cause can be assessed by considering the diversity of all devices where failure could cause a demand and all devices of the BPCS protection layer and/or the SIS used for risk reduction.

NOTE 2 An example of common cause between the SIS and the cause of demand is if loss of process control through sensor fault or failure can cause a demand and the sensor used for control is of the same type as the sensor used for the SIS.

– common cause of failure with other protection layers providing risk reduction;

NOTE 3 The extent of the common cause can be assessed by considering the diversity of all devices of the BPCS protection layer and/or the SIS used to achieve the risk reduction requirements.

NOTE 4 An example of common cause between SISs providing risk reduction is when two separate and independent SISs with diverse measurements and diverse logic solvers are used but the final actuation devices are two shut off valves of similar types or a single shut off valve actuated by both SISs.

– any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times;

NOTE 5 Even if the protective layers are diverse then synchronous proof testing will reduce the overall risk reduction achieved and this can be a significant factor impeding achievement of the necessary risk reduction for the hazardous event.

NOTE 6 When high levels of risk reduction are required and proof tests are desynchronised according to Note 5 then the dominant factor is normally common cause failure even if multiple independent protection layers are used to reduce risk. Dependency within and between protection layers providing risk reduction for the same hazardous event can be assessed and shown to be sufficiently low.

9.2.7 If a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is to be implemented, whether allocated to a single SIS or multiple SIS or SIS in conjunction with a BPCS protection layer, then a further risk assessment shall be carried out using a quantitative methodology to confirm that the safety integrity requirements are achieved. The methodology shall take into consideration dependency and common cause failures between the SIS and:

– any other protection layer whose failure would place a demand on it;

– any other SIS reducing the likelihood of the hazardous event;

– any other risk reduction means that reduce the likelihood of the hazardous event (e.g., safety alarms).

9.2.8 If the risk reduction required for a hazardous event is allocated to multiple SIFs in a single SIS, then the SIS shall meet the overall risk reduction requirement.

9.2.9 The results of the allocation process shall be recorded so that the SIFs are described in terms of the functional needs of the process, e.g., the actions to be taken, set points, reaction times, activation delays, fault treatment, valve closure requirements, and in terms of the risk reduction requirements.

NOTE This description can be in an unambiguous logical form and can be referred to as the process requirements specification or the safety description. The description can make the intent and the approach used in the allocation process clear. The process requirements specification is used as input information for the SRS covered in Clause 10 and can be sufficiently detailed to ensure adequate specification of the SIS and its devices. For example, the description can include the set-points for sensors, the process safety time available for response, and the valve closure requirements.

9.3 Requirements on the basic process control system as a protection layer

9.3.1 The basic process control system may be claimed as a protection layer as shown in Figure 9.

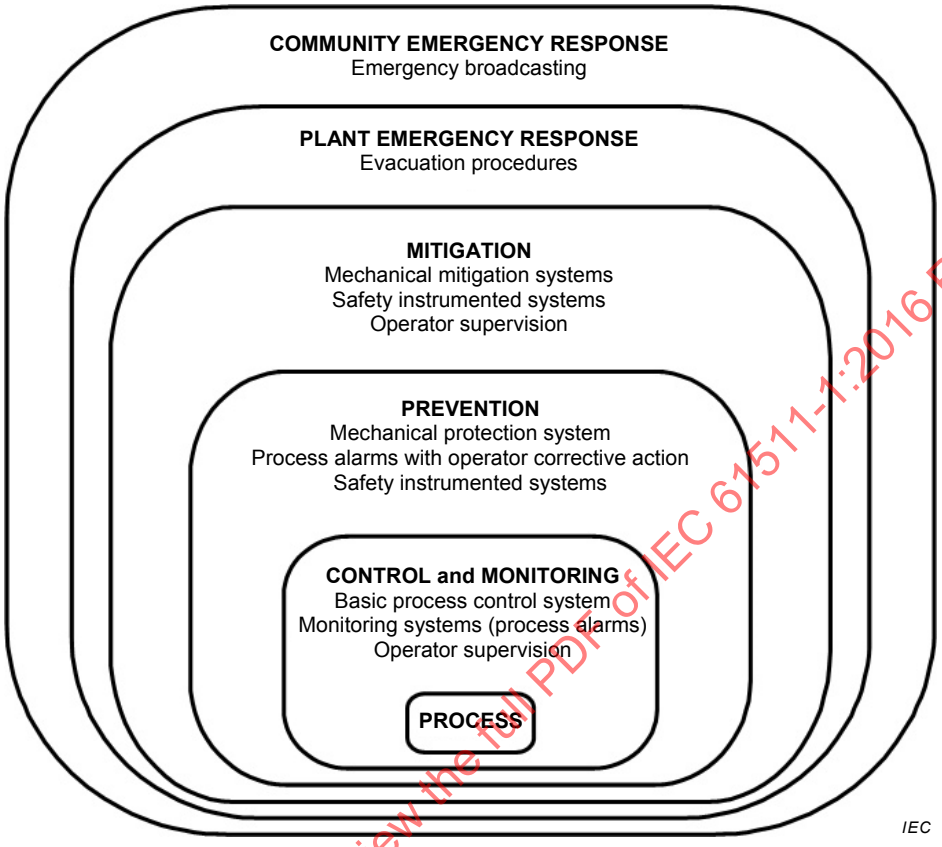


Figure 9 – Typical protection layers and risk reduction means

9.3.2 The risk reduction claimed for a BPCS protection layer shall be ≤10.

NOTE Consideration can be given to the fact that a BPCS may also be an initiating source for the demand on the protection layer.

9.3.3 If the risk reduction claimed for a BPCS protection layer is > 10, then the BPCS shall be designed and managed to the requirements within the IEC 61511 series.

9.3.4 If it is not intended that the BPCS conform to the IEC 61511 series, then:

- no more than one BPCS protection layer shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is the initiating source for the demand on the protection layer; or
- no more than two BPCS protection layers shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is not the initiating source of the demand.

NOTE The identified BPCS protection layer can consist of one BPCS as the initiating source for the demand (see 8.2.2) and a second independent BPCS protection layer (see 9.3.2 and 9.3.3) or up to two independent BPCS protection layers when the initiating source is not related to BPCS failure.

9.3.5 When 9.3.4 applies, each BPCS protection layer shall be independent and separate from the initiating source and from each other to the extent that the claimed risk reduction of each BPCS protection layer is not compromised.

NOTE 1 The assessment of separation and independence can consider what is necessary to achieve the risk reduction, e.g., the central processing units (CPU), input/output modules, relays, field devices, application

programming, networks, program database, engineering tools, human machine interface, by-pass tools and other devices.

NOTE 2 A hot backup controller is not considered to be independent of the primary controller because it is subject to common cause failure (for example, hot backup controllers have components that are common to both the primary and the backup controller, such as the backplane, firmware, diagnostics, transfer mechanisms and undetected dangerous failures).

9.4 Requirements for preventing common cause, common mode and dependent failures

9.4.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between:

- protection layers;
- protection layers and the BPCS.

are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.

NOTE A definition of dependent failure is provided in 3.2.12.

9.4.2 The assessment shall consider the following:

- independence between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS.

NOTE 1 Common causes from the process can be addressed. Plugging of relief valves may cause the same problems as plugging of sensors in a SIS.

NOTE 2 Independence and physical separation can be addressed. A Human Machine Interface, SIS/BPCS networks or bypass means can cause common cause failure.

10 SIS safety requirements specification (SRS)

10.1 Objective

The objective of Clause 10 is to specify the requirements for the SIS, including any application programs and the architecture of the SIS.

10.2 General requirements

The safety requirements shall be derived from the allocation of SIF and from those requirements identified during H&RA. The SIS requirements shall be expressed and structured in such a way that they are

- clear, precise, verifiable, maintainable and feasible;
- written to aid comprehension and interpretation by those who will utilise the information at any phase of the safety life-cycle.

10.3 SIS safety requirements

10.3.1 Addresses issues that shall be considered when developing the SIS safety requirements.

10.3.2 These requirements shall be sufficient to design the SIS and shall include a description of the intent and approach applied during the development of the SIS safety requirements as applicable:

- a description of all the SIF necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative);
- a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);
- requirements to identify and take account of common cause failures;
- a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated;
- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system);
- the assumed sources of demand and demand rate on each SIF;
- requirements relating to proof test intervals;
- requirements relating to proof test implementation;
- response time requirements for each SIF to bring the process to a safe state within the process safety time;

  NOTE See IEC 61511-2:2016 for further discussion of process safety time.
- the required SIL and mode of operation (demand/continuous) for each SIF;
- a description of SIS process measurements, range, accuracy and their trip points;
- a description of SIF process output actions and the criteria for successful operation, e.g., leakage rate for valves;
- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives for each SIF;
- requirements for manual shutdown for each SIF;
- requirements relating to energize or de-energize to trip for each SIF;
- requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element resets after trips);
- maximum allowable spurious trip rate for each SIF;
- failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shut-down);
- any specific requirements related to the procedures for starting up and restarting the SIS;
- all interfaces between the SIS and any other system (including the BPCS and operators);
- a description of the modes of operation of the plant and requirements relating to SIF operation within each mode;
- the application program safety requirements as listed in 10.3.2;
- requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared;
- the specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors;
- the mean repair time which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints;
- identification of the dangerous combinations of output states of the SIS that need to be avoided;
- identification of the extremes of all environment conditions that are likely to be encountered by the SIS during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration,

electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;

- identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIFs may be required to support these process operating modes;
- definition of the requirements for any SIF necessary to survive a major accident event, e.g., time required for a valve to remain operational in the event of a fire.

10.3.3 The application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS. The application program safety requirements may be located in the SRS or in a separate document (e.g., application program requirements specification). The input to the application program safety requirements for each SIS subsystem shall include:

a) the specified safety requirements of each SIF, including sensor voting, etc.;

b) the requirements resulting from the SIS architecture and the safety manual such as limitations and constraints of the hardware and embedded software;

c) any requirements of safety planning arising from 5.2.4.

10.3.4 The application program safety requirements shall be specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS.

10.3.5 The application program safety requirements specification shall be sufficiently detailed to allow the design and implementation to achieve the required functional safety and to allow a functional safety assessment to be carried out. The following shall be considered:

- the SIFs supported by the application program and their SIL;
- real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a specified time period;
- program sequencing and time delays if applicable;
- equipment and operator interfaces and their operability;
- all relevant modes of operation of the process as specified in the SRS;
- action to be taken on bad process variable such as sensor value out of range, excessive range of change, frozen value, detected open circuit, detected short circuit;
- functions enabling proof testing and automated diagnostics tests of external devices (e.g., sensors and final elements) performed in the application program;
- application program self-monitoring (e.g., application driven watch-dogs and data range validation);
- monitoring of other devices within the SIS (e.g., sensors and final elements);
- any requirements related to periodic testing of SIF when the process is operational;
- references to the input documents (e.g., specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS);
- the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;
- process dangerous states (for example closure of two isolation gas valves at the same time that could lead to pressure fluctuations thus leading to a dangerous state) generated by the application program shall be identified and avoided;
- definitions of process variable validation criteria for each SIF.

10.3.6 The application program safety requirements specification shall be expressed and structured in such a way that they:

- describe the intent and approach underpinning the application program safety requirements;
- are clear and understandable to those who will utilize the document at any phase of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by all users (e.g., plant operators, maintenance personnel, application programmers);
- are verifiable, testable, modifiable;
- are traceable back through all deliverables including the detailed design documents, the SRS and the H&RA that identifies the required SIF and SIL.

11 SIS design and engineering

11.1 Objective

The objective of the requirements of Clause 11 is to design one or multiple SIS to provide the SIF and meet the specified integrity requirements (e.g., SIL, associated risk reduction, PFD and /or PFH).

11.2 General requirements

11.2.1 The design of the SIS shall be in accordance with the SIS safety requirements specifications, taking into account all the requirements of Clause 11.

11.2.2 Where the SIS is to implement both SIFs and non-SIFs then all the hardware, embedded software and application program that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL of any of the SIFs it can impact.

11.2.3 Where the SIS is to implement SIF of different SIL, then the shared or common hardware and embedded software and application program shall conform to the highest SIL.

NOTE Embedded software or application programs of different SIL could coexist in the same device provided it can be demonstrated that the SIF of lower SIL cannot negatively affect the SIF of the higher SIL.

11.2.4 If it is intended not to qualify the BPCS to the IEC 61511 series, then the SIS shall be designed to be separate and independent from the BPCS to the extent that the safety integrity of the SIS is not compromised.

NOTE 1 Operating information can be exchanged but not compromise the functional safety of the SIS.

NOTE 2 Devices of the SIS can also be used for functions of the BPCS if it can be demonstrated that a failure of the BPCS does not compromise the SIF of the SIS.

11.2.5 Requirements for operability, maintainability, diagnostics, inspection and testability shall be addressed during the design of the SIS in order to reduce the likelihood of dangerous failures.

11.2.6 The design of the SIS shall take into account human capabilities and limitations and be suitable for the tasks assigned to operators and maintenance staff. The design of operator interfaces shall follow good human factors practice and shall accommodate the likely level of training that operators should receive.

NOTE 1 For example, human factor studies may be necessary if operation requires data entry of limits or other operator input on a regular basis.

11.2.7 The SIS shall be designed in such a way that once it has placed the process in a safe state, the process shall remain in the safe state until a reset has been initiated unless otherwise directed by the SRS.

11.2.8 Manual means (e.g., emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the SRS.

11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependency between the SIS and BPCS, and the SIS and other protection layers.

11.2.10 A device used by the BPCS shall not be used by the SIS where a failure of that device may result in both a demand on the SIF and a dangerous failure of the SIF, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand on the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared device because if the shared device fails, a demand will be created immediately to which the SIS may not be capable of responding. For that reason, additional analysis can be necessary in these cases to ensure that the dangerous failure rates of the shared devices are sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.

11.2.11 For any SIS device that on loss of utility (e.g., electrical power, air, hydraulics or pneumatic supply) does not fail to the safe state, loss of utility and SIS circuit integrity shall be detected and alarmed (e.g., end-of-line monitoring, supply pressure measurement, hydraulic or pneumatic pressure monitoring) and action taken according to 11.3.

NOTE 1 Utility integrity can be improved through using a supplementary supply (e.g., battery back-up, uninterruptible power supplies, air reservoir, hydraulic accumulator, second gas supply).

NOTE 2 The loss of a utility is likely to affect multiple SIFs and, possibly, multiple SISs. Hence common cause failure of multiple SIFs can be considered.

11.2.12 The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

NOTE Guidance related to SIS security is provided in ISA TR84.00.09 and IEC 62443-2-1:2010.

11.2.13 A safety manual covering operation, maintenance, fault detection and constraints associated with the SIS shall be available covering the intended configurations of the devices and the intended operating environment.

11.2.14 All communications used to implement a SIF shall be established using techniques appropriate for safety applications to meet the required SIL.

11.3 Requirements for system behaviour on detection of a fault

11.3.1 When a dangerous fault in a SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation. If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken. Where the compensating measures depend on an operator taking specific action in response to an alarm (e.g., opening or closing a valve) then the alarm shall be considered part of the SIS.

NOTE 1 The specified action (fault reaction) required to achieve or maintain a safe state of the process can be specified in the SRS (see 10.3.1). It can consist of the safe shutdown of the process or of that part of the process which relies on the faulty SIS for risk reduction.

NOTE 2 The compensating measures required for continued safe operations can depend on safety integrity requirements, the tolerable risk associated with the hazardous event, the hardware fault tolerance of the SIS, the anticipated MRT and the availability of any other layers of protection. In some cases it can be adequate to ensure action is taken to ensure repair of the dangerous failure within the assumed MPRT in the calculation of the PFDavg but in other cases it can be judged necessary to provide other measures to compensate for the reduced risk reduction until the SIS is fully restored. See also 16.2.3.

11.3.2 Where any dangerous fault in an SIS is brought to the attention of an operator by an alarm then the alarm shall be subject to appropriate proof testing and management of change.

11.4 Hardware fault tolerance

11.4.1 The SIS shall have a minimum HFT with respect to each SIF it implements.

NOTE This does not exclude the possibility that the HFT may be reduced below the minimum requirement at certain times during operation of the system following the occurrence of faults.

11.4.2 When the SIS can be split into independent SIS subsystems (e.g. sensors, logic solvers and final elements), then the HFT can be assigned at the SIS subsystem level.

11.4.3 The HFT of the SIS or its SIS subsystems shall be in accordance with;

- 11.4.5 to 11.4.9 of clause 11 or,
- the requirements of 7.4.4.2 (route 1H) of IEC 61508-2:2010 or,
- the requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.

NOTE The route developed in IEC 61511 is derived from route 2_H of IEC 61508-2:2010.

11.4.4 When determining the achieved HFT, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements. Any such fault exclusions shall be justified and documented.

NOTE Further information about fault exclusion can be found in ISO13849-1:2006 and ISO13849-2:2012.

11.4.5 The minimum HFT for a SIS (or its SIS subsystems) implementing a SIF of a specified SIL shall be in accordance with Table 6 and if appropriate 11.4.6 and 11.4.7.

NOTE The HFT requirements in Table 6 represent the minimum system or, where relevant, the SIS subsystem redundancy. Depending on the application, device failure rate and proof-testing interval, additional redundancy can be required to satisfy the failure measure for the SIL of the SIF according to 11.9.

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

11.4.6 For a SIS or SIS subsystem that does not use FVL or LVL programmable devices and if the minimum HFT as specified in Table 6, would result in additional failures and lead to decreased overall process safety, then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.

NOTE Fault tolerance is the preferred solution to achieve the required confidence that a robust architecture has been achieved. When 11.4.6 applies, the purpose of the justification is to demonstrate that the proposed alternative architecture provides an equivalent or better solution. This may vary depending on the application and/or the technology in use; examples include: back-up arrangements (e.g., analytical redundancy, replacing a failed sensor output by physical calculation results from other sensors outputs); using more reliable items of the same technology (if available); changing for a more reliable technology; decreasing common cause failure impact by using diversified technology; increasing the design margins; constraining the environmental conditions (e.g. for electronic components); decreasing the reliability uncertainty by gathering more field feedback or expert judgment.

11.4.7 If a fault tolerance equal to zero results from applying 11.4.6, the justification required by 11.4.6 shall provide evidence that the related dangerous failure modes can be excluded, in accordance with 11.4.4 including consideration of the potential for systematic failures.

11.4.8 FVL and LVL programmable devices shall have diagnostic coverages not less than 60 %.

11.4.9 Reliability data used in the calculation of the failure measure shall be determined by an upper bound statistical confidence limit of no less then 70 %.

11.5 Requirements for selection of devices

11.5.1 Objectives

The objectives of the requirements of 11.5 are to:

- specify the requirements for the selection of devices which are to be used as part of the SIS;
- specify the requirements to enable a device to be integrated in the architecture of a SIS;
- specify acceptance criteria for devices in terms of associated SIF and safety integrity requirements.

11.5.2 General requirements

11.5.2.1 Devices selected for use as part of a SIS with a specified SIL shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010 and/or 11.5.3 through 11.5.6, as appropriate.

NOTE Devices assessed against IEC 61508-2:2010 and IEC 61508-3:2010 can be applied in accordance with the requirements for systematic capability in IEC 61508-2:2010.

11.5.2.2 All devices shall be suitable for the operating environment as determined through consideration of the manufacturer's documentation, the constraints within the SRS and the reliability parameters assumed in respect of 11.9. Suitability of the selected devices shall always be considered in the context of the operating environment.

NOTE Devices may exhibit different failure rates dependent on the operating environment and mode of operation. Failure rate data available from manufacturers may not be valid in all applications. For example, the failure rate and failure mode distribution can be different for a valve that is frequently exercised versus one that stands still for long periods of time.

11.5.3 Requirements for the selection of devices based on prior use

11.5.3.1 Appropriate evidence shall be available that the devices are suitable for use in the SIS.

NOTE 1 The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 2 Level of detail of the evidence can be in accordance with the complexity of the considered device.

NOTE 3 A prior use evaluation involves gathering documented information concerning the device performance in a similar operating environment. Prior use demonstrates the functionality and integrity of the installed device, including the process interfaces, full device boundary, communications, and utilities. The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 4 Prior use data can contribute to a database for the calculation of hardware failure rates as described in 11.9.3.

11.5.3.2 The evidence of suitability shall include the following:

- consideration of the manufacturer's quality, management and configuration management systems;
- adequate identification and specification of the devices;
- demonstration of the performance of the devices in similar operating environments;

NOTE 1 In the case of field devices (e.g., sensors and final elements) fulfilling a given specification, the behaviour of the device in the operating environment is usually identical in safety and non-safety applications. Therefore, evidence of the performance of similar devices in non-safety applications can also be used to satisfy this requirement.

- the volume of the operating experience.

NOTE 2 For field devices, information relating to operating experience is mainly recorded in the user's list of equipment approved for use in their facilities, based on an extensive history of successful performance in safety and non-safety applications, and on the elimination of equipment not performing in a satisfactory manner. The list of field devices can be used to support claims of experience in operation, provided that:

– the list is updated and monitored regularly;

– field devices are only added when sufficient operating experience has been obtained;

– field devices are removed when they show a history of not performing in a satisfactory manner;

– the operating environment is included in the list where relevant.

NOTE 3 Device performance is highly affected by the operating environment. It is generally recommended that selection of devices can be based on adequate performance of an installed sufficient number of devices in multiple installations for a sufficient operating time. The gained experience can allow time to reveal early failures, such as those related to specification, handling, installation, and commissioning.

NOTE 4 The amount of operational experience to gain credible statistical reliability data is typically much higher compared to the operational experience necessary to get evidence of prior use.

11.5.3.3 All devices selected on the basis of prior use shall be identified by a specified revision number and shall be under the control of a management of change procedure. In the case of a change being made to the device, the continued validity of the evidence of prior use shall be justified by evaluating the significance of the change made.

11.5.4 Requirements for selection of FPL programmable devices (e.g., field devices) based on prior use

11.5.4.1 For SIL 1, SIL 2, and SIL 3, the requirements of 11.5.2 and 11.5.3 apply, together with the following subclauses.

11.5.4.2 All configuration options of the device possibly influencing safety shall be identified and considered. It is important to check that wherever specific settings are not defined that the default settings of the device are confirmed to be appropriate. Unused features of the devices shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required SIF.

11.5.4.3 For the specific configuration and operating environment of the device, the evidence of suitability shall consider:

- characteristics of input and output signals;
- modes of use;
- functions and configurations used;
- prior use in similar operating environments.

11.5.4.4 In addition, for SIL 3 applications, an assessment of the FPL device shall be carried out to show that:

- the FPL device is both able to perform the required functions and that prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;
- appropriate standards for hardware and software have been applied;
- the FPL device has been used or tested in configurations representative of the intended operational profiles.

11.5.5 Requirements for selection of LVL programmable devices based on prior use

11.5.5.1 The following requirements apply to PE devices used in SISs which implement SIL 1 or SIL 2 SIFs.

11.5.5.2 The requirements of 11.5.4 apply.

11.5.5.3 Where there is any difference between the operating environment of a device as experienced previously, and the operating environment of the device when used within the SIS, then any such differences shall be identified and there shall be an assessment based on analysis and testing, as appropriate, to show that the likelihood of systematic faults when used in the SIS is sufficiently low.

11.5.5.4 The operating experience considered necessary to justify the suitability shall be determined taking into account:

- the SIL of the SIF;
- the complexity and functionality of the devices.

11.5.5.5 For SIL 1 or 2 applications, a safety configured PE logic solver may be used provided that all the following additional provisions are met:

- understanding of unsafe failure modes;
- use of techniques for safety configuration that address the identified failure modes;
- the embedded software has a good history of use for safety applications;
- protection against unauthorized or unintended modifications.

NOTE A safety configured PE logic solver is a general purpose industrial grade PE logic solver which is specifically configured by the OEM, a systems engineer or the end-user for use in safety applications.

11.5.5.6 A formal assessment of any PE logic solver used in a SIL 2 application shall be carried out to show that:

- it is both able to perform the required functions and that prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;
- measures are implemented to detect faults during program execution and initiate appropriate responses; these measures shall comprise all of the following:
  - program sequence monitoring;
  - protection of code against modifications or failure detection by on-line monitoring;
  - failure assertion or diverse programming;
  - range check of variables or plausibility check of values;
  - modular approach;
  - appropriate coding standards have been used for the embedded and utility software;
  - testing in typical configurations, with test cases representative of the intended operational profiles;
  - trusted verified software modules and components have been used;
  - the system has undergone dynamic analysis and testing;
  - the system does not use artificial intelligence or dynamic reconfiguration;
  - documented fault-insertion testing (negative testing) has been performed.

11.5.6 Requirements for selection of FVL programmable devices

When the applications are programmed using a FVL, the PE device shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010.

11.6 Field devices

11.6.1 Field devices shall be selected and installed to minimize failures that could result in inaccurate information due to conditions arising from the operating environment. Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, coking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse lines.

11.6.2 Energize to trip circuits shall apply means to ensure circuit and power supply integrity.

NOTE 1 An example of such means is an end-of-line monitor, where a pilot current is continuously monitored to detect circuit continuity and where the pilot current is not of sufficient magnitude to affect proper I/O operation.

NOTE 2 Additional requirements for loss of power can be found in 11.2.11.

11.6.3 Smart sensors shall be write-protected to prevent inadvertent modification, unless appropriate safety review (e.g., H&RA) allows the use of read/write.

NOTE The review can take into account human factors such as failure to follow procedures.

11.7 Interfaces

11.7.1 General

Interfaces to the SIS can include, but are not limited to:

- operator interface(s);
- maintenance/engineering interface(s);
- communication interface(s).

11.7.2 Operator interface requirements

11.7.2.1 Where the SIS operator interface is via the BPCS operator interface, account shall be taken of credible failures that may occur in the BPCS operator interface.

NOTE This can include preparing plans to enable an orderly safe shutdown in the event of total failure of the operational displays.

11.7.2.2 The design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while hazards are present. If the design does require the use of operator actions, the design should include facilities for protection against operator error.

NOTE If the operator has to select a particular option, there can be a confirmation step.

11.7.2.3 Bypass switches or means shall be protected to prevent unauthorized use (e.g., by key locks or passwords in conjunction with effective management controls).

NOTE Consideration can be given to enforcing time limits on bypass operation and to limiting the number of bypasses that can be active at any one time.

11.7.2.4 The SIS status information that is critical to maintaining the SIF shall be available as part of the operator interface. This information may include:

- where the process is in its sequence;
- indication that SIS protective action has occurred;

- indication that a protective function is bypassed;
- indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- status of sensors and final elements;
- the loss of energy where that energy loss impacts safety;
- the results of diagnostics;
- failure of environmental conditioning equipment which is necessary to support the SIS.

11.7.2.5 The SIS operator interface design (see 11.7.2.7) shall be such as to prevent changes to the SIS application program.

11.7.2.6 Where information is transferred from the BPCS to the SIS, systems, equipment or procedures shall be applied to confirm that the correct information has been transferred and that the safety integrity of the SIS is not compromised.

NOTE The systems, equipment or procedures used can include control over selective writing from the BPCS to specific SIS variables.

11.7.2.7 The design of the SIS operator interface via the BPCS operator interface shall be such that provision of incorrect information or data from the BPCS to the SIS shall not compromise safety.

11.7.3 Maintenance/engineering interface requirements

11.7.3.1 The design of the SIS maintenance/engineering interface shall ensure that any failure of this interface shall not adversely affect the ability of the SIS to carry out the required SIFs. This may require disconnecting of maintenance/engineering interfaces, such as programming panels, during normal SIS operation.

11.7.3.2 The maintenance/engineering interface shall provide the following functions with access security protection to each:

- SIS mode of operation, program, data, means of disabling alarm communication, test, bypass, maintenance;
- SIS diagnostic, voting and fault handling services;
- add, delete, or modify application program;
- data necessary to troubleshoot the SIS;
- where bypasses are required they should be installed such that alarms and manual shutdown facilities are not disabled.

11.7.3.3 The maintenance/engineering interface shall not be used as the operator interface.

11.7.3.4 Enabling and disabling the read-write access shall be carried out only by a configuration management process using the maintenance/engineering interface with appropriate documentation and security measures such as authentication and user secure channels.

11.7.4 Communication interface requirements

11.7.4.1 The design of any SIS communication interface shall ensure that any failure of the communication interface shall not adversely affect the ability of the SIS to achieve or maintain a safe state of the process.

11.7.4.2 When the SIS is able to communicate with the BPCS and peripherals, the communication interface, BPCS, or peripherals shall not adversely impact any of the SIFs within the SIS.

11.7.4.3 The communication interface shall be sufficiently robust to withstand electromagnetic interference including power surges without causing a dangerous failure of the SIS.

11.7.4.4 The communication interface shall be suitable for communication between devices referenced to different electrical ground potentials.

NOTE An alternate medium (e.g., fibre optics) can be required.

11.8 Maintenance or testing design requirements

11.8.1 The design shall allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.

NOTE The term “end-to-end” means from process fluid at sensor end to process fluid at actuation end.

11.8.2 When on-line proof testing is required, test facilities shall be an integral part of the SIS design.

11.8.3 When test or bypass facilities are included in the SIS, they shall conform with the following:

- The SIS shall be designed in accordance with the maintenance and testing requirements defined in the SRS;
- The operator shall be alerted to the bypass of any portion of the SIS via an alarm or operating procedure.

11.8.4 The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.

11.8.5 Compensating measures that ensure continued safe operation shall be provided in accordance with 11.3 when the SIS is in bypass (repair or testing).

11.8.6 Forcing of inputs and outputs in PE SIS shall not be used as a part of application program(s), operating procedure(s) and maintenance (except as noted below).

Forcing of inputs and outputs without taking the SIS out of service shall not be allowed unless supplemented by procedures and access security. Any such forcing shall be announced or set off an alarm, as appropriate.

11.9 Quantification of random failure

11.9.1 The calculated failure measure of each SIF shall be equal to, or better than, the target failure measure related to the SIL as specified in the SRS. This shall be determined by calculation.

NOTE In complex applications, the hazardous event frequency can be used as an alternative to the target failure measures (e.g., where different demand causes have different safety integrity requirements or where non-independent SISs act in sequence).

11.9.2 The calculated failure measure of each SIF due to random failures shall take into account all contributing factors including the following:

a) the architecture of the SIS and of its SIS subsystems where relevant as they relate to each SIF under consideration;

b) the estimated failure rate related to each failure mode, due to random hardware failures, which would contribute to a dangerous failure of the SIS but which are detected by diagnostic tests;

c) the estimated failure rate related to each failure mode, due to random hardware failures, which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests but which are detected by proof tests:

d) the estimated failure rate related to each failure mode, due to random hardware failure, which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests and undetected by proof tests;

e) the susceptibility of the SIS to failures caused by the proof tests themselves;

f) the susceptibility of the SIS to common cause failures;

g) the diagnostic coverage of any periodic diagnostic tests, the associated diagnostic test interval and the probability of failure of the diagnostic facilities;

h) the coverage of any periodic proof tests, the associated proof test procedure and the reliability for the proof test facilities and procedure;

i) the repair times for detected failures and the state of the SIS during repairs (on line or off line);

j) the estimated dangerous failure rate of any communication process in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);

k) the estimated likelihood that operator response would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);

l) the reliability of any utility necessary for the SIS.

NOTE Several modelling approaches are available and the most appropriate approach is a matter for the analyst and can depend on the circumstances. Available means include (see IEC 61508-6:2010, annex B):

– cause consequence analysis;

– reliability block diagrams;

– fault-tree analysis;

– Markov models;

– Petri nets models.

The probabilistic calculations can be performed analytically or by numerical simulation (e.g., Monte Carlo simulation).

11.9.3 The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified and shall be based on field feedback from similar devices used in a similar operating environment.

NOTE 1 This includes user collected data, vendor/provider/user data derived from data collected on devices, data from general field feedback reliability databases, etc. In some cases, engineering judgement can be used to assess missing reliability data or evaluate the impact on reliability data collected in a different operating environment.

NOTE 2 The lack of reliability data reflective of the operating environment is a recurrent shortcoming of probabilistic calculations. End-users can organize relevant device reliability data collections in accordance with IEC 60300-3-2:2004 or ISO 14224:2006 to improve the implementation of the IEC 61511 series.

NOTE 3 Vendor data based on returns can be restricted to a population where there is full knowledge of the operational environment and fully recorded in accordance with IEC 60300-3-2:2004 or ISO 14224:2006. The user can also record the operational environment for the SIF and be able to demonstrate that the vendor's operational environment data matches the environment of the SIF.

11.9.4 The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.

NOTE 1 The reliability data uncertainties can be evaluated according to the amount of field feedback (less field feedback results in more uncertainty) or/and exercise of expert judgement. Published standards (IEC 60605-4), Bayesian approaches, engineering judgement techniques, etc. can be used to estimate the reliability data uncertainties.

NOTE 2 The following techniques can be used for calculating the failure measures (more information can be found in IEC 61511-2:2016):

– use of an upper bound confidence of 70 % for each input reliability parameter instead of its mean in order to obtain conservative point estimations of the failure measures, or;

– use the probabilistic distributions functions of input reliability parameters, perform Monte Carlo simulations to obtain an histogram representing the distribution of the failure measure and assess a conservative value from this distribution (e.g., that there is a 90 % confidence that the true failure measure is better than the value calculated).

11.9.5 If, for a particular design, the target failure measure for the relevant SIF is not achieved then:

a) identify the devices or parameters contributing most to the failure measure;

NOTE Fault tree cut-set analysis can be useful here.

b) evaluate the effect of possible improvement measures on the identified devices or parameters (e.g., more reliable devices, additional defences against common mode failures, increased diagnostic or proof test coverage, increased redundancy, reduced proof test interval, staggering tests, etc.);

c) select and implement improvement measures to establish the new result;

d) compare the new result to the target failure measure and repeat the steps a) to d) until the target failure measure is achieved in a conservative manner.

12 SIS application program development

12.1 Objective

The objective of Clause 12 is to define the requirements for the development of the application program.

12.2 General requirements

12.2.1 The application program of the SIS shall be in accordance with the application program safety requirements (see 10.3.3) and all the requirements of this clause for all SIL up to and including SIL 3.

12.2.2 The application programmer shall review the information in the SRS and the application program safety requirements to ensure that the requirements are comprehensive, unambiguous, understandable and consistent. Any deficiencies in the application program safety requirements shall be identified and resolved, and if changes are made to the application program safety requirements, an impact analysis shall be carried out.

12.2.3 The IEC 61511 series addresses programming in Limited Variability Languages (LVL) and the use of devices using Fixed Program Languages (FPL). The IEC 61511 series does not address Full Variability Language (FVL) and the IEC 61511 series does not address SIL 4 application programming. Where function blocks are written in FVL then these shall be developed and modified under IEC 61508-3:2010.

12.2.4 Where the application program of the SIS is to implement both safety and non-safety functions, then all of the application program shall be treated as part of the SIS and shall comply with this standard and in addition, it shall be shown through assessment and test that the non-safety functions cannot interfere with the safety functions.

12.2.5 The application program shall be designed in such a way as to ensure that once the SIS has placed the process in a safe state, the process remains in the safe state, including under loss of power conditions and on power restoration, until a reset has been initiated unless otherwise directed by the SRS.

NOTE 1 If the SIF does not have a reset then there can be a documented engineering argument as to why it is acceptable to reinitiate the process without requiring the safe delay a reset would impose.

NOTE 2 More information can be found in 11.2.7.

12.2.6 During SIS start-up (or power up) the application program shall ensure that safety outputs remain in the safe state (typically de-energized state) until a reset has been initiated unless otherwise directed by the SRS.

12.2.7 The application program shall be designed in such a way that all parts of the application program are executed on every application program scan unless there is a specific alternate requirement that is supported in the safety manual. Process safety time requirements shall be considered when establishing application program scanning requirements.

12.2.8 The SIS application program and data shall be subject to modification, revision control, version management, back-up and restoration procedures.

12.2.9 The application program specifies requirements for application programming for users and integrators of SISs. In particular, requirements for the following are specified:

- SIS safety life-cycle phases and activities that are to be applied during the design and development of the application program. These requirements include the application of measures and techniques, which are intended to avoid errors in the application program and to control failures which may occur;
- information relating to the application program validation to be passed to the organization carrying out the SIS integration;
- preparation of information and procedures concerning the application program needed by the user for the operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications of the application program.

12.3 Application program design

12.3.1 An application program design shall address all SIS logic including all process operating modes for each SIF.

12.3.2 The input to the application program design shall be the SRS including the application program requirements (see Clause 10), the SIS architecture (see Clause 11) and the means and tools for developing the application program design (see 12.6). The application program design shall be consistent with and traceable back to the SRS.

12.3.3 The application program design shall allow an assessment of functional safety to be carried out.

12.3.4 The application program design and its decomposition into modules if applicable, shall address how the requirements are to be implemented, including the following as appropriate:

- the functions that enable the process to achieve or maintain a safe state;
- the specification of all identified application program components, and the description of connections and interactions between identified components;
- the timing constraints associated with the application program functions and their implementation in program scan time(s);
- a detailed description of the standard library modules (function blocks) being used;
- a detailed description of the application specific modules (function blocks) being used;
- a description of the way memory allocation has been achieved;
- the list of global variables used and the way in which their integrity is protected;
- identification of all non-SIF and the interfaces to non-safety related parts of the application program, to ensure that they cannot affect the proper operation of any SIF;

- definition of input and output interfaces, including tag listings and the associated data types;
- details of the data exchanged between the SIS application program and the operator interfaces;
- details of the data exchanged between the SIS application program and the BPCS and peripherals such as printers, data storage, etc.;
- how external and internal diagnostic information will be processed and logged;
- detailed description of how the operation and maintenance interfaces are implemented, including the way in which alarms are prioritised, indicated and accepted;
- a detailed description of any application level diagnostics that may be implemented such as external watch dogs, application data integrity checking, sensor validation to meet the required SIL;
- system configuration checks including the existence and accessibility of expected hardware devices and software modules;
- how the complexity in the application program design is minimised e.g., through use of modular design and simple functionality;
- functions related to the detection, annunciation and management of faults in SIS subsystems;
- functions related to the periodic testing of SIF on-line;
- functions related to the periodic testing of SIF off-line;
- functions that allow maintenance of the SIS to be carried out safely;
- references to documents on which the application program design specification is based.

12.3.5 The application program design shall ensure:

- completeness with respect to the SRS and its intended purpose;
- correctness with respect to the SRS and its intended purpose;
- freedom from ambiguity, i.e., clear to those who will utilize the document at any stage of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by plant operators and system maintainers, as well as the application programmers;
- freedom from design faults.

12.4 Application program implementation

12.4.1 The application program development methodology shall comply with the development tools and restrictions given by the manufacturer of the SIS PE subsystem on which the application program shall be used.

12.4.2 The following information shall be contained in the application program or related documentation:

a) the application program originator;

b) a description of the purpose of the application program;

c) the versions of the safety manuals that were used;

d) identification of the dependency of each SIF on the parts (modules) of the application program;

e) traceability to the application program safety requirements specification;

f) identification of each SIF and its SIL;

g) identification and description of the symbols used, including logic conventions, standard library functions, application library functions;

h) identification of the SIS logic solver input and output signals;

i) where the overall SIS utilises communications, a description of the communications information flow;

NOTE An example would be where a SIF uses several logic solvers.

j) a description of the program structure, including a description of the order of the logical processing of data with respect to the input/output sub-systems and any limitations imposed by scan times;

k) If required by the SRS, the means by which:

- the correctness of field data is ensured, (e.g., comparison between analog sensors to improve the diagnostic coverage);
- the correctness of data sent over a communication link is ensured (e.g., when communicating from an HMI, before implementation of a command an 'ack' or 'acknowledge' is transmitted);
- communications are made secure (e.g., cyber security measures);

l) version identification and a history of changes.

12.4.3 If previously developed application program library functions are to be used as part of the design, their suitability shall be justified and based upon:

- compliance to IEC 61508; if proven-in-use evaluation for FVL in compliance to IEC 61508-3:2010 is undertaken, the programmable devices on which the application program library functions execute shall also be evaluated as proven-in-use according to IEC 61508-2:2010; or
- compliance to IEC 61511 prior use requirements (see 11.5.4 or 11.5.5) when using FPL or LVL;
- in all cases, demonstrating that any unused functions do not adversely impact the application program.

12.4.4 The application program shall be produced in a structured way so as to achieve:

- modular decomposition of the functionality;
- keep the complexity of SIF application program to a minimum consistent with that of the complexity of the required SIF;
- testability of functionality (including fault tolerant features) and of the internal structure of the application program;
- traceability to, and explanation of, application functions and associated constraints;
- one to one mapping between the hardware architecture and application program architecture.

12.5 Requirements for application program verification (review and testing)

12.5.1 Verification planning shall be carried out in accordance with Clause 7.

12.5.2 The application program including its documentation shall be reviewed by a competent person not involved in the original development. The approach used for the review and the review results shall be documented.

12.5.3 The application program, including its decomposition into modules if appropriate, shall be verified through review, analysis, simulation and testing techniques using written procedures and test specifications, that shall be carried out to confirm that the application program functions meet the SRS and that unintended functions are not executed and that there are no unintended side effects with respect to the SIF. The following shall be addressed:

- conformance to the application program design specification, the defined means and procedures, and the requirements of safety validation and test planning;
- exercising of all parts of the application program;
- exercising a representative range of data conditions;
- testing for failure conditions (i.e., negative testing);
- timing and the sequence of execution;
- testing of communications to and from the SIS;

  NOTE Wherever feasible the communication overload condition can be verified and tested.
- integration of the off-line application program with the logic solver hardware and the underlying PE;
- internal data flow checks to confirm that the logic solver is not just apparently working, but is working as expected;
- when possible, integration of the application program and 3rd party devices.

12.5.4 The mapping of the I/O data to the application program, including data type and range, shall be verified.

12.5.5 During testing, modifications to the application program shall be subject to an impact analysis in order to determine:

- all application program parts impacted;
- the necessary re-design and re-verification activities.

12.5.6 The results of application program testing shall be documented and include:

- the versions of the application program and its supporting documentation being tested;
- the versions of supporting software and test tools;
- names of the person(s) who performed the tests and reviews and dates;
- descriptions of the tests, reviews and dates performed;
- the test results;
- whether the objective and criteria of the tests have been met;
- if there was a failure during the test, the reasons why the failure occurred, the analysis of the failure and the records of its correction and re-test requirements.

12.6 Requirements for application program methodology and tools

12.6.1 The application program development shall comply with the constraints in the applicable safety manual(s).

NOTE The safety manual(s) can be reviewed and, if required for a specific application, additional procedures for and/or constraints on the use of methodologies and tools can be implemented.

12.6.2 Methods, techniques and tools shall be selected and applied for each life-cycle phase so as to:

- minimize the risk of introducing faults into the application program;
- reveal and remove faults that already exist in the application program;
- ensure as far as is practicable that any faults remaining in the application program will not lead to unacceptable results;
- enhance the means of managing modifications of the application program throughout the lifetime of the SIS;
- provide evidence that the application program has the required quality.

13 Factory acceptance test (FAT)

13.1 Objective

The objective of Clause 13 is to test the devices of the SIS to ensure that the requirements defined in the SRS are met.

NOTE 1 By testing the logic solver, associated software and hardware prior to installation, errors can be readily identified and corrected.

NOTE 2 The FAT is sometimes referred to as an integration test and can be part of the validation.

NOTE 3 Testing of field elements together with the logic solver can be recommended when there needs to be a high confidence in operation prior to final installation, e.g., subsea applications.

13.2 Recommendations

13.2.1 The need for a FAT shall be specified during the safety planning for a project.

NOTE 1 Close co-operation between the logic solver supplier and design contractor can be required in order to develop the integration tests.

NOTE 2 The activities follow the design and development phases and precede the installation and commissioning.

NOTE 3 The activities are applicable to the SIS subsystems with or without programmable electronics.

NOTE 4 It is usual for the FAT to take place in a factory environment prior to installation and commissioning in the plant.

13.2.2 The planning for a FAT shall specify the following:

- Types of tests to be performed including black-box system functionality tests; performance tests; internal checks; performance tests; environmental tests; interface testing; testing in degraded or faulted condition; exception testing; testing for safe reaction in case of power failure (including restart after power restored); and application of the SIS maintenance and operating manuals;

  NOTE 1 Black-box functionality testing is a test design method that treats the system as a “black box”, so it does not explicitly use knowledge of its internal structure. Black- box test design is usually described as focusing on testing function requirements. Synonyms for black box include behavioural, functional, opaque-box, and closed-box testing.

  NOTE 2 Performance tests determine whether the system meets timing, reliability and availability, integrity, safety targets and constraints.

  NOTE 3 Environmental tests include EMC, life-and stress-testing.

  NOTE 4 Internal data flow checks can be carried out to that the SIS is processing input data and generating output response as specified.

- Test cases, test description and test data;

  NOTE 5 Clarity in defining who is responsible for developing the test case and who is going to be responsible for carrying out the test and witnessing the test can be very important.

- Dependence on other systems/interfaces;
- Test environment and tools;
- Logic solver, sensor and final element configuration;
- Test criteria on which the completion of the test shall be judged;
- Procedures for corrective action on failure of test;
- Test personnel competences;
- Physical location;
- Hazards posed by the testing especially dealing with stored energy;
- A clear diagram of the test-set up.
- Recording of tests conducted, data, results and observations whilst the tests are being conducted.

NOTE 6 Tests that cannot be physically demonstrated are normally resolved by a formal line of reasoning as to why the SIS achieves the requirement, target or constraint.

13.2.3 The FAT shall take place on a defined version of the logic solver.

13.2.4 The FAT shall be conducted in accordance with the FAT planning. These tests shall show that all the logic performs correctly.

13.2.5 For each test carried out the following shall be addressed:

- the version of the test planning being used;
- the SIF and performance characteristic being tested;
- the detailed test procedures and test descriptions;
- a chronological record of the test activities;
- the tools, equipment and interfaces used.

13.2.6 The results of FAT shall be documented, stating

- the test cases;
- the test results;
- whether the objectives and test criteria have been met.

If there is a failure during test, the reasons for the failure shall be documented and analysed and the appropriate corrective action should be implemented.

13.2.7 During FAT, any modification or change shall be subject to a safety analysis to determine:

- the extent of impact on each SIF;
- the extent of testing and verification which shall be defined and implemented.

NOTE Commissioning can commence whilst corrective action is undertaken, depending on the results of the FAT.

14 SIS installation and commissioning

14.1 Objectives

The objectives of the requirements of Clause 14 are to:

- install the SIS according to the specifications and drawings;
- commission the SIS so that it is ready for final system validation.

NOTE The purpose of commissioning activities is to ensure that each of the SIS devices is individually ready to operate, as specified in the design phase.

14.2 Requirements

14.2.1 Installation and commissioning planning shall define all activities required for installation and commissioning. The planning shall provide the following:

- the installation and commissioning activities;
- the procedures, measures and techniques to be used for installation and commissioning;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities.

Installation and commissioning planning may be integrated in the overall project planning where appropriate.

14.2.2 All SIS devices shall be properly installed according to the design and installation plan(s).

14.2.3 The SIS shall be commissioned in accordance with planning in preparation for the final system validation. Commissioning activities shall include, but not be limited to, confirmation of the following:

- earthing (grounding) has been properly connected;
- energy sources have been properly connected and are operational;
- transportation stops and packing materials have been removed;
- no physical damage is present;
- all instruments have been properly calibrated and configured;
- all field devices are operational;
- logic solver and input/outputs are operational;
- the interfaces to other systems and peripherals are operational;
- all communications between remote SIS systems are operational.

14.2.4 Appropriate records of the commissioning of the SIS shall be produced, stating the results of the activities and whether the objectives and criteria identified during the design phase have been met. If there is a failure, the reasons for the failure shall be recorded.

14.2.5 Where it has been established that the actual installation does not conform to the design information then the difference shall be evaluated by a competent person and impact of the difference on safety shall be determined. If it is established that the difference has no impact on safety, then the design information shall be updated to "as-built" status. If the difference has a negative impact on safety, then the installation shall be modified to meet the design requirements.

15 SIS safety validation

15.1 Objective

The objective of the requirements of Clause 15 is to validate, through inspection and testing, that the installed and commissioned SIS and its associated SIF(s) achieve the requirements as stated in the SRS.

NOTE This is sometimes referred to as a site acceptance test (SAT).

15.2 Requirements

15.2.1 Validation planning of the SIS shall be carried out throughout the SIS safety life-cycle and shall define all activities and equipment required for validation. The following items shall be included:

- the validation activities including validation of the SIS with respect to the SRS including implementation and resolution of resulting recommendations;
- validation of all relevant process operating modes of the process and its associated equipment including;
  - preparation for use including setting and adjustment;
  - start-up, automatic, manual, semi-automatic, steady state of operation;
  - re-setting, shutdown, maintenance;
  - other modes identified in previous phases of the SIS safety life-cycle;

- the procedures, measures and techniques to be used for validation, including how validation activities can be performed, without putting the plant and process at risk of the hazardous events the SIS is to protect against;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities and the levels of independence for validation activities;
- reference to information against which validation shall be carried out (e.g., cause and effect chart);
- the equipment and facilities that needs to be installed or made available (e.g. isolation valves and leak detection equipment that will be needed for the testing of valves).

NOTE Examples of validation activities include loop testing, logic testing, calibration procedures, simulation of application program.

15.2.2 Validation planning for the application program shall include the following:

- identification of the application program functions which needs to be validated for each process operating mode before commissioning begins;
- the technical strategy for the validation including (where relevant):
  - manual and automated techniques;
  - static and dynamic techniques;
  - analytical and statistical techniques.
- in accordance with the preceding bullet, the measures (techniques) and procedures that will be used for confirming that each SIF conforms with the specified safety requirements and the specified SIL;
- the required environment in which the validation activities are to take place (e.g., for tests this would include calibrated tools and equipment);
- the application program;
- the pass/fail criteria for accomplishing validation including:
  - the required process and operator input signals with their sequences and their values;
  - the anticipated output signals with their sequences and their values;
  - other acceptance criteria, for example memory usage, timing and value tolerances.
- the policies and procedures for evaluating the results of the validation, particularly failures;
- all documents (see Clause 19) are validated for accuracy, consistency and traceability of the SIF from inception during the H&RA through the final installed SIF.

15.2.3 Where measurement accuracy is required as part of the validation then instruments used for this function should be calibrated against a specification traceable to a standard within an uncertainty appropriate to the application. If such a calibration is not feasible, an alternative method shall be used and documented.

15.2.4 The validation of the SIS and its associated SIF(s) shall be carried out in accordance with the SIS validation planning. Validation activities shall include, but not be limited to, the following:

- confirmation that the SIS performs under normal and abnormal process operating modes (e.g., start-up, shutdown) as identified in the SRS;
- confirmation that adverse interaction of the BPCS and other connected systems do not affect the proper operation of the SIS;
- the SIS properly communicates (where required) with the BPCS or any other system or network, including during abnormal conditions such as a data overload;

- sensors, logic solver, and final elements perform in accordance with the SRS, including all redundant channels, including abnormal condition such as data overload;

  NOTE If a factory acceptance test (FAT) was performed on the logic solver as described in Clause 13, credit can be taken for validation of the logic solver by the FAT. After all equipment is installed in the plant, full loop validation will test the logic solver functionality and its connections to other SIS subsystems.

- SIS design documentation is consistent with the installed system;
- confirmation that the SIF performs as specified on invalid process variable values (e.g., out of range);
- the proper shutdown sequence is activated;
- the SIS provides the proper annunciation and proper operation display;
- computations that are included in the SIS are correct for expected range of values but also at limits and over the limits;
- the SIS reset functions perform as defined in the SRS;
- bypass functions operate correctly;
- start-up overrides operate correctly;
- manual shutdown systems operate correctly;
- the proof-test policy documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- confirmation that the SIS performs as required on loss of utilities (e.g., electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the SIS returns to the desired state;
- confirmation that the EMC immunity, as specified in the SRS (see 10.3), has been achieved.

15.2.5 The validation of the application program shall determine whether:

- all of the specified application program safety requirements (see 10.3.2) are correctly performed;
- the application program does not jeopardize the safety requirements under SIS fault conditions and in degraded modes of operation and for BPCS fault conditions for any interfaces between the SIS and BPCS;
- the application program does not jeopardize the safety requirements by executing ''unused'' software functionality, i.e., functionality not defined in the specification.

The information of the validation activities shall be available.

15.2.6 The results from the validation plan activities shall represent and cover the entire SIS validation process. SIS validation documentation shall be produced which provides:

- the version of the SIS validation planning being used;
- the SIF(s) under test (or analysis), along with the specific reference to the requirement identified during the SIS validation planning;
- tools and equipment used, along with their calibration data;
- the results of each test;
- the version of the test specification used;
- the criteria for acceptance of the completed tests;
- the version of the SIS hardware, application program(s), and other software being tested;
- any discrepancy between expected and actual results and the resolution of that discrepancy;

- the analysis made and the decisions taken on whether to continue the test or to issue a change request, in the case where discrepancies occur.

15.2.7 The results shall be verified against the expected results. All discrepancies shall be analysed and the findings shall be available as part of the validation documentation. This shall include the analysis made and the decisions taken on whether to continue the validation or to issue a change request and to return to an earlier part of the development life-cycle.

15.2.8 After the SIS validation and prior to the identified hazards being present, the following activities shall be carried out:

- all bypass functions (e.g., PE logic solver and PE sensor forces, disabled alarms) shall be returned to their normal position;
- all process isolation valves shall be set according to the process start-up requirements and procedures;
- all test materials (e.g., fluids) shall be removed;
- all commissioning overrides and force permissives shall be removed.

16 SIS operation and maintenance

16.1 Objectives

The objectives of the requirements of Clause 16 are to ensure that:

- the required SIL of each SIF is maintained during operation and maintenance;
- the SIS is operated and maintained in a way that sustains the required safety integrity.

16.2 Requirements

16.2.1 Operation and maintenance planning for the SIS shall be carried out. It shall provide the following:

- routine and abnormal operation activities;
- inspection, proof testing, preventive and breakdown maintenance activities;
- the procedures, measures and techniques to be used for operation and maintenance;
- the operational response to faults and failures identified by diagnostics, inspections or proof-tests;
- verification of conformity to operations and maintenance procedures;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities;
- a SIS maintenance plan.

NOTE The SIS maintenance plan can state different maintenance features depending on the SIL level.

16.2.2 Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:

a) the routine methods and procedures which need to be carried out to maintain the "as designed" functional safety of the SIS;

b) the procedures used to ensure the quality and consistency of proof testing, and to ensure adequate validation is being performed after replacement of any device;

c) the measures and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (e.g., when a system needs to be bypassed for testing or maintenance, what additional risk reduction needs to be implemented);

d) the methods and procedures which are used to test the diagnostics;

e) the information which needs to be maintained on SIS failure and the demand rates on the SIS;

f) procedures for collecting data related to the demand rate and SIS reliability parameters;

NOTE 1 Collection and analysis of failure data has many benefits including the potential to reduce maintenance costs if failures rates in operation are significantly lower than what were predicted during design. Implementation costs of new installations can also be reduced because new designs can be based on less conservative failure rates.

g) the information which needs to be maintained showing results of audits and tests on the SIS;

h) the maintenance procedures to be followed when faults or failures occur in the SIS, including:

- procedures for fault diagnostics and repair;
- procedures for revalidation;
- maintenance reporting requirements;
- procedures for tracking maintenance performance.

NOTE 2 Considerations include:

– procedures for reporting failures;

– procedures for analysing systematic failures;

– the actions to allow safe shutdown in the event of BPCS failure;

– ensuring that test equipment is properly calibrated and maintained.

16.2.3 Operation procedures shall be made available. Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.). The operator shall be provided with information on the procedures to be applied before and during bypass and what should be done before the removal of the bypass and the maximum time allowed to be in the bypass state. This information shall be reviewed on a regular basis.

NOTE The operating and maintenance procedures can include verification that bypasses are removed after proof testing.

16.2.4 Continued process operation with a SIS device in bypass shall only be permitted if a hazards analysis has determined that compensating measures are in place and that they provide adequate risk reduction. Operating procedures shall be developed accordingly.

16.2.5 Operation and maintenance shall proceed in accordance with the relevant procedures.

16.2.6 Operators shall be trained on the function and operation of the SIS in their area. This training shall ensure that they understand:

- how the SIS functions (trip points and the resulting action that is taken by the SIS);

NOTE 1 This can also include impact of an SIS action to remaining operational plant.

- the hazard the SIS is protecting against;
- the correct operation and management of all bypass/override switches and under what circumstances these bypasses are to be used;
- the operation of any manual shutdown switches and manual start-up activity and when these manual switches are to be activated;

NOTE 2 This can include “system reset” and “system restart”.

- expectation on activation of any diagnostic alarms (e.g., what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS);
- the proper verification of the diagnostics.

16.2.7 The status of all bypasses shall be recorded in a bypass log. All bypasses need authorization and indication.

16.2.8 Maintenance personnel shall be trained as required to sustain full functional performance of the SIS (hardware and software) to meet the target SIL of each SIF.

16.2.9 Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:

- the demand rate on each SIF (see 5.2.5.3);
- the actions taken following a demand on the system;
- the failures and failure modes of equipment forming part of the SIS, including those identified during normal operation, inspection, testing or demand on a SIF;
- the cause of the demands;
- the cause and frequency of spurious trips;
- the failure of equipment forming part of any compensating measures.

16.2.10 The operation and maintenance procedures may require revision, if necessary, following:

- functional safety audits;
- tests on the SIS;
- experience from normal or abnormal operation and maintenance events.

16.2.11 Written proof-test procedures shall be developed for every SIF to reveal dangerous failures undetected by diagnostics. These written test procedures shall describe every step that is to be performed and shall include:

- the correct operation of each sensor and final element;
- correct logic action;
- correct alarms and indications.

NOTE The following methods can be used to determine the undetected failures that need to be tested:

– examination of fault trees;

– failure mode and effect analysis;

– reliability centred maintenance.

16.2.12 SIS spare parts shall be identified and shall be made available to minimize the bypass duration due to unavailability of any replacement part for the SIS.

NOTE Replacements that are not in kind (like for like) can be managed as a modification to the SIS.

16.2.13 Persons responsible for operations and maintenance shall review the hazard and risk analysis, allocation and design to ensure the assumptions made are valid e.g. assumptions on occupancy and corrosion protection.

16.3 Proof testing and inspection

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.

NOTE 1 Particular attention can be made to identify failure causes that may lead to common cause failures.

NOTE 2 Functional test procedures can also emphasize the need to avoid introducing common cause failures.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).

NOTE Testing of the SIS can be performed either end-to-end or in segments (see 11.8.1).

16.3.1.3 The schedule for the proof tests shall be according to the SRS. The frequency of proof tests for a SIF shall be determined through PFD_{avg} or PFH calculation in accordance with 11.9 for the SIS as installed in the operating environment.

NOTE Different parts of the SIS can require different test intervals, for example, the logic solver can require a different test interval than the sensors or final elements.

16.3.1.4 Any deficiencies found during the proof testing shall be repaired in a safe and timely manner. A proof test shall be repeated after the repair is completed.

16.3.1.5 At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.

NOTE The user can adjust the test frequency based on this data and an analysis of the original basis for test frequency.

16.3.1.6 Any change to the application program requires full validation and a proof test of any SIF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were designed per the updated safety requirements and correctly implemented.

16.3.1.7 Suitable management procedures shall be applied to review deferrals and prevent significant delay to proof testing.

16.3.2 Inspection

Each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (e.g., missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation).

NOTE These problems could indicate an increase in the frequency of faults.

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

a) description of the tests and inspections performed including identification of the test procedure used;

b) dates of the tests and inspections;

c) name of the person(s) who performed the tests and inspections;

d) serial number or other unique identifier of the system tested (e.g., loop number, tag number, equipment number, and SIF number);

e) results of the tests and inspection including the “as-found” condition, all faults found (including the failure mode) and the "as-left" condition.

17 SIS modification

17.1 Objectives

The objectives of the requirements of Clause 17 are:

- that modifications to any SIS are properly planned, reviewed, approved and documented prior to making the change;
- to ensure that the required safety integrity of the SIS is maintained despite of any changes made to the SIS.

NOTE Modifications to the BPCS, other equipment, process or operating conditions can be reviewed to determine whether they are such that the nature or frequency of demands on the SIS will be affected. Those having an adverse effect can be considered further to determine whether the level of risk reduction will still be sufficient.

17.2 Requirements

17.2.1 Prior to carrying out any modification to a SIS, procedures for authorizing and controlling changes shall be in place.

17.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and the hazards that may be affected.

17.2.3 Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification could impact safety then there shall be a return to the first phase of the SIS safety life-cycle affected by the modification.

17.2.4 Safety planning for the modification and re-verification shall be available. Modifications and re-verifications shall be carried out in accordance with the planning.

17.2.5 All documentation affected by the modification shall be updated.

17.2.6 Modification activity shall not begin until a FSA is completed in accordance with 5.2.6.1.9 and after proper authorisation.

17.2.7 Appropriate information shall be maintained for all changes to the SIS. The information shall include:

- a description of the modification or change;
- the reason for the change;
- identified hazards and SIFs which may be affected;
- an analysis of the impact of the modification activity on the SIS;
- all approvals required for the changes;
- tests used to verify that the change was properly implemented and the SIS performs as required;
- details of all SIS modification activities (e.g., a modification log);
- appropriate configuration history;
- tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.

17.2.8 Modification shall be performed with qualified personnel who have been properly trained. All affected and appropriate personnel should be notified of the change and trained with regard to the change.

18 SIS decommissioning

18.1 Objectives

The objectives of the requirements of Clause 18 are to ensure that:

- prior to decommissioning any SIS from active service, a proper review is conducted and required authorization is obtained;
- the required SIF(s) remain operational during decommissioning activities.

18.2 Requirements

18.2.1 Prior to carrying out any decommissioning of part or all of a SIS or SIF, procedures for authorizing and controlling changes shall be in place.

18.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and identifying the hazards that may be affected.

18.2.3 An analysis shall be carried out on the impact on functional safety as a result of the proposed decommissioning activity. The assessment shall include an update of the H&RA sufficient to determine the scope of impact to the SIS safety life cycle. The subsequent SIS safety life-cycle phases shall need to be re-evaluated. The assessment shall also consider:

- functional safety during the execution of the decommissioning activities;
- the impact of decommissioning the SIS on adjacent operating units and facility services.

18.2.4 The results of the impact analysis shall be used during safety planning to re-implement the relevant requirements of the IEC 61511 series including re-verification and re-validation.

18.2.5 Decommissioning activities shall not begin without proper documentation and authorization.

19 Information and documentation requirements

19.1 Objectives

The objectives of the requirements of Clause 19 are to ensure that the necessary information is available and documented in order that:

- all phases of the SIS safety life-cycle can be effectively performed;
- verification, validation and FSA activities can be effectively performed.

19.2 Requirements

19.2.1 The documentation required by the IEC 61511 series shall be available to personnel implementing the requirements of the IEC 61511 series.

19.2.2 The documentation shall:

- describe the installation, system or equipment and the use of it;
- be accurate and up to date;
- be easy to understand;
- suit the purpose for which it is intended;
- be available in an accessible, maintainable and editable form, so that appropriate and relevant documents can be readily and accurately identified, located, retrieved and revised.

NOTE Further details of the requirements for information are included in Clause 14 and Clause 15.

19.2.3 The documentation shall have unique identities so it shall be possible to reference the different parts.

19.2.4 The documentation shall have designations indicating the type of information.

19.2.5 The documentation shall be traceable to the functional and integrity requirements arising from this standard, including the H&RA.

19.2.6 The documentation shall have a revision index (for example, version numbers) to make it possible to identify different versions of the information.

19.2.7 The documentation shall be structured to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document.

NOTE The physical structure of the documentation can vary depending upon a number of factors such as the size of the system, its complexity and the organizational requirements.

19.2.8 All relevant documentation shall be revised, amended, reviewed, approved and shall be under the control of an appropriate information control scheme.

19.2.9 Current documentation pertaining to the following shall be maintained:

a) the results of the H&RA and the related assumptions;
b) the equipment used for SIF together with its safety requirements;
c) the organization responsible for maintaining functional safety;
d) the procedures necessary to achieve and maintain functional safety of the SIS;
e) the modification information as defined in 17.2.5;
f) the safety manual(s);
g) design, implementation, test and validation.

NOTE Further details of the requirements for information are included in 12.4.2, Clauses 14 and 15 and in 16.3.3.

Bibliography

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at <http://www.electropedia.org/)

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

IEC 60300-3-2:2004, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60605-4:2001, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60617-12:1997, *Graphical symbols for diagrams – Part 12: Binary logic elements*[1]

IEC TS 61000-1-2:2008, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61131-3:2013, *Programmable controllers – Part 3: Programming language*

IEC 61131-6:2012, *Programmable controllers – Part 6: Functional Safety*

IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

IEC 61511-3:__, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443-2-1:2010, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC 62682:2014, *Management of alarms for the process industry*

ISO/IEC 2382:2006, *Information technology – Vocabulary*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

[1] Withdrawn.

ISO/IEC 90003:2014, *Software engineering – Part 3: Guidelines for the application of ISO 9001:2000 to computer software*

ISO 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

ISO 9001:2008, *Quality management systems – Requirements*

ISO TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

ISO 13849-1:2006, *Safety of machinery – Safety related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety related parts of control systems – Part 2: Validation*

ISO 14224:2006, *Petroleum, petrochemical and natural gas industries- Collection and exchange of reliability and maintenance of data for equipment*

ISA TR 84.00.04 Part 1:2015, *Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

ISA TR 84.00.09:2013, *Security Countermeasures Related to Safety Instrumented Systems (SIS)*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITE FONCTIONNELLE – SYSTÈMES INSTRUMENTES DE SÉCURITÉ POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION –

Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61511-1 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 2003. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- remplacement des références et exigences logiciel par des références et exigences de programmation d'application;
- exigences d'évaluation de la sécurité fonctionnelle décrites avec plus de détails pour améliorer la gestion de la sécurité fonctionnelle.
- ajout de la gestion des exigences de changement;
- ajout des exigences d'évaluation du risque de sécurité;
- extension des exigences au système de base de contrôle de processus comme couche de protection;
- modification des exigences relatives à la tolérance de panne matérielle et réexamen minutieux pour comprendre les options utilisateurs/intégrateurs.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/777/FDIS	65A/784/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 61511, publiées sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

Le contenu du corrigendum de septembre 2016 a été pris en considération dans cet exemplaire.

INTRODUCTION

Les systèmes instrumentés de sécurité (SIS, Safety Instrumented System) sont utilisés dans les industries de transformation depuis de nombreuses années pour remplir des fonctions instrumentées de sécurité (SIF, Safety Instrumented Function). Si l'instrumentation doit être effectivement utilisée pour réaliser des SIF, il est essentiel que cette instrumentation satisfasse à certaines normes et certains niveaux de performance minimaux.

La série IEC 61511 concerne l'application des SIS aux industries de transformation. La série IEC 61511 porte également sur la réalisation d'une analyse de danger et de risque relative au processus (H&RA) visant à en déduire la spécification relative aux SIS. D'autres contributions du système de sécurité sont uniquement prises en compte eu égard aux exigences de performance du SIS. Le SIS inclut tous les appareils nécessaires à l'acheminement de la SIF entre le capteur et l'élément terminal.

La série IEC 61511 aborde deux concepts essentiels à son application: le cycle de vie de sécurité des SIS et les niveaux d'intégrité de sécurité (SIL).

La série IEC 61511 concerne les SIS reposant sur l'utilisation d'une technologie électrique/électronique/électronique programmable. Si d'autres technologies sont utilisées pour les unités logiques, il convient d'appliquer les principes de base de la série IEC 61511 pour garantir que les exigences de sécurité fonctionnelle soient satisfaites. La série IEC 61511 concerne également les capteurs et les éléments terminaux des SIS, quelle que soit la technologie utilisée. La série IEC 61511 est propre aux industries de transformation, dans le cadre de la série IEC 61508.

La série IEC 61511 définit une approche concernant les activités relatives au cycle de vie de sécurité des SIS dans le but de satisfaire à ces principes minimaux. Cette approche a été adoptée afin de mettre en œuvre une politique technique cohérente et rationnelle.

Dans la plupart des cas, la sécurité est obtenue de la meilleure façon par une conception de processus à sécurité intrinsèque. Toutefois, dans certains cas, cela s'avère impossible ou peu pratique. Si nécessaire, cette approche peut être combinée à un ou plusieurs systèmes de protection afin de couvrir les risques résiduels identifiés éventuels. Les systèmes de protection peuvent reposer sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). Pour faciliter cette approche, la série IEC 61511:

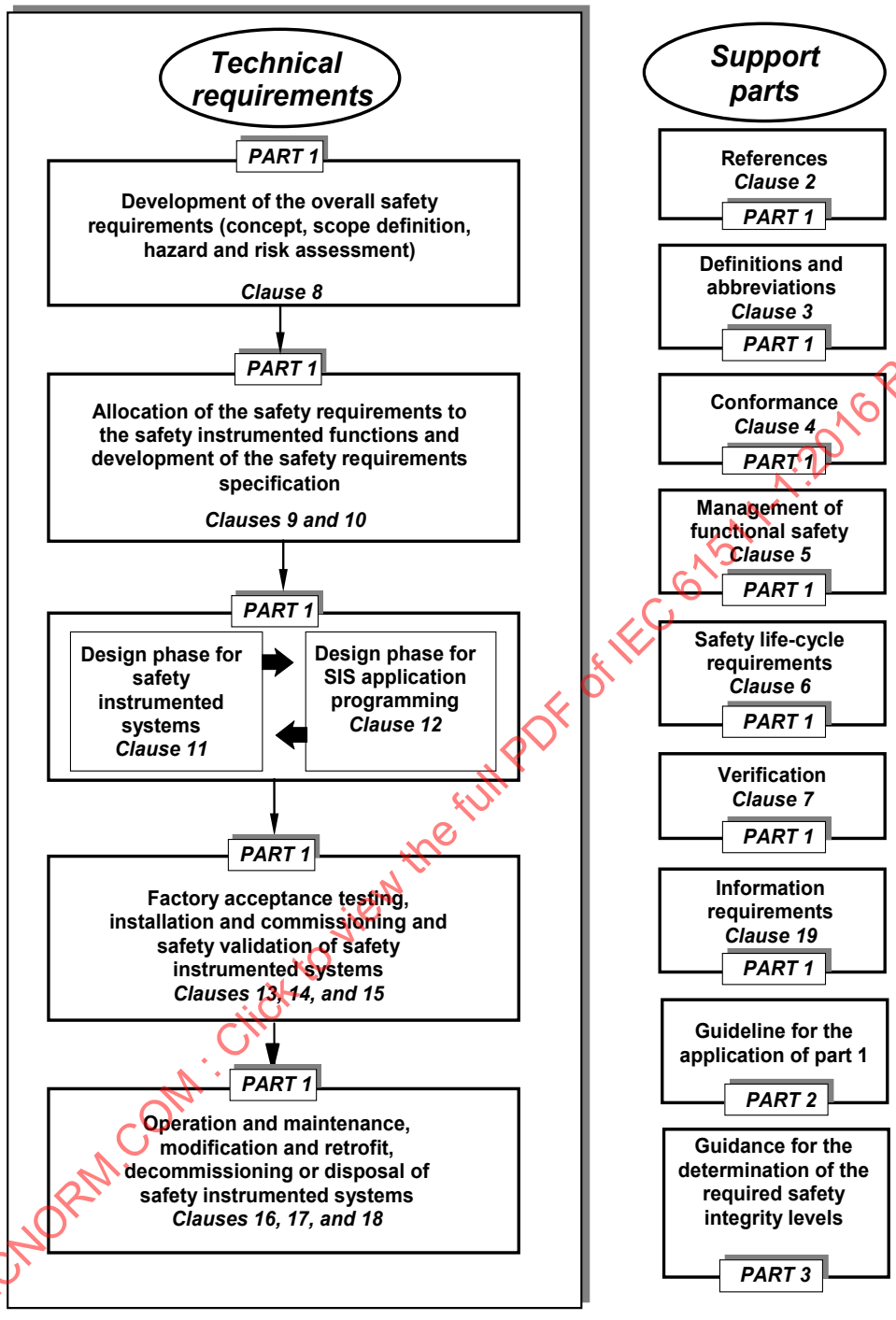
- aborde la réalisation d'une analyse de danger et de risque pour identifier les exigences de sécurité globales;
- prend en compte l'affectation des exigences de sécurité aux SIS;
- s'inscrit dans un cadre applicable à tous les moyens instrumentés qui permettent d'obtenir la sécurité fonctionnelle;
- détaille l'utilisation de certaines activités, telles que la gestion de la sécurité, qui peuvent être applicables à toute méthode permettant d'obtenir la sécurité fonctionnelle.

La série IEC 61511 relative aux SIS pour les industries de transformation:

- prend en compte toutes les phases relatives au cycle de vie de sécurité des SIS (concept initial, conception, mise en œuvre, fonctionnement, maintenance et déclassement);
- permet d'harmoniser les normes des industries de transformation nationales existantes ou nouvelles par rapport à la série IEC 61511.

L'IEC 61511 vise à obtenir un haut niveau de cohérence (p. ex.: des principes sous-jacents, de la terminologie et de l'information) dans le secteur des industries de transformation. Il convient de noter que cela présente des avantages tant du point de vue de la sécurité que du point de vue économique. La Figure 1 ci-dessous présente un cadre général de la série IEC 61511.

Dans les juridictions où les autorités compétentes (p. ex.: nationales, fédérales, étatiques, provinciales, cantonales, municipales) ont défini des réglementations relatives à la conception de la sécurité des processus, la gestion de la sécurité des processus ou autres, ces réglementations sont prioritaires par rapport aux exigences définies dans la série IEC 61511.



Anglais	Français
Technical requirements	Exigences techniques
PART 1	PARTIE 1
PART 2	PARTIE 2
PART 3	PARTIE 3
Development of the overall safety requirements (concept, scope definition, hazard and risk assessment) Clause 8	Développement des exigences de sécurité globales (concept, définition du domaine d'application, analyse de danger et de risque) Article 8
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification Clauses 9 and 10	Allocation des exigences de sécurité aux fonctions instrumentées de sécurité et développement de la spécification des exigences de sécurité Articles 9 et 10
Design phase for safety instrumented systems Clause 11	Phase de conception pour les systèmes instrumentés de sécurité Article 11
Design phase for SIS application programming Clause 12	Phase de conception pour la programmation d'application du SIS Article 12
Factory acceptance testing, installation and commissioning and safety validation of safety instrumented systems Clauses 13, 14, and 15	Essais de réception en usine, installation et mise en service, et validation de la sécurité des systèmes instrumentés de sécurité Articles 13, 14, et 15
Operation and maintenance, modification and retrofit, decommissioning or disposal of safety instrumented systems Clauses 16,17, and 18	Fonctionnement et maintenance, modification et remise à niveau, déclassement ou mise au rebut des systèmes instrumentés de sécurité Articles 16, 17, et 18
Support parts	Parties de prise en charge
References Clause 2	Références Article 2
Definitions and abbreviations Clause 3	Définitions et abréviations Article 3
Conformance Clause 4	Conformité Article 4
Management of functional safety Clause 5	Gestion de la sécurité fonctionnelle Article 5
Safety life-cycle requirements Clause 6	Exigences relatives au cycle de vie de sécurité Article 6
Verification Clause 7	Vérification Article 7
Information requirements Clause 19	Exigences relatives aux informations Article 19
Guideline for the application of part 1	Ligne directrice pour l'application de la partie 1
Guidance for the determination of the required safety integrity levels	Ligne directrice pour la détermination des niveaux d'intégrité de sécurité exigés

Figure 1 – Cadre général de la série IEC 61511

SÉCURITE FONCTIONNELLE – SYSTÈMES INSTRUMENTES DE SÉCURITÉ POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION –

Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

1 Domaine d'application

La présente partie de l'IEC 61511décrit les exigences relatives à la spécification, la conception, l'installation, au fonctionnement et à la maintenance d'un système instrumenté de sécurité (SIS, Safety Instrumented System) de manière à ce qu'il puisse être mis en œuvre en toute confiance pour établir ou maintenir le processus dans un état de sécurité convenable. L'IEC 61511-1 a été conçue pour être une mise en œuvre de l'IEC 61508:2010 dans le secteur des industries de transformation.

En particulier, l'IEC 61511-1:

a) spécifie les exigences permettant d'obtenir la sécurité fonctionnelle, mais ne spécifie pas la responsabilité de la mise en œuvre des exigences (p. ex.: les concepteurs, les fournisseurs, la société propriétaire/exploitante, l'entrepreneur). Cette responsabilité sera assignée aux différentes parties selon la planification de la sécurité, la planification et la gestion de projets, ainsi que les règlements nationaux;

b) s'applique lorsque des appareils satisfaisant aux exigences de la série IEC 61508 parue en 2010 ou de l'IEC 61511-1:2016 [11.5] sont intégrés dans un système qui doit être utilisé pour une application du secteur des industries de transformation. Elle ne concerne pas les fabricants qui souhaitent revendiquer la possibilité d'utiliser ces appareils dans les SIS du secteur des industries de transformation (voir l'IEC 61508-2:2010 et l'IEC 61508-3:2010);

c) définit les relations entre les normes IEC 61511 et IEC 61508 (voir Figures 2 et 3);

d) s'applique lorsque des programmes d'application sont développés pour des systèmes possédant un langage de variabilité limitée ou lors de l'utilisation d'appareil à langage de programmation figé, mais ne s'applique pas aux fabricants, concepteurs, intégrateurs et utilisateurs du SIS qui développent des logiciels intégrés (logiciels système) ou utilisent des langages de variabilité totale (voir l'IEC 61508-3:2010);

e) s'applique à de nombreuses industries de transformation (p. ex.: produits chimiques, pétrole et gaz, pâte à papier et papier, produits pharmaceutiques, produits alimentaires et boissons, production d'électricité non-nucléaire);

NOTE 1 Dans le secteur des industries de transformation, certaines applications peuvent faire l'objet d'exigences supplémentaires qui doivent être satisfaites.

f) met en évidence les relations entre les SIF et d'autres fonctions instrumentées (voir Figure 4);

g) aboutit à l'identification des exigences fonctionnelles et des exigences concernant l'intégrité de sécurité relatives aux SIF en tenant compte de la réduction de risque obtenue par d'autres méthodes;

h) spécifie les exigences relatives au cycle de vie de l'architecture du système et la configuration du matériel, ainsi que de la programmation d'application et de l'intégration du système;

i) spécifie les exigences relatives à la programmation d'application pour les intégrateurs et utilisateurs de SIS;

j) s'applique lorsque la sécurité fonctionnelle est obtenue en utilisant une ou plusieurs SIF pour la protection du personnel, la protection du grand public ou la protection de l'environnement;

k) peut s'appliquer dans des applications non liées à la sécurité (la protection de biens, par exemple);

l) définit les exigences pour la mise en œuvre des SIF dans le cadre des dispositions globales permettant d'obtenir la sécurité fonctionnelle;

m) utilise le cycle de vie de sécurité d'un SIS (voir Figure 7) et définit une liste des activités devant être réalisées pour déterminer les exigences fonctionnelles, ainsi que les exigences concernant l'intégrité de sécurité relatives au SIS;

n) spécifie qu'une H&RA doit être réalisée pour définir les exigences de sécurité fonctionnelle et les niveaux d'intégrité de sécurité (SIL) de chaque SIF;

NOTE 2 Pour avoir une vue d'ensemble des moyens de réduction de risque, voir la Figure 9.

o) établit des objectifs quantitatifs relatifs à la probabilité moyenne de défaillance en cas de sollicitation (en mode sollicitation) et à la fréquence moyenne de défaillance dangereuse (en mode sollicitation ou en mode continu) pour chaque SIL;

p) spécifie des exigences minimales pour la tolérance aux défauts du matériel (HFT);

q) spécifie les mesures et techniques exigées pour obtenir le SIL indiqué;

r) définit un niveau maximal de performance de sécurité fonctionnelle (SIL 4) qui peut être atteint pour une SIF mise en œuvre conformément à l'IEC 61511-1;

s) définit un niveau minimal de performance de sécurité fonctionnelle (SIL 1) au-dessous duquel l'IEC 61511-1 ne s'applique pas;

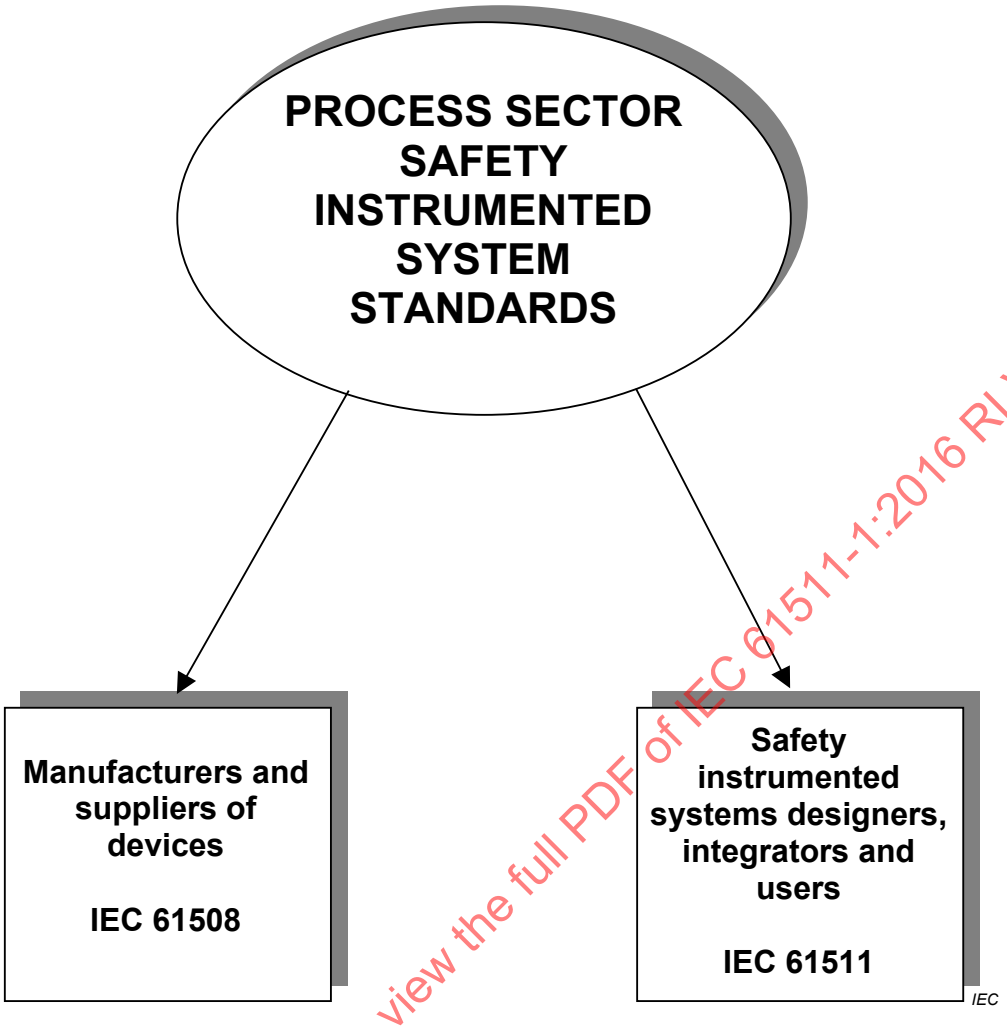
t) fournit un cadre pour l'établissement du SIL, mais ne spécifie pas le SIL exigé pour les applications spécifiques (qu'il convient d'établir sur la base de la connaissance de l'application particulière et par rapport à la réduction de risque globale souhaitée);

u) spécifie les exigences pour toutes les parties du SIS, depuis le capteur jusqu'à l'élément terminal ou jusqu'aux éléments terminaux;

v) définit les informations qui sont nécessaires pendant le cycle de vie de sécurité du SIS;

w) spécifie que la conception du SIS tient compte des facteurs humains;

x) n'applique aucune exigence directe relative à l'opérateur individuel ou au technicien de maintenance.



Anglais	Français
PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS	NORMES RELATIVES AUX SYSTEMES INSTRUMENTES DE SECURITE DANS LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
Manufacturers and suppliers of devices	Fabricants et fournisseurs d'appareils
IEC 61508	IEC 61508
Safety instrumented systems designers, integrators and users	Concepteurs, intégrateurs et utilisateurs de systèmes instrumentés de sécurité
IEC 61511	IEC 61511

Figure 2 – Relations entre l'IEC 61511 et l'IEC 61508

NOTE 3 L'IEC 61508 est également utilisée par les concepteurs, intégrateurs et utilisateurs de SIS lorsque cela est indiqué dans l'IEC 61511.

- remplacement des références et exigences logiciel par des références et exigences de programmation d'application;
- exigences d'évaluation de la sécurité fonctionnelle décrites avec plus de détails pour améliorer la gestion de la sécurité fonctionnelle.
- ajout de la gestion des exigences de changement;
- ajout des exigences d'évaluation du risque de sécurité;
- extension des exigences au système de base de contrôle de processus comme couche de protection;
- modification des exigences relatives à la tolérance de panne matérielle et réexamen minutieux pour comprendre les options utilisateurs/intégrateurs.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/777/FDIS	65A/784/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 61511, publiées sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

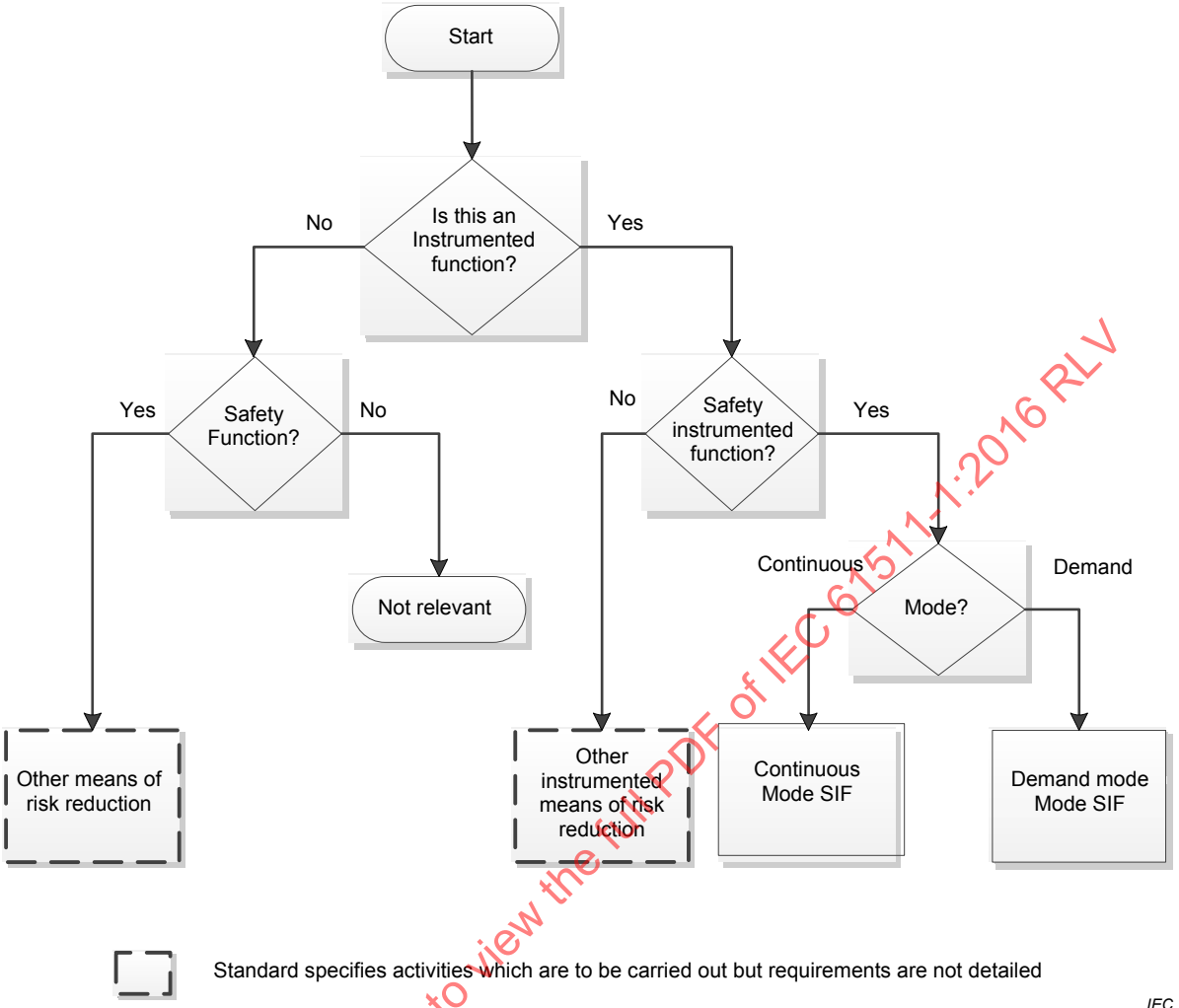
- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

Le contenu du corrigendum de septembre 2016 a été pris en considération dans cet exemplaire.

Anglais	Français
PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS	NORMES RELATIVES AUX SYSTEMES INSTRUMENTES DE SECURITE DANS LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
PROCESS SECTOR HARDWARE	MATERIEL POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
PROCESS SECTOR SOFTWARE & APPLICATION PROGRAM	LOGICIEL ET PROGRAMME D'APPLICATION POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
DEVELOPING NEW HARDWARE DEVICES	DEVELOPPEMENT DE NOUVEAUX APPAREILS MATERIELS
FOLLOW IEC 61508	SUIVRE L'IEC 61508
USING PRIOR USE HARDWARE DEVICES	UTILISATION D'APPAREILS MATERIELS BASES SUR L'UTILISATION ANTERIEURE
FOLLOW IEC 61511	SUIVRE L'IEC 61511
USING HARDWARE DEVELOPED AND ASSESSED ACCORDING TO IEC 61508	UTILISATION DE MATERIEL DEVELOPPE ET EVALUE CONFORMEMENT A L'IEC 61508
DEVELOPING EMBEDDED (SYSTEM) SOFTWARE	DEVELOPPEMENT DE LOGICIELS (SYSTEME) INTEGRES
FOLLOW IEC 61508-3	SUIVRE L'IEC 61508-3
DEVELOPING APPLICATION PROGRAM USING FULL VARIABILITY LANGUAGES	DEVELOPPEMENT DE PROGRAMME D'APPLICATION UTILISANT DES LANGAGES DE VARIABILITE TOTALE
DEVELOPING APPLICATION PROGRAM USING LIMITED VARIABILITY OR FIXED PROGRAM LANGUAGES	DEVELOPPEMENT DE PROGRAMME D'APPLICATION UTILISANT DES LANGAGES DE VARIABILITE LIMITEE OU DES LANGAGES DE PROGRAMME FIGE

Figure 3 – Relations détaillées entre l'IEC 61511 et l'IEC 61508

NOTE 4 Pour connaître les lignes directrices concernant le traitement de l'intégration des sous-systèmes qui satisfont à d'autres normes (machines, brûleur, etc.), voir 7.2.2 de l'IEC 61511-1:2016 et l'IEC 61511-2:2016.



Anglais	Français
Start	Démarrage
Is this an Instrumented function?	Est-ce une fonction instrumentée?
No	Non
Yes	Oui
Safety Function?	Fonction de sécurité?
Safety instrumented function?	Fonction instrumentée de sécurité?
Not relevant	Non pertinent
Mode?	Mode?
Continuous	Continu
Demand	Sollicitation
Other means of risk reduction	Autres moyens de réduction de risque
Other instrumented means of risk reduction	Autres moyens instrumentés de réduction de risque
Continuous Mode SIF	SIF en mode continu
Demand mode Mode SIF	SIF en mode sollicitation
Standard specifies activities which are to be carried out but requirements are not detailed	La norme spécifie les activités devant être réalisées, mais les exigences ne sont pas détaillées

Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

3 Termes, définitions et abréviations

3.1 Termes

Les termes figurent dans l'ordre alphabétique en 3.2.

3.2 Termes et définitions

Pour les besoins du présent document, les définitions suivantes s'appliquent.

Dans certains cas, ces définitions diffèrent de celles correspondant aux mêmes termes dans l'IEC 61508-4:2010. Dans certains cas, cela est dû à la terminologie utilisée dans le secteur des industries de transformation. Dans d'autres cas, ces définitions ont été alignées avec d'autres références définitives pertinentes (p. ex.: l'IEC 60050, le Vocabulaire Electrotechnique International, l'ISO/IEC Guide 51:2013). Toutefois, sauf indication contraire, il n'existe aucune différence de signification technique entre ces définitions et celles des mêmes termes dans l'IEC 61508-4:2010.

3.2.1
architecture
configuration
configuration spécifique des éléments matériels et logiciels dans un système

Note 1 à l'article: Dans la série IEC 61511, cela peut signifier, par exemple, la disposition des sous-systèmes SIS, la structure interne d'un sous-système SIS ou la structure interne des programmes d'application du SIS.

3.2.2
protection de biens
fonction allouée à la conception d'un système dans le but de prévenir la perte ou l'endommagement de biens

3.2.3
système de commande de processus de base
BPCS
système qui répond aux signaux d'entrée provenant du processus, de ses équipements associés, d'autres systèmes programmables et/ou des opérateurs, et qui génère des signaux de sortie faisant fonctionner le processus et ses équipements associés de la manière souhaitée, mais qui n'exécute aucune fonction instrumentée de sécurité (SIF)

Note 1 à l'article: Un BPCS inclut tous les appareils nécessaires pour s'assurer que le processus fonctionne de la manière souhaitée.

Note 2 à l'article: Un BPCS peut habituellement mettre en œuvre différentes fonctions (p. ex.: fonctions de commande de processus, surveillance, et alarmes).

Note 3 à l'article: L'abréviation «BPCS» est dérivée du terme anglais développé correspondant «basic process control system».

3.2.4
dérivation
action ou installation empêchant l'exécution de tout ou partie des fonctionnalités du SIS

Note 1 à l'article: Des exemples de dérivation incluent ce qui suit:

– le signal d'entrée en provenance du circuit de déclenchement est bloqué, mais les paramètres d'entrée et l'alarme sont toujours présentés à l'opérateur;
– le signal de sortie du circuit de déclenchement à un élément terminal est maintenu à l'état normal empêchant le fonctionnement de l'élément terminal;
– une ligne de dérivation physique est fournie autour de l'élément terminal;
– un état d'entrée présélectionné (p. ex.: acheminer/arrêter le signal d'entrée) ou un ensemble de paramètres est forcé par l'intermédiaire d'un outil d'ingénierie (p. ex.: dans le programme d'application).

Note 2 à l'article: La notion de dérivation est également rendue par d'autres termes (p. ex.: neutralisation, mise en échec, désactivation, forçage, inhibition, shuntage ou blocage).

3.2.5
canal
appareil ou groupe d'appareils exécutant une fonction indépendante spécifique

Note 1 à l'article: Les appareils d'un canal peuvent comporter des appareils d'entrée et de sortie (E/S), des unités logiques, des capteurs et des éléments terminaux.

Note 2 à l'article: Une configuration à double canal (à deux canaux) comprend deux canaux réalisant indépendamment la même fonction. Les canaux peuvent être identiques ou différents.

Note 3 à l'article: Ce terme peut être utilisé pour décrire un système complet ou une partie seulement d'un système (p. ex.: les capteurs ou les éléments terminaux).

Note 4 à l'article: Un canal décrit les éléments architecturaux matériels d'un SIS souvent utilisés pour satisfaire aux exigences de tolérance aux défauts du matériel.

3.2.6
cause commune

3.2.6.1
défaillances de cause commune, pl
défaillances concomitantes affectant plusieurs appareils, qui proviennent d'un événement unique et ne résultent pas les unes des autres

Note 1 à l'article: Toutes les défaillances résultant d'une cause commune ne se produisent pas nécessairement exactement à la même heure, et cela peut laisser du temps pour détecter l'occurrence de la cause commune avant qu'un SIF ne subisse réellement une défaillance.

Note 2 à l'article: Les défaillances de cause commune peuvent également donner lieu à des défaillances de mode commun.

Note 3 à l'article: La possibilité de défaillances de cause commune réduit l'efficacité de la redondance ou de la tolérance aux anomalies d'un système (p. ex.: augmente la probabilité de défaillance de deux canaux ou plus dans un système multicanal).

Note 4 à l'article: Les défaillances de cause commune sont des défaillances dépendantes. Elles peuvent résulter d'événements extérieurs (p. ex.: température, humidité, surtension, incendie et corrosion), d'erreurs systématiques (p. ex.: erreurs de conception, d'assemblage ou d'installation, bogues), d'erreurs humaines (p. ex.: mauvaise utilisation), etc.

Note 5 à l'article: Par extension, une défaillance de cause commune (au singulier) est une défaillance appartenant à un ensemble de défaillances concomitantes (au pluriel) selon la définition donnée en 3.2.6.1.

3.2.6.2
défaillances de mode commun, pl
défaillances concomitantes affectant plusieurs appareils, caractérisées par le même mode de défaillance (c'est-à-dire des défaillances identiques)

Note 1 à l'article: Les défaillances de mode commun peuvent avoir différentes causes.

Note 2 à l'article: Les défaillances de mode commun peuvent également être le résultat de défaillances de cause commune (3.2.6.1).

Note 3 à l'article: La possibilité de défaillances de mode commun réduit l'efficacité de la redondance ou de la tolérance aux anomalies d'un système (p. ex.: défaillance de deux canaux ou plus de la même manière, ce qui entraîne le même résultat erroné).

Note 4 à l'article: Par extension, une défaillance de mode commun (au singulier) est une défaillance appartenant à un ensemble de défaillances concomitantes (au pluriel) selon la définition donnée en 3.2.6.2.

3.2.7
mesure compensatoire
mise en œuvre temporaire de méthodes planifiées et documentées de gestion des risques au cours d'une période de maintenance ou de fonctionnement du processus lorsque les performances du SIS sont réputées être dégradées

3.2.8
composant
l'une des parties d'un système, d'un sous-système SIS ou d'un appareil, exécutant une fonction spécifique

Note 1 à l'article: Un composant peut également inclure des logiciels.

3.2.9
gestion de configuration
discipline d'identification des composants d'un système évolutif et des dispositions de ces composants ayant pour objectif de maîtriser les modifications de ces composants et de maintenir la continuité du système et la traçabilité des changements apportés tout au long du cycle de vie

3.2.9.1
approche prudente
manière prévoyante de réaliser des analyses et calculs

Note 1 à l'article: Dans le domaine de la sécurité, chaque fois qu'une analyse ou qu'une hypothèse doit être formulée ou qu'un calcul doit être réalisé (concernant des modèles, des données d'entrée, des calculs, etc.), une approche prudente peut être choisie pour s'assurer de produire des résultats pessimistes.

3.2.10
système de commande
système qui réagit à des signaux d'entrée provenant du processus et/ou d'un opérateur et qui produit des signaux de sortie qui font que le processus fonctionne de la manière souhaitée

Note 1 à l'article: Le système de commande comprend des capteurs et des éléments terminaux et peut être soit un BPCS, soit un SIS ou une combinaison des deux.

3.2.11
défaillance dangereuse
défaillance qui neutralise ou désactive une action de sécurité donnée

Note 1 à l'article: Une défaillance est "dangereuse" uniquement au regard d'une SIF donnée.

Note 2 à l'article: Lorsque la tolérance aux anomalies est mise en œuvre, une défaillance dangereuse peut conduire à:

– une SIF dégradée où l'action de sécurité est disponible, mais où il existe une plus grande probabilité de PFD (fonctionnement en mode sollicitation) ou une plus grande probabilité de déclencher un événement dangereux (fonctionnement en mode continu), ou

– une SIF désactivée où l'action de sécurité est complètement désactivée (fonctionnement en mode sollicitation) ou l'événement dangereux a été induit (fonctionnement en mode continu).

Note 3 à l'article: Lorsqu'aucune tolérance aux anomalies n'est mise en œuvre, toutes les défaillances dangereuses conduisent à une SIF désactivée.

3.2.12
défaillance dépendante
défaillance dont la probabilité ne peut pas être exprimée en tant que simple produit des probabilités non conditionnelles de chacun des événements individuels qui l'ont provoquée

Note 1 à l'article: Deux événements A et B sont dépendants si la probabilité d'occurrence de A et B, P(A et B), est supérieure à P(A) × P(B).

Note 2 à l'article: Pour plus d'informations sur les défaillances dépendantes entre les couches de protection, voir 9.4.2 et l'IEC 61511-3:2016, Annexe J.

Note 3 à l'article: Les défaillances dépendantes incluent la cause commune.

3.2.13
détecté
révélé
déclaré
se rapporte aux défaillances ou erreurs du matériel et du logiciel qui ne sont pas cachées, parce qu'elles s'annoncent elles-mêmes ou qu'elles sont détectées lors du fonctionnement normal ou par des méthodes de détection dédiées

Note 1 à l'article: Il existe quelques différences pour l'utilisation de ces adjectifs:

– L'adjectif "déclaré" désigne les défaillances ou erreurs qui s'annoncent elles-mêmes au moment où elles surviennent (p. ex.: du fait du changement d'état). La réparation de telles défaillances peut débuter dès leur occurrence.

– L'adjectif "détecté" désigne les défaillances ou erreurs qui ne s'annoncent pas elles-mêmes au moment où elles surviennent et qui restent cachées jusqu'à ce qu'elles soient détectées par les essais de diagnostic, les essais périodiques ou l'intervention de l'opérateur (p. ex.: examen physique et essais manuels). La réparation de telles défaillances ne peut débuter qu'une fois qu'elles ont été révélées. Pour connaître l'usage spécifique de ce terme dans l'IEC 61511, se reporter à la Note 2.

– L'adjectif "révélé" désigne les défaillances ou erreurs qui deviennent évidentes parce qu'elles sont déclarées ou ont été détectées.

Note 2 à l'article: Dans l'IEC 61511 et excepté lorsque le contexte suggère une autre signification, le terme "défaillances/erreurs détectées dangereuses" se rapporte aux défaillances/erreurs dangereuses détectées par les essais de diagnostic.

Note 3 à l'article: Lorsque la détection est très rapide (p. ex.: essais de diagnostic), les défaillances ou erreurs détectées peuvent être considérées comme des défaillances ou erreurs déclarées.

Lorsque la détection n'est pas très rapide (p. ex.: essais périodiques), les défaillances ou erreurs détectées ne peuvent pas être considérées comme des défaillances ou erreurs déclarées en ce qui concerne les niveaux d'intégrité de sécurité.

Note 4 à l'article: Une défaillance révélée dangereuse peut uniquement être traitée comme une défaillance en sécurité si des mesures efficaces (automatiques ou manuelles) sont mises en œuvre dans un délai suffisamment court pour maintenir la sécurité du processus.

3.2.14
appareil
matériel, avec ou sans logiciel, capable de réaliser une fonction spécifiée

Note 1 à l'article: Des exemples incluent les capteurs, les unités logiques, les éléments terminaux, les interfaces opérateur et les raccordements à l'installation.

3.2.14.1
appareil de terrain
appareil SIS ou BPCS connecté directement au processus ou situé à proximité du processus

Note 1 à l'article: Des exemples incluent les capteurs, les éléments terminaux et les commutateurs manuels.

3.2.15
diagnostic
essai automatique fréquent (lié au temps de sécurité du processus) visant à révéler des défaillances

3.2.15.1
couverture du diagnostic
DC
taux de défaillances dangereuses détectées par les diagnostics. La couverture du diagnostic ne comprend aucune défaillance détectée par les essais périodiques

Note 1 à l'article: La couverture du diagnostic s'applique habituellement aux appareils SIS ou aux sous-systèmes SIS. Par exemple, la couverture du diagnostic est généralement déterminée pour un capteur, un élément terminal ou une unité logique.

Note 2 à l'article: Pour les applications de sécurité, la couverture du diagnostic s'applique habituellement aux défaillances dangereuses des appareils SIS ou des sous-systèmes SIS. Par exemple, la couverture du diagnostic pour les défaillances dangereuses d'un appareil est DC = $\lambda_{DD}/\lambda_{DT}$, où λ_{DD} est le taux de défaillances dangereuses détectées et λ_{DT} est le taux de défaillances dangereuses totales. Pour un sous-système SIS avec redondance interne, DC dépend du temps: $DC(t) = \lambda_{DD}(t)/\lambda_{DT}(t)$.

Note 3 à l'article: Lorsque la couverture du diagnostic (DC) et le taux de défaillances dangereuses totales (λ_{DT}) sont donnés, les taux de défaillances dangereuses détectées (λ_{DD}) et non détectées (λ_{DU}) peuvent être calculés comme suit:

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

Note 4 à l'article: L'abréviation «DC» est dérivée du terme anglais développé correspondant «diagnostics coverage».

3.2.16
diversité
moyens différents pour réaliser une fonction exigée

Note 1 à l'article: La diversité peut être réalisée en utilisant des moyens physiques, des techniques de programmation ou des approches de conception différents.

3.2.17
erreur
écart entre une valeur ou condition calculée, observée ou mesurée et la valeur ou condition vraie, spécifiée ou théoriquement correcte

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

3.2.18
défaillance
perte de l'aptitude à fonctionner tel que requis

Note 1 à l'article: La défaillance d'un appareil est un événement qui provoque un état d'anomalie de cet appareil.

Note 2 à l'article: Lorsque la perte d'aptitude est causée par une panne latente, la défaillance survient lorsqu'un ensemble particulier de circonstances est réuni.

Note 3 à l'article: L'accomplissement des fonctions exigées exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportement à éviter. L'occurrence d'un tel comportement est une défaillance.

Note 4 à l'article: Les défaillances sont soit aléatoires, soit systématiques (voir 3.2.61 et 3.2.83).

[SOURCE: IEC 60050-192:2015, 192-03-01, modifiée – Les notes à l'article ont été modifiées]

3.2.18.1
mode de défaillance
manière selon laquelle une défaillance se produit

Note 1 à l'article: Un mode de défaillance peut être défini par la fonction perdue ou par la transition d'état qui s'est produite.

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

3.2.19
anomalie
inaptitude à fonctionner tel que requis, due à un état interne

Note 1 à l'article: La panne d'une entité est due soit à une défaillance de l'entité elle-même, soit à une imperfection lors d'une étape précédente du cycle de vie, telle que la spécification, la conception, la fabrication ou la maintenance.

Note 2 à l'article: Une panne d'un appareil donne lieu à une défaillance lorsqu'un ensemble particulier de circonstances est réuni.

[SOURCE: IEC 60050-192:2015, 192-04-01, modifiée – Certaines notes à l'article ont été modifiées, d'autres supprimées. "Panne" a été changé en "anomalie"]

3.2.20
évitement des anomalies
utilisation de techniques et procédures destinées à éviter l'apparition d'anomalies durant chacune des phases du cycle de vie de sécurité du SIS

3.2.20.1
exclusion des anomalies
élimination dans les examens futurs d'anomalies résultant de modes de défaillance improbables

Note 1 à l'article: Pour plus d'informations sur l'exclusion des anomalies, l'ISO 13849-1 et l'ISO 13849-2 peuvent être consultées. Outre ces normes, l'exclusion des anomalies peut reposer sur:

– l'improbabilité technique de l'occurrence de certaines anomalies;

– l'expérience technique généralement acceptée, indépendamment de l'application concernée;

– les exigences techniques relatives à l'application et au danger spécifique.

Note 2 à l'article: Les modes de défaillance (identifiés dans les appareils réalisant la fonction de sécurité) peuvent être exclus, car leurs taux de défaillances dangereuses sont très faibles par rapport au niveau objectif de défaillances relatif à la fonction de sécurité à l'étude. Autrement dit, la somme des taux de défaillances dangereuses de tous les appareils en série sur lesquels l'exclusion des anomalies est revendiquée ne peut en général pas être supérieure à 1 % du niveau objectif de défaillances.

3.2.21
tolérance aux anomalies
aptitude d'une entité fonctionnelle à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs

3.2.22
élément terminal
partie du BPCS ou du SIS qui met en œuvre l'action physique nécessaire pour obtenir ou maintenir un état de sécurité

Note 1 à l'article: Des exemples sont les vannes, appareils de commutation et moteurs, comprenant leurs éléments auxiliaires (p. ex.: une électrovanne et un actionneur utilisés pour faire fonctionner une vanne).

3.2.23
sécurité fonctionnelle
sous-ensemble de la sécurité globale se rapportant au processus et au BPCS, qui dépend du fonctionnement correct du SIS et d'autres couches de protection

3.2.24
évaluation de la sécurité fonctionnelle
FSA
recherche, à partir de preuves, destinée à juger de l'état de sécurité fonctionnelle atteint par un ou plusieurs SIS et/ou d'autres couches de protection

Note 1 à l'article: L'abréviation «FSA» est dérivée du terme anglais développé correspondant «functional safety assessment».

3.2.25
audit de la sécurité fonctionnelle
examen systématique et indépendant destiné à déterminer si les procédures spécifiques aux exigences sur la sécurité fonctionnelle sont conformes aux procédures prévues, sont effectivement mises en œuvre et permettent d'atteindre les objectifs spécifiés

Note 1 à l'article: Un audit de la sécurité fonctionnelle peut être mené dans le cadre d'une FSA.

3.2.26
intégrité de sécurité du matériel
partie de l'intégrité de sécurité du SIS liée aux défaillances aléatoires du matériel en mode de défaillance dangereux

Note 1 à l'article: Les deux niveaux de défaillances qui sont pertinents dans ce contexte sont la fréquence moyenne de défaillance dangereuse (fonctionnement en mode continu) et la probabilité moyenne de défaillance en cas de sollicitation (fonctionnement en mode sollicitation).

Note 2 à l'article: Voir 3.2.82.

Note 3 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.27
dommage
blessure ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement

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

3.2.27.1
événement préjudiciable
événement dangereux qui conduit à un dommage

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés à la situation dangereuse et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence. Un événement dangereux qui a conduit à un dommage est appelé "événement préjudiciable".

3.2.28
danger
source potentielle de dommage

Note 1 à l'article: Ce terme comprend le danger sur des personnes survenant dans un court laps de temps (p. ex.: feu ou explosion), et aussi le danger à long terme sur la santé d'une personne (p. ex.: dégagement d'une substance toxique ou radioactivité).

[SOURCE: ISO/IEC Guide 51:2014, 3.2, modifiée – La Note 1 à l'article a été ajoutée]

3.2.28.1
événement dangereux
événement pouvant conduire à un dommage

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés à la situation dangereuse et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence.

[SOURCE: ISO/IEC Guide 51:2014: 3.3, modifiée – voir Note 1]

3.2.28.2
situation dangereuse
situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs dangers

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

3.2.29
erreur humaine
action humaine ou absence d'intervention prévue ou non prévue, qui produit un résultat non approprié

Note 1 à l'article: Les fautes, chutes et inattentions constituent des exemples d'erreurs humaines.

Note 2 à l'article: Les actions malveillantes sont exclues.

3.2.30
analyse d'impact
activité consistant à déterminer l'effet que la modification à une fonction ou à un composant d'un système aura sur les autres fonctions ou les autres composants de ce système tout comme sur d'autres systèmes

3.2.31
organisation indépendante
organisation distincte et séparée, par sa direction et ses autres ressources, de celles responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité du SIS et qui est chargée de la FSA ou de la validation

3.2.32
personne indépendante
personne distincte et séparée de celles responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité du SIS, qui est chargée de la FSA ou de la validation, et qui n'a pas de responsabilité directe dans ces activités

3.2.33
fonction d'entrée
fonction qui contrôle le processus et ses équipements associés afin de fournir des informations d'entrée à l'unité logique

Note 1 à l'article: Une fonction d'entrée peut être une fonction manuelle.

3.2.34
instrument
appareil utilisé pour effectuer une action (généralement présent dans les systèmes instrumentés)

3.2.34.1
système instrumenté
système composé de capteurs (p. ex.: transmetteurs de pression, de débit et de température), d'unités logiques (p. ex.: contrôleurs programmables, systèmes de commande distribués, contrôleurs discrets) et d'éléments terminaux (p. ex.: vannes de commande, circuits de commande moteur)

Note 1 à l'article: Les systèmes instrumentés réalisent des fonctions instrumentées, notamment des fonctions de commande, de surveillance, d'alarme et de protection. Les systèmes instrumentés peuvent être des SIS (voir 3.2.67) ou des BPCS (voir 3.2.3).

3.2.35
fonction logique
fonction qui réalise les transformations entre les informations d'entrée (fournies par une ou plusieurs fonctions d'entrée) et les informations de sortie (utilisées par une ou plusieurs fonctions de sortie)

Note 1 à l'article: Les fonctions logiques assurent la transformation d'une ou de plusieurs fonctions d'entrée en une ou plusieurs fonctions de sortie.

Note 2 à l'article: Pour d'autres lignes directrices, voir l'IEC 61131-3:2012 et l'IEC 60617-12:1997.

3.2.36
unité logique
partie d'un BPCS ou d'un SIS qui exécute une ou plusieurs fonctions logiques

Note 1 à l'article: Dans l'IEC 61511, les termes suivants sont utilisés pour désigner des unités logiques:

- systèmes logiques électriques pour la technologie électromécanique;
- systèmes logiques électroniques pour la technologie électronique;
- systèmes logiques programmables (PE) pour les systèmes électroniques programmables.

Note 2 à l'article: Des exemples incluent les systèmes électriques, les systèmes électroniques, les systèmes électroniques programmables, les systèmes pneumatiques et les systèmes hydrauliques. Les capteurs et les éléments terminaux ne font pas partie de l'unité logique.

3.2.36.1
unité logique PE configurée pour la sécurité
unité logique de catégorie "électronique programmable pour usage général industriel" spécifiquement configurée pour être utilisée dans des applications de sécurité

Note 1 à l'article: D'autres lignes directrices peuvent être consultées en 11.5.

3.2.37
interface de maintenance/d'ingénierie
matériels et logiciels fournis pour permettre la maintenance ou la modification ad hoc du SIS

Note 1 à l'article: L'interface de maintenance/d'ingénierie peut comprendre des instructions et des diagnostics, pouvant être trouvés dans le logiciel, les terminaux de programmation avec les protocoles de transmission appropriés, des outils de diagnostic, des indicateurs, des appareils de dérivation, des appareils d'essai, et des appareils d'étalonnage.

3.2.37.1
temps moyen de dépannage
MRT
durée totale de dépannage prévue

Note 1 à l'article: Le MRT comprend les temps (b), (c) et (d) pour les durées applicables à la MTTR (voir 3.2.37.2).

Note 2 à l'article: L'abréviation «MRT» est dérivée du terme anglais développé correspondant «mean repair time».

3.2.37.2
durée moyenne de rétablissement
MTTR
durée prévue de rétablissement effectif

Note 1 à l'article: La MTTR comprend:

– le temps de détection de la défaillance (a);
– le temps écoulé avant de commencer la réparation (b);
– le temps de réparation effectif (c);
– le temps écoulé avant la remise en fonctionnement du composant (d).

Le temps de démarrage applicable à (b) est la fin du temps (a); le temps de démarrage applicable à (c) est la fin du temps (b) et le temps de démarrage applicable à (d) est la fin du temps (c).

Note 2 à l'article: L'abréviation «MTTR» est dérivée du terme anglais développé correspondant «mean time to restoration».

3.2.37.3
temps de dépannage maximal admis
MPRT
durée maximale admise pour réparer une défaillance après sa détection

Note 1 à l'article: Le MRT peut être utilisé comme MPRT, mais le MPRT peut être défini sans rapport avec le MRT:

– Un MPRT inférieur au MRT peut être choisi pour diminuer la probabilité d'un événement dangereux.
– Un MPRT supérieur au MRT peut être choisi si la probabilité d'un événement dangereux peut être réduite.

Note 2 à l'article: Lorsqu'un MPRT a été défini, il peut être utilisé à la place du MRT lors du calcul de la probabilité des défaillances aléatoires du matériel.

Note 3 à l'article: L'abréviation «MPRT» est dérivée du terme anglais développé correspondant «maximum permitted repair time».

3.2.38
atténuation
action qui atténue la (les) conséquence(s) d'un événement dangereux

Note 1 à l'article: Il s'agit, par exemple, de la dépressurisation de secours ou de la fermeture des clapets de ventilation en cas de détection ou de confirmation d'incendie ou de fuite de gaz ou le déclenchement de déluge suite à la détection confirmée d'un incendie.

3.2.39
mode de fonctionnement (d'une SIF)
manière dont fonctionne une SIF qui peut être le mode à faible sollicitation, le mode à sollicitation élevée ou le mode continu

a) **mode à faible sollicitation:** mode de fonctionnement dans lequel la SIF n'est réalisée que sur sollicitation, afin de faire passer le processus dans un état de sécurité spécifié, et où la fréquence des sollicitations n'est pas supérieure à une par an.
b) **mode à sollicitation élevée:** mode de fonctionnement dans lequel la SIF n'est réalisée que sur sollicitation, afin de faire passer le processus dans un état de sécurité spécifié, et où la fréquence des sollicitations est supérieure à une par an.
c) **mode continu:** mode de fonctionnement dans lequel la SIF maintient le processus dans un état de sécurité en fonctionnement normal.

3.2.39.1
SIF en mode sollicitation
fonctionnement de la SIF en mode à faible sollicitation (3.2.39 a)) ou en mode à sollicitation élevée (3.2.39 b))

Note 1 à l'article: Dans l'éventualité d'une défaillance dangereuse de la SIF, un événement dangereux ne peut se produire que:

– si la défaillance n'est pas détectée et qu'une sollicitation survient avant l'essai périodique suivant;
– si la défaillance est détectée par les essais de diagnostic, mais que le processus concerné et ses équipements associés n'ont pas basculé dans un état de sécurité avant qu'une sollicitation ne survienne.

Note 2 à l'article: En mode à sollicitation élevée, il sera normalement approprié d'utiliser les critères du mode continu.

Note 3 à l'article: Les niveaux d'intégrité de sécurité des SIF fonctionnant en mode sollicitation sont définis au Tableau 4 et au Tableau 5.

3.2.39.2
SIF en mode continu
SIF fonctionnant en mode continu (3.2.39 c))

Note 1 à l'article: Dans l'éventualité d'une défaillance dangereuse de la SIF, un événement dangereux se produira, sans autre défaillance, sauf si une action est entreprise pour l'empêcher dans le temps de sécurité du processus.

Note 2 à l'article: Le mode continu couvre les SIF qui mettent en œuvre une commande continue pour maintenir la sécurité fonctionnelle.

Note 3 à l'article: Les niveaux d'intégrité de sécurité des SIF fonctionnant en mode continu sont définis au Tableau 5.

3.2.40
module
partie monobloc d'un programme d'application SIS (peut être interne à un programme ou un ensemble de programmes) exécutant une fonction spécifique (p. ex.: séquence de démarrage/d'arrêt/d'essai d'un élément terminal, séquence spécifique à une application au sein d'une SIF)

Note 1 à l'article: Dans le contexte de l'IEC 61131-3:2012, un module logiciel est une fonction ou un bloc de fonctions.

Note 2 à l'article: La plupart des modules ont une utilisation répétitive au sein d'un programme d'application.

3.2.41
MooN
SIS, ou partie de celui-ci, composé de "N" canaux indépendants, qui sont connectés de telle manière que "M" canaux sont suffisants pour exécuter la SIF

3.2.42
réduction de risque nécessaire
réduction de risque devant être réalisée par le ou les SIS et/ou d'autres couches de protection afin de s'assurer que le risque tolérable n'est pas dépassé

3.2.43
système non programmable
système (NP)
système non basé sur les technologies de l'informatique (c'est-à-dire un système non basé sur une électronique programmable [PE] ou sur un logiciel)

Note 1 à l'article: Des exemples incluraient les systèmes électriques ou électroniques câblés, les systèmes mécaniques, hydrauliques ou pneumatiques.

3.2.44
environnement de fonctionnement
conditions inhérentes à l'installation d'un appareil affectant potentiellement ses fonctionnalités et son intégrité de sécurité, telles que:

- l'environnement externe (p. ex.: besoins d'hivernage, classification en zones dangereuses);
- les conditions de fonctionnement des processus (p. ex.: valeurs extrêmes de température, pression et vibration);
- la composition des processus (p. ex.: solides, sels ou corrosifs);
- les interfaces de processus;
- l'intégration aux systèmes globaux de gestion du fonctionnement et de la maintenance de l'installation;
- le débit des communications (p. ex.: interférences électromagnétiques); et
- la qualité du réseau d'alimentation (p. ex.: puissance électrique, air, hydraulique).

Note 1 à l'article: Certaines applications de processus peuvent comporter des exigences d'environnement de fonctionnement particulières nécessaires pour survivre à un événement accidentel majeur. Par exemple, certains équipements exigent des enveloppes spéciales, une purge ou une protection contre l'incendie.

3.2.45
mode de fonctionnement
mode de fonctionnement du processus
état de fonctionnement planifié du processus incluant des modes tels que le démarrage après un arrêt d'urgence, le démarrage, le fonctionnement et l'arrêt normaux, les opérations temporaires, ainsi que le fonctionnement et l'arrêt d'urgence

3.2.46
interface opérateur
moyens par lesquels les informations sont communiquées entre un opérateur humain et le SIS (p. ex.: interfaces d'affichage, voyants lumineux, boutons-poussoirs, klaxons, alarmes)

Note 1 à l'article: L'interface opérateur est parfois désignée sous le nom d'interface homme-machine (IHM).

3.2.47
fonction de sortie
fonction qui commande le processus et ses équipements associés, en fonction des informations de sortie, à partir de la fonction logique

3.2.48
performance
réalisation d'une action ou d'une tâche donnée mesurée par rapport à la spécification et à la série de normes IEC 61511

3.2.49
phase
période comprise dans le cycle de vie de sécurité du SIS, où sont mises en œuvre les activités décrites dans la série IEC 61511

3.2.50
prévention
action qui réduit la probabilité d'occurrence d'un événement dangereux

3.2.51
utilisation antérieure
évaluation documentée par un utilisateur, démontrant qu'un appareil convient à l'utilisation dans un SIS et qu'il peut satisfaire aux exigences fonctionnelles et aux exigences concernant l'intégrité de sécurité, en s'appuyant sur une expérience de fonctionnement antérieure dans des environnements de fonctionnement similaires

Note 1 à l'article: Pour qualifier un appareil SIS sur la base d'une utilisation antérieure, l'utilisateur peut justifier le fait que l'appareil a atteint des performances satisfaisantes dans un environnement de fonctionnement similaire. La manière dont les équipements se comportent dans l'environnement de fonctionnement doit être comprise afin d'obtenir un degré élevé de certitude que les pratiques prévues de conception, d'inspection, d'essai, de maintenance et de fonctionnement sont suffisantes.

Note 2 à l'article: La validation en utilisation s'appuie sur les bases de conception du fabricant (p. ex.: limite de température, limite de vibration, limite de corrosion, support de maintenance souhaité) de cet appareil. L'utilisation antérieure concerne les performances installées de l'appareil au sein d'une application du secteur des industries de transformation, dans un environnement de fonctionnement particulier souvent différent des bases de conception du fabricant.

3.2.52
risque de processus
risque provenant des conditions du processus provoquées par des événements anormaux (comprenant un mauvais fonctionnement du BPCS)

Note 1 à l'article: Dans ce contexte, il s'agit du risque associé à l'événement dangereux spécifique pour lequel les SIS doivent être utilisés afin d'apporter la réduction de risque nécessaire (c'est-à-dire le risque associé à la sécurité fonctionnelle).

Note 2 à l'article: L'analyse de risque de processus est décrite dans l'IEC 61511-3:2016. L'objectif principal dans la détermination du risque de processus est d'établir un point de référence pour le risque, sans prendre en compte les couches de protection.

Note 3 à l'article: L'évaluation de ce risque peut comprendre les problèmes associés aux facteurs humains.

Note 4 à l'article: Ce terme équivaut au "risque EUC" de l'IEC 61508-4:2010.

3.2.52.1
temps de sécurité du processus
durée entre l'occurrence d'une défaillance se produisant dans le processus ou le système de commande de processus de base (avec risque de donner lieu à un événement dangereux) et l'occurrence de l'événement dangereux si la SIF n'est pas exécutée

Note 1 à l'article: Il s'agit d'une propriété du processus uniquement. La SIF doit détecter la défaillance et exécuter son action suffisamment tôt pour empêcher l'événement dangereux, en tenant compte du décalage de processus (p. ex.: le refroidissement d'une cuve).

3.2.53
électronique programmable
PE
entité basée sur les technologies de l'informatique pouvant se composer de matériel, de logiciel, ainsi que d'unités d'entrée et/ou de sortie

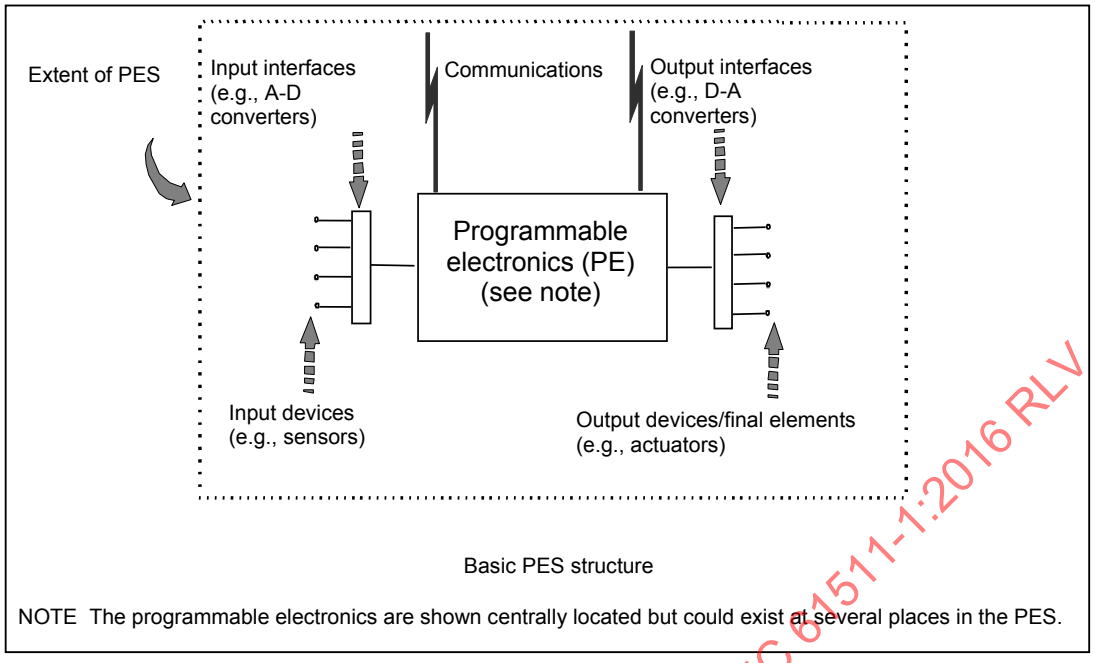
Note 1 à l'article: Ce terme recouvre les appareils microélectroniques basés sur une ou plusieurs unités centrales de traitement (CPU, Central Processing Unit) associées à des mémoires. Des exemples d'appareils électroniques programmables dans le secteur des industries de transformation comprennent:

– capteurs intelligents et éléments terminaux;
– unités logiques électroniques programmables, notamment:
– contrôleurs programmables;
– automates programmables;
– contrôleurs de boucle.

Note 2 à l'article: L'abréviation «PE» est dérivée du terme anglais développé correspondant «programmable electronics».

3.2.54
système électronique programmable
PES
système de commande, de protection ou de surveillance basé sur un ou plusieurs appareils électroniques programmables, comprenant tous les éléments du système, tels que les alimentations, les capteurs et d'autres appareils d'entrée, en passant par les autoroutes de données et d'autres voies de communication, jusqu'aux actionneurs et d'autres appareils de sortie (voir Figure 5)

Note 1 à l'article: L'abréviation «PES» est dérivée du terme anglais développé correspondant «programmable electronic system»



Anglais	Français
Extent of PES	Etendue du PES
Input interfaces (e.g., A-D converters)	Interfaces d'entrée (p. ex.: convertisseurs A-C)
Communications	Communications
Output interfaces (e.g., D-A converters)	Interfaces de sortie (p. ex.: convertisseurs C-A)
Programmable electronics (PE) (see note)	Electronique programmable (PE) (voir note)
Input devices (e.g., sensors)	Appareils d'entrée (p. ex.: capteurs)
Output devices/final elements (e.g., actuators)	Appareils de sortie/éléments terminaux (p. ex.: actionneurs)
Basic PES structure	Structure de base d'un PES
NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.	NOTE L'électronique programmable est présentée de façon centrale, mais pourrait se situer en différents endroits du PES.

Figure 5 – Système électronique programmable (PES): structure et terminologie

3.2.55
programmation
codage
processus consistant à concevoir, à écrire et à soumettre à l'essai un ensemble d'instructions pour résoudre un problème ou traiter des données

Note 1 à l'article: Dans la série IEC 61511, la programmation est typiquement associée à une électronique programmable (PE).

3.2.56
essai périodique
essai périodique destiné à détecter les anomalies dangereuses cachées dans un SIS de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition "comme neuf" ou dans une condition aussi proche que possible de celle-ci

3.2.57
couche de protection
tout mécanisme indépendant réduisant le risque par contrôle, prévention ou atténuation

Note 1 à l'article: Il peut s'agir d'un mécanisme d'ingénierie de processus, tel que la taille des cuves contenant des produits chimiques dangereux, un mécanisme de génie mécanique, tel qu'une soupape de sécurité, un SIS ou une procédure administrative, telle qu'un plan de secours contre un danger imminent. Ces réponses peuvent être automatisées ou déclenchées par des actions humaines (voir Figure 9).

3.2.58
qualité
ensemble des caractéristiques d'une entité portant sur sa capacité à satisfaire aux besoins exprimés et implicites

Note 1 à l'article: Voir l'ISO 9000 pour plus de détails.

3.2.59
défaillance aléatoire du matériel
défaillance survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel

Note 1 à l'article: Il existe de nombreux mécanismes de dégradation se produisant à des fréquences différentes dans divers composants et, puisque les tolérances de fabrication ont pour conséquence une défaillance des composants causée par ces mécanismes après des durées de fonctionnement inégales, les défaillances survenant dans un équipement comprenant plusieurs composants surviennent à des fréquences prévisibles, mais à des instants imprévisibles (c'est-à-dire aléatoires).

Note 2 à l'article: Deux différences majeures permettent de distinguer les défaillances aléatoires du matériel et les défaillances systématiques:

– une défaillance aléatoire du matériel implique le système proprement dit seulement, tandis qu'une défaillance systématique implique à la fois le système proprement dit (une anomalie) et une condition particulière (voir 3.2.81). Ensuite, une défaillance aléatoire du matériel est caractérisée par un seul paramètre de fiabilité (c'est-à-dire le taux de défaillance) alors qu'une défaillance systématique est caractérisée par deux paramètres de fiabilité (c'est-à-dire la probabilité de l'anomalie préexistante et le taux de danger de la condition particulière);
– une défaillance systématique peut être éliminée après avoir été détectée tandis que les défaillances aléatoires du matériel ne le peuvent pas.

Cela implique que les paramètres de fiabilité des défaillances aléatoires du matériel peuvent être estimés à partir des informations de situation alors qu'il est très difficile de réaliser la même chose pour les défaillances systématiques. Une approche qualitative est préférentielle pour les défaillances systématiques.

[SOURCE: IEC 61508-4:20103.6.5, modifiée – Les notes ont été changées]

3.2.60
redondance
existence de plusieurs moyens pour accomplir une fonction exigée ou représenter des informations

Note 1 à l'article: Des exemples incluent l'utilisation d'appareils en double et l'adjonction de bits de parité.

Note 2 à l'article: La redondance sert essentiellement à améliorer la fiabilité ou la disponibilité.

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

3.2.61
risque
combinaison de la probabilité d'un dommage et de sa gravité

Note 1 à l'article: La probabilité d'une occurrence inclut l'exposition à une situation dangereuse, survenue d'un événement dangereux et lapossibilité d'éviter ou de limiter le dommage.

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

3.2.62
défaillance en sécurité
défaillance qui privilégie une action de sécurité donnée

Note 1 à l'article: Une défaillance est "en sécurité" uniquement au regard d'une fonction de sécurité donnée.

Note 2 à l'article: Lorsque la tolérance aux anomalies est mise en œuvre, une défaillance en sécurité peut conduire à:

– un fonctionnement où l'action de sécurité est disponible, mais avec une probabilité plus élevée de réussite en sollicitation (fonctionnement en mode sollicitation) ou une probabilité plus faible d'engendrer un événement dangereux (fonctionnement en mode continu);

– un fonctionnement parasite où l'action de sécurité est déclenchée.

Note 3 à l'article: Lorsqu'aucune tolérance aux anomalies n'est mise en œuvre, les défaillances en sécurité donnent lieu au déclenchement de l'action de sécurité, quelle que soit la condition du processus. Ce phénomène est également connu sous le nom de "déclenchement parasite".

Note 4 à l'article: Un déclenchement parasite peut être en sécurité au regard d'une fonction de sécurité donnée, mais peut être dangereux au regard d'une autre fonction de sécurité.

Note 5 à l'article: Des déclenchements parasites peuvent également avoir des effets néfastes sur la disponibilité en production du processus.

3.2.63
état de sécurité
état du processus lorsque la sécurité est réalisée

Note 1 à l'article: Certains états apportent une plus grande sécurité que d'autres pendant le passage d'une condition dangereuse à l'état de sécurité final ou le passage de la condition de sécurité nominale à une condition dangereuse, le processus pouvant devoir traverser un certain nombre d'états de sécurité intermédiaires.

Note 2 à l'article: Dans certaines situations, l'état de sécurité n'existe que durant le laps de temps où le processus est continuellement contrôlé. Ce contrôle continu peut s'étendre sur une période de temps courte ou indéfinie.

Note 3 à l'article: Un état dit de sécurité au regard d'une fonction de sécurité donnée peut augmenter la probabilité d'engendrer un événement dangereux au regard d'une autre fonction de sécurité donnée. Dans ce cas, l'augmentation de risque potentielle associée à l'autre fonction dans le calcul de la fréquence de déclenchement parasite moyenne maximale admissible (voir 10.3.2) de la première fonction peut être considérée.

Note 4 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.64
sécurité
absence de risque intolérable

Note 1 à l'article: Selon l'ISO/IEC Guide 51, les termes "risque acceptable" et "risque tolérable" sont considérés comme des synonymes.

[SOURCE: ISO/IEC Guide 51:2014, 3.14, modifiée – La note à l'article a été ajoutée]

3.2.65
fonction de sécurité
fonction à réaliser par une ou plusieurs couches de protection, prévue pour assurer ou maintenir un état de sécurité au processus, par rapport à un événement dangereux spécifique

3.2.66
fonction instrumentée de sécurité
SIF
fonction de sécurité devant être mise en œuvre par un système instrumenté de sécurité (SIS)

Note 1 à l'article: Une SIF est conçue pour atteindre un SIL exigé qui est déterminé par rapport aux autres couches de protection participant à la réduction du même risque.

Note 2 à l'article: L'abréviation «SIF» est dérivée du terme anglais développé correspondant «safety instrumented function».

3.2.67
système instrumenté de sécurité
SIS
système instrumenté utilisé pour mettre en œuvre une ou plusieurs SIF

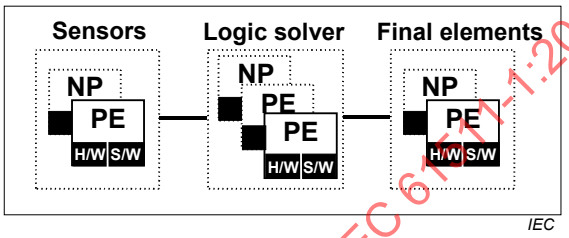
Note 1 à l'article: Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unité(s) logique(s) et d'élément(s) terminal(aux) (p. ex.: voir Figure 6). Il inclut également des équipements de communication et auxiliaires (p. ex.: câbles, tuyauterie, alimentation, lignes d'impulsion, réchauffage des conduites).

Note 2 à l'article: Un SIS peut inclure le logiciel.

Note 3 à l'article: Un SIS peut inclure une action humaine dans le cadre d'une SIF (voir l'ISA TR84.00.04:2015, Partie 1).

Note 4 à l'article: L'abréviation «SIS» est dérivée du terme anglais développé correspondant «safety instrumented system».

SIS architecture and safety instrumented function example with different devices shown



Anglais	Français
SIS architecture and safety instrumented function example with different devices shown	Architecture SIS et exemple de fonction instrumentée de sécurité avec différents appareils
Sensors	Capteurs
Logic solver	Unité logique
Final elements	Eléments terminaux
NP	NP
PE	PE
H/W	matériel
S/W	logiciel

Figure 6 – Exemple d'architectures SIS comprenant trois sous-systèmes SIS

3.2.68
intégrité de sécurité
aptitude du SIS à exécuter la SIF exigée lorsque cela est exigé

Note 1 à l'article: Cette définition est équivalente à la sûreté de fonctionnement du SIS au regard de la SIF exigée. Pour éviter toute confusion, le terme "sûreté de fonctionnement", qui est souvent considéré au sens économique plutôt qu'en tant que concept de sécurité, n'a pas été utilisé.

Note 2 à l'article: L'aptitude inclut à la fois la réponse fonctionnelle (p. ex.: fermeture d'une vanne spécifiée dans un intervalle de temps spécifié) et la probabilité que le SIS agisse comme cela est exigé.

Note 3 à l'article: L'évaluation de l'intégrité de sécurité peut prendre en compte toutes les causes des défaillances aléatoires du matériel et des défaillances systématiques conduisant à un état de non-sécurité (p. ex.: défaillances de matériel, défaillances induites du logiciel et défaillances dues aux perturbations électriques). Certaines de ces défaillances, en particulier les défaillances aléatoires du matériel, peuvent être quantifiées à l'aide de mesures telles que la fréquence moyenne de défaillance dangereuse ou la probabilité de défaillance en cas de sollicitation. Cependant, l'intégrité de sécurité dépend également de plusieurs facteurs systématiques, qui ne peuvent pas être précisément quantifiés, mais simplement considérés d'un point de vue qualitatif tout au long du cycle de vie. La probabilité que les défaillances systématiques conduisent à une défaillance dangereuse du SIS est réduite par le biais de la tolérance aux défauts du matériel (voir 11.4) ou d'autres méthodes et techniques.

Note 4 à l'article: L'intégrité de sécurité comprend l'intégrité de sécurité du matériel (voir 3.2.26) et l'intégrité de sécurité systématique (voir 3.2.82), mais les défaillances complexes engendrées par la conjonction des défaillances du matériel et des défaillances systématiques peuvent également être prises en compte.

3.2.69
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) affecté à la SIF permettant de spécifier les exigences concernant l'intégrité de sécurité devant être réalisées par le SIS

Note 1 à l'article: Plus le SIL est élevé, plus la PFD_{avg} attendue en mode sollicitation ou la fréquence moyenne d'une défaillance dangereuse causant un événement dangereux en mode continu est faible.

Note 2 à l'article: Les relations entre le niveau objectif de défaillances et le SIL sont données dans les Tableaux 4 et 5.

Note 3 à l'article: Le SIL 4 possède le plus haut niveau d'intégrité de sécurité; le SIL 1 possède le niveau le plus bas

Note 4 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

Note 5 à l'article: L'abréviation «SIL» est dérivée du terme anglais développé correspondant «safety integrity level»

3.2.69.1
exigences concernant l'intégrité de sécurité, pl
ensemble des exigences de l'IEC 61511 devant être satisfaites par un SIS afin de revendiquer un SIL donné pour une SIF mise en œuvre par ce SIS

Note 1 à l'article: Les exigences concernant l'intégrité de sécurité sont renforcées lorsque le SIL associé augmente.

3.2.70
cycle de vie de sécurité du SIS
activités nécessaires à la mise en œuvre de SIF, se déroulant au cours d'une période de temps, qui commence à la phase de conception d'un projet et se termine lorsque toutes les SIF ne sont plus disponibles à l'utilisation

Note 1 à l'article: Le terme "cycle de vie de sécurité fonctionnelle" est strictement plus précis, mais l'adjectif "fonctionnelle" n'est pas considéré comme étant nécessaire dans ce cas, c'est-à-dire dans le contexte de la série IEC 61511.

Note 2 à l'article: Le modèle de cycle de vie de sécurité du SIS utilisé dans l'IEC 61511 est donné par la Figure 7.

3.2.71
manuel de sécurité
manuel de sécurité fonctionnelle
informations qui définissent comment un appareil, un sous-système ou un système SIS peuvent être appliqués sans risque

Note 1 à l'article: Le manuel de sécurité peut comporter des données d'entrée du fabricant, mais également de l'utilisateur.

Note 2 à l'article: Concernant les appareils conformes à l'IEC 61508, les données d'entrée du fabricant correspondent au manuel de sécurité.

Note 3 à l'article: Ce terme pourrait recouvrir un document autonome générique ou un ensemble de documents.

Note 4 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.72
spécification des exigences de sécurité
SRS
spécification qui contient les exigences fonctionnelles pour les SIF et leurs niveaux d'intégrité de sécurité associés

Note 1 à l'article: L'abréviation «SRS» est dérivée du terme anglais développé correspondant «safety requirements specification»

[SOURCE: IEC 61508-4:2010, 3.5.11, modifiée – Alignée sur la terminologie de l'IEC 61511]

3.2.73
capteur
partie du BPCS ou du SIS qui mesure ou détecte la condition du processus

Note 1 à l'article: Des exemples incluent les transmetteurs, les transducteurs, les interrupteurs de processus et les interrupteurs de position.

3.2.74
logiciel
programmes, procédures, données, règles, ainsi que toute documentation se référant au fonctionnement d'un système de traitement de données

Note 1 à l'article: Le logiciel est indépendant du support sur lequel il a été enregistré.

Note 2 à l'article: Pour des exemples des différents types de logiciels, voir 3.2.75 et 3.2.76.

3.2.75
langages de programmation d'application

3.2.75.1
langage de programme figé
FPL
langage dans lequel l'utilisateur est limité à l'ajustement de quelques jeux de paramètres prédéfinis et figés

Note 1 à l'article: Des exemples représentatifs d'applications d'appareil avec FPL sont: les capteurs intelligents (p. ex.: transmetteur de pression sans algorithmes de commande), les éléments terminaux intelligents (p. ex.: vannes sans algorithmes de commande), les séquences d'un enregistreur d'événements, les points de consigne d'un boîtier d'alarme intelligent. L'utilisation de FPL est souvent nommée "configuration de l'appareil".

Note 2 à l'article: L'abréviation «FPL» est dérivée du terme anglais développé correspondant «fixed program language»

3.2.75.2
langage de variabilité limitée
LVL
langage de programmation destiné aux automates programmables industriels du commerce dont les capacités sont limitées à leur mise en oeuvre, telle que définie par le manuel de sécurité associé. La notation de ce langage peut être textuelle, graphique ou présenter les caractéristiques des deux.

Note 1 à l'article: Ce type de langage est conçu pour être aisément compris par les utilisateurs du secteur des industries de transformation, et permet de combiner des fonctions de bibliothèque, prédéfinies, spécifiques à une application, pour mettre en œuvre les SRS. Les LVL fournissent une correspondance fonctionnelle étroite avec les fonctions exigées pour réaliser l'application.

Note 2 à l'article: L'IEC 61511 part du principe que les contraintes nécessaires à l'obtention des propriétés de sécurité sont le résultat de la combinaison du manuel de sécurité, de la proximité de la notation avec les fonctions dont le programmateur d'application a besoin pour définir les algorithmes de commande de processus et du temps de compilation et des vérifications d'exécution que le fournisseur de l'unité logique intègre dans le logiciel de base de l'unité logique et son environnement de développement. Les contraintes identifiées dans le rapport de certification et le manuel de sécurité peuvent garantir que les exigences de l'IEC 61508-3:2010 sont satisfaites.

Note 3 à l'article: Le LVL est le langage le plus fréquemment utilisé lorsque la série IEC 61511 fait référence au terme "programme d'application".

Note 4 à l'article: L'abréviation "LVL" est dérivée du terme anglais développé correspondant "limited variability language".

3.2.75.3
langage de variabilité totale
FVL
langage conçu pour être compréhensible par les informaticiens (programmeurs), et qui permet de mettre en œuvre une plage étendue de fonctions et d'applications

Note 1 à l'article: Un exemple type de système utilisant le FVL est l'ordinateur d'usage général.

Note 2 à l'article: Dans le secteur des industries de transformation, le FVL se trouve dans les logiciels intégrés et rarement dans la programmation d'application.

Note 3 à l'article: Des exemples de FVL incluent: l'Ada, le C, le Pascal, le langage Liste d'instructions, les langages d'assemblage, le C++, le Java et le SQL.

Note 4 à l'article: L'abréviation «FVL» est dérivée du terme anglais développé correspondant «full variability language»

3.2.76
types de logiciels et de programmes

3.2.76.1
programme d'application
programme spécifique à l'application de l'utilisateur contenant, en général, des séquences logiques, des autorisations, des limites et des expressions qui contrôlent l'entrée, la sortie, les calculs et les décisions nécessaires pour satisfaire aux exigences fonctionnelles des SIS

3.2.76.2
logiciel intégré
logiciel qui fait partie du système fourni par le fabricant et qui n'est pas accessible pour des modifications par l'utilisateur final

Note 1 à l'article: Le logiciel intégré est également désigné sous le nom de microprogramme ou de logiciel système. Voir 3.2.75.3 "langage de variabilité totale".

3.2.76.3
logiciel utilitaire
outils logiciels pour la création, la modification et la documentation des programmes d'application

Note 1 à l'article: Ces outils logiciels ne sont pas exigés pour le fonctionnement du SIS.

3.2.77
cycle de vie du programme d'application
ensemble d'activités qui se déroulent au cours d'une période de temps débutant lorsque le programme d'application est conçu et se terminant lorsque le programme d'application est retiré du service

Note 1 à l'article: Le cycle de vie d'un programme d'application inclut habituellement une phase de définition d'exigences, une phase de développement, une phase d'essai, une phase d'intégration, une phase d'installation et une phase de modification.

Note 2 à l'article: Le logiciel (notamment le programme d'application) ne peut pas être entretenu; au lieu de cela, il est modifié.

3.2.78
sous-système SIS
partie indépendante d'un SIS dont une défaillance dangereuse invalidante donne lieu à une défaillance dangereuse invalidante du SIS

Note 1 à l'article: La Figure 6 présente un SIS composé de trois sous-systèmes SIS.

Note 2 à l'article: Concernant l'approche de coupe (voir IEC 61025), une coupe minimale d'un sous-système SIS est également une coupe minimale du SIS global. Par conséquent, les SIF mises en œuvre au sein d'un SIS dépendent totalement des sous-systèmes SIS de ce SIS (autrement dit lorsqu'un sous-système SIS est défaillant, les SIF associées sont également défaillantes).

3.2.79
système
ensemble d'appareils qui interagissent selon une spécification

Note 1 à l'article: Une personne peut faire partie d'un système.

Note 2 à l'article: Cette définition diffère de celle donnée par l'IEC 61508 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.80
capabilité systématique
mesure (exprimée sur une échelle de SC 1 à SC 4) de la confiance dans le fait que l'intégrité de sécurité systématique d'un appareil satisfait aux exigences du SIL spécifié, par rapport à la fonction de sécurité spécifiée, lorsque l'appareil est appliqué conformément aux instructions spécifiées dans le manuel de sécurité de l'appareil

Note 1 à l'article: La capabilité systématique est déterminée par référence aux exigences concernant l'évitement et la maîtrise des défaillances systématiques dans l'IEC 61508-2:2010 et l'IEC 61508-3:2010.

Note 2 à l'article: Le mécanisme de défaillance systématique dépend de la nature de l'appareil. Pour un appareil comprenant uniquement du matériel, seuls les mécanismes de défaillance du matériel sont considérés. Pour un appareil comprenant du matériel et du logiciel, les interactions entre les mécanismes de défaillance du matériel et du logiciel doivent être considérées.

Note 3 à l'article: Une capabilité systématique de SC N pour un appareil signifie que l'intégrité de sécurité systématique de SC N a été satisfaite lorsque l'appareil est appliqué conformément aux instructions spécifiées dans le manuel de sécurité de l'appareil par rapport au SC N.

3.2.81
défaillance systématique
défaillance relative à une anomalie préexistante, qui survient systématiquement dans des conditions particulières, ne pouvant être éliminée qu'en supprimant l'anomalie par une modification de la conception ou du processus de fabrication, des procédures de fonctionnement, de la documentation ou d'autres facteurs appropriés

Note 1 à l'article: La cause des défaillances systématiques du logiciel peut être désignée sous le nom de "bogues".

Note 2 à l'article: La maintenance corrective sans modification n'éliminerait pas, habituellement, la cause de la défaillance qui implique la défaillance dans des conditions particulières.

Note 3 à l'article: Une défaillance systématique peut être reproduite en appliquant délibérément les mêmes conditions, même si toutes les défaillances reproductibles ne sont pas systématiques.

Note 4 à l'article: Des exemples d'erreurs conduisant à une défaillance systématique incluent l'erreur humaine survenant dans:

– la SRS;
– la conception, la fabrication, l'installation, le fonctionnement ou la maintenance du matériel;
– la conception ou la mise en œuvre du logiciel (notamment le programme d'application).

Note 5 à l'article: Des appareils similaires conçus, installés, mis en fonctionnement, mis en œuvre ou entretenus de la même façon sont susceptibles de contenir les mêmes anomalies. Par conséquent, ils font l'objet de défaillances de cause commune lorsque les conditions particulières surviennent.

3.2.82
intégrité de sécurité systématique
partie de l'intégrité de sécurité des SIS qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux

Note 1 à l'article: L'intégrité de sécurité systématique ne peut normalement pas être quantifiée (à la différence de l'intégrité de sécurité du matériel).

Note 2 à l'article: Voir également 3.2.26.

3.2.83
niveau objectif de défaillances
performance exigée de la SIF et spécifiée en termes de probabilité moyenne de défaillance lors du fonctionnement de la SIF en mode sollicitation (fonctionnement en mode sollicitation) ou de fréquence moyenne d'une défaillance dangereuse (fonctionnement en mode continu)

Note 1 à l'article: Les relations entre les niveaux objectifs de défaillances et le SIL sont données dans les Tableaux 4 et 5.

3.2.84
risque tolérable
niveau de risque accepté dans un certain contexte et fondé sur les valeurs admises par la société

Note 1 à l'article: Voir l'IEC 61511-3:2016, Annexe A.

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

3.2.85
non détecté
non révélé
non déclaré
qui n'est pas détecté, ni révélé, ni déclaré

Note 1 à l'article: Dans l'IEC 61511 et excepté lorsque le contexte suggère une autre signification, le terme "défaillances/erreurs non détectées dangereuses" se rapporte aux défaillances/erreurs dangereuses non détectées par les essais de diagnostic.

3.2.86
validation
confirmation par examen et apport de preuves objectives que les exigences particulières à une utilisation prévue spécifique sont satisfaites

Note 1 à l'article: Dans la série IEC 61511, cela signifie démontrer que la ou les SIF et le SIS après installation satisfont en tous points à la SRS.

3.2.87
vérification
confirmation par examen et apport de preuves objectives que les exigences ont été satisfaites

Note 1 à l'article: Dans la série IEC 61511, cela désigne l'activité qui consiste, pour chaque phase du cycle de vie de sécurité du SIS correspondant, à démontrer par analyse et/ou par essais que, pour les entrées spécifiques, les sorties satisfont en tous points aux objectifs et aux exigences fixés pour la phase spécifique.

Note 2 à l'article: Des exemples incluent les activités de vérification qui suivent:

– les revues relatives aux sorties (documents concernant toutes les phases du cycle de vie de sécurité) destinées à assurer la conformité avec les objectifs et exigences de la phase, et prenant en compte les entrées spécifiques à cette phase;
– les revues de conception;
– les essais réalisés sur les produits conçus, afin d'assurer que leur fonctionnement est conforme à leur spécification;
– les essais d'intégration réalisés lors de l'assemblage de différentes parties d'un système, élément par élément, et par la réalisation d'essais d'environnement, afin d'assurer que toutes les parties fonctionnent les unes avec les autres, conformément à ce qui est spécifié.

3.2.88
chien de garde
combinaison de diagnostics et d'un appareil de sortie (typiquement un commutateur) pour effectuer la surveillance du bon fonctionnement de l'appareil électronique programmable (PE) et entreprendre une action lors de la détection d'un fonctionnement incorrect

Note 1 à l'article: Le chien de garde confirme que le système logiciel fonctionne correctement en réinitialisant régulièrement un appareil externe (p. ex.: temporisateur électronique de chien de garde matériel), par un appareil de sortie commandé par le logiciel.

Note 2 à l'article: Le chien de garde peut être utilisé pour mettre hors tension un groupe de sorties de sécurité, lorsque des défaillances dangereuses sont détectées, afin d'atteindre ou de maintenir un état de sécurité du processus par rapport à l'événement dangereux. Le chien de garde est utilisé pour augmenter la couverture du diagnostic en ligne de l'unité logique PE (voir 3.2.13 et 3.2.15).

3.3 Abréviations

Les abréviations utilisées tout au long de l'IEC 61511 sont données au Tableau 1. Sont également incluses certaines abréviations communes relatives à la sécurité fonctionnelle du secteur des industries de transformation.

Tableau 1 – Abréviations utilisées dans l'IEC 61511

Abréviation	Expression développée
AC/DC	Alternating current/direct current, Courant alternatif/Courant continu (CA/CC)
AIChE	American Institute of Chemical Engineers
ALARP	As low as reasonably practicable, Aussi faible que raisonnablement possible
ANSI	American National Standards Institute, Organisme national de normalisation américain
AP	Application program, Programme d'application
BPCS	Basic process control system, Système de commande de processus de base
CCPS	Centre for Chemical Process Safety (AIChE), Centre pour la sécurité des processus chimiques
DC	Diagnostic coverage, Couverture du diagnostic
E/E/PE	Electrical/electronic/programmable electronic, Electrique/électronique/électrique programmable
EMC	Electro-magnetic compatibility, Compatibilité électromagnétique (CEM)
FAT	Factory acceptance test, Essai de réception en usine (ERU)
FPL	Fixed program language, Langage de programme figé
FSA	Functional safety assessment, Evaluation de la sécurité fonctionnelle
FSMS	Functional safety management system, Système de gestion de la sécurité fonctionnelle
FTA	Fault tree analysis, Analyse par arbre des défaillances
FVL	Full variability language, Langage de variabilité totale
HFT	Hardware fault tolerance, Tolérance aux défauts du matériel
H&RA	Hazard & risk assessment, Analyse de danger et de risque
HMI	Human Machine Interface, Interface homme-machine (IHM)
IEC	International Electrotechnical Commission, Commission Electrotechnique Internationale
ISA	International Society of Automation, Société internationale d'automation
ISO	International Organization for Standardization, Organisation internationale de normalisation
LVL	Limited variability language, Langage de variabilité limitée
MooN	"M" out of "N" channel architecture, Architecture de "M" pour "N" canaux
MPRT	Maximum permitted repair time, Temps de dépannage maximal admis
MRT	Mean repair time, Temps moyen de dépannage
MTTR	Mean time to restoration, Durée moyenne de rétablissement
NFPA	National Fire Protection Association(US), National Fire Protection Association (Etats-Unis)
NP	Non-programmable, Non programmable
OEM	Original Equipment Manufacturer, Fabricant original de l'équipement
PE	Programmable electronics, Electronique programmable
PES	Programmable electronic system, Système électronique programmable

Abréviation	Expression développée
PFD	Probability of dangerous failure on demand, Probabilité de défaillance dangereuse en cas de sollicitation
PFD_{avg}	Average probability of dangerous failure on demand, Probabilité moyenne de défaillance dangereuse en cas de sollicitation
PFH	Probability (average frequency of dangerous failures) of failure per hour, Probabilité (fréquence moyenne de défaillance dangereuse) de défaillance par heure
pl	Plural, Pluriel
PLC	Programmable logic controller, Automate programmable
SAT	Site acceptance test, Essai de réception sur site (ERS)
SC	Systematic capability, Capabilité systématique
SIF	Safety instrumented function, Fonction instrumentée de sécurité
SIL	Safety integrity level, Niveau d'intégrité de sécurité
SIS	Safety instrumented system, Système instrumenté de sécurité
SRS	Safety requirement specification, Spécification des exigences de sécurité

4 Conformité à l'IEC 61511-1:2016

Afin de se conformer à l'IEC 61511-1:2016, il doit être démontré que chacune des exigences décrites de l'Article 5 à l'Article 19 a été satisfaite eu égard aux critères définis, et que le ou les objectifs spécifiés dans ces articles ont donc été atteints.

5 Gestion de la sécurité fonctionnelle

5.1 Objectif

L'objectif des exigences de l'Article 5 est d'identifier les activités de gestion nécessaires pour s'assurer que les objectifs de sécurité fonctionnelle sont bien atteints.

NOTE 1: L'Article 5 a seulement pour but la réalisation et la maintenance de la sécurité fonctionnelle des SIS. Il est dissocié et distinct des mesures générales concernant la santé et la sécurité nécessaires à l'obtention de la sécurité sur le lieu de travail.

5.2 Exigences

5.2.1 Généralités

La politique et la stratégie pour atteindre la sécurité fonctionnelle doivent être identifiées, ainsi que les méthodes utilisées pour évaluer leur réalisation, et doivent être communiquées au sein de l'organisation.

5.2.2 Organisation et ressources

5.2.2.1 Les personnes, services, organisations ou autres unités qui sont responsables de l'exécution et de la revue de chacune des phases du cycle de vie de sécurité du SIS doivent être identifiés et être informés des responsabilités qui leur sont affectées.

5.2.2.2 Les personnes, les services ou les organisations impliqués dans les activités du cycle de vie de sécurité du SIS doivent être compétents pour conduire les activités dont ils sont responsables.

Les points suivants doivent être traités et documentés en considérant la compétence des personnes, services, organisations ou autres unités impliqués dans les activités du cycle de vie de sécurité du SIS: