LICENCE

for

AS IEC 61511.1-2004 (R2015) Functional safety - Safety instrumented systems for the process industry sector Framework, definitions, systems, hardware and software requirements

Licensee: Hoslab Pty Ltd

Date: 03-Sep-2018

To read the full licence agreement, simply click within the red box above and scroll through with your cursor

AS IEC 61511.1—2004
IEC 61511-1:2003
Reconfirmed 2015

Australian Standard™

Functional safety—Safety instrumented systems for the process industry sector

Part 1: Framework, definitions, systems, hardware and software requirements

STANDARDS AUSTRALIA

This Australian Standard was prepared by Committee IT-006, Information Technology for Industrial Automation and Integration. It was approved on behalf of the Council of Standards Australia on 5 March 2004 and published on 10 May 2004.

The following are represented on Committee IT-006:

Association of Consulting Engineers Australia

Australian Electrical and Electronic Manufacturers Association

CSIRO Centre for Planning and Design

CSIRO Manufacturing & Infrastructure Technology

Department of Defence (Australia)

Institute of Instrumentation, Control and Automation Australia

Institution of Engineers Australia

Monash University

RMIT University

The University of Melbourne

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 04055.

STANDARDS AUSTRALIA

RECONFIRMATION

OF

AS IEC 61511.1—2004

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

RECONFIRMATION NOTICE

Technical Committee IT-006 has reviewed the content of this publication and in accordance with Standards Australia procedures for reconfirmation, it has been determined that the publication is still valid and does not require change.

Reconfirmed documents cannot be amended, but may be formally revised and a new edition published.

Certain documents referenced in the publication may have been amended since the original date of publication. Users are advised to ensure that they are using the latest versions of such documents as appropriate, unless advised otherwise in this Reconfirmation Notice.

Approved for reconfirmation in accordance with Standards Australia procedures for reconfirmation on 14 July 2015.

The following are represented on Technical Committee IT-006:

Australia Safety Critical Systems Association
Australian Computer Society
Australian Industry Group
Australian Petroleum Production and Exploration Association
Consult Australia
Engineers Australia
Institute of Chemical Engineers Australia
Institute of Instrumentation, Control & Automation
ISACA
Process Control Society
The University of Queensland
Workplace Health and Safety Queensland

NOTES

Australian Standard™

Functional safety—Safety instrumented systems for the process industry sector

Part 1: Framework, definitions, systems, hardware and software requirements

First published as AS IEC 61511.1—2004.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5913 0

PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Information Technology for Industrial Automation and Integration.

This Standard is identical with, and has been reproduced from, IEC 61511-1:2003, *Functional safety—Safety instrumented systems for the process industry sector*—Part 1: *Framework, definitions, systems, hardware and software requirements*.

The objective of this Standard is to provide requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state.

This Standard is Part 1 of AS IEC 61511, *Functional safety—Safety instrumented systems for the process industry sector*, which is published in parts as follows:

Part 1: Framework, definitions, system, hardware and software requirements (this Standard)
Part 2: Guidelines for the application of AS IEC 61511-1
Part 3: Guidance for the determination of the required safety integrity levels

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover

(b) In the source text ‘this International Standard’ should read ‘this Australian Standard’.

(c) A full point substitutes for a comma when referring to a decimal marker.

CONTENTS

INTRODUCTION

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

This standard addresses the application of safety instrumented systems for the process industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. Other safety systems are only considered so that their contribution can be taken into account when considering the performance requirements for the safety instrumented systems. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

This standard has two concepts which are fundamental to its application; safety lifecycle and safety integrity levels.

This standard addresses safety instrumented systems which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This standard is process industry specific within the framework of IEC 61508 (see Annex A).

This standard sets out an approach for safety life-cycle activities to achieve these minimum standards. 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. 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, programmable electronic). To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;
- works within a framework which is applicable to all instrumented methods 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.

This standard on safety instrumented systems for the process industry

- addresses all 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 this standard.

This International Standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example, national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

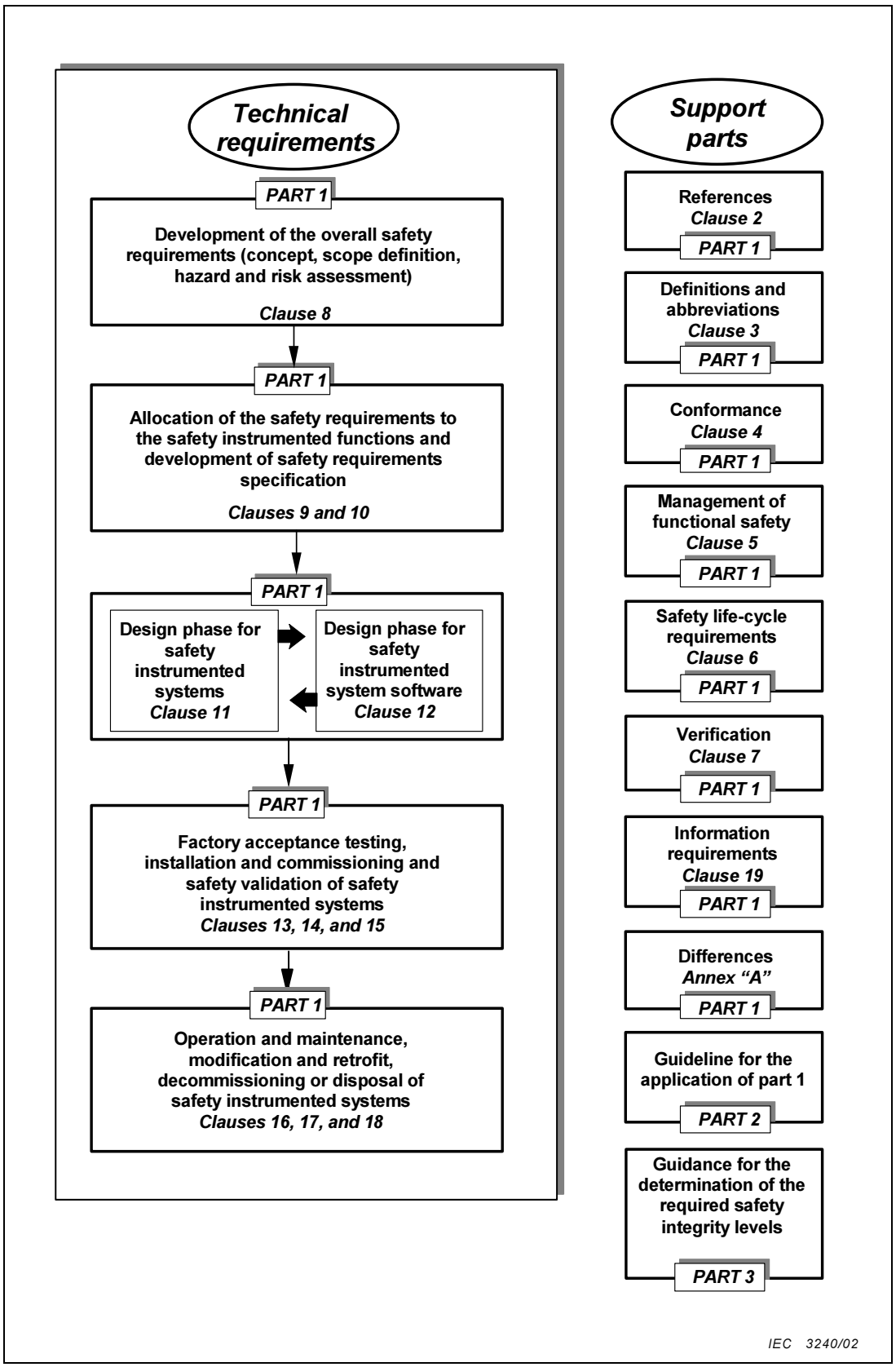


Figure 1 – Overall framework of this standard

NOTES

STANDARDS AUSTRALIA

Australian Standard

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

Any table, figure or text of the international standard that is struck through is not part of this standard. Any Australian/New Zealand table, figure or text that is added is part of this standard and is identified by shading.

1 Scope

This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.

In particular, this standard

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

b) applies when equipment that meets the requirements of IEC 61508, or of 11.5 of IEC 61511-1, is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC 61508-2 and IEC 61508-3);

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

d) applies when application software is developed for systems having limited variability or fixed programmes but does not apply to manufacturers, safety instrumented systems designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3);

e) applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation;

NOTE Within the process sector some applications, (for example, off-shore), may have additional requirements that have to be satisfied.

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

g) results in the identification of the functional requirements and safety integrity requirements for the safety instrumented function(s) taking into account the risk reduction achieved by other means;

h) specifies requirements for system architecture and hardware configuration, application software, and system integration;

i) specifies requirements for application software for users and integrators of safety instrumented systems (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 safety instrumented functions for the protection of personnel, protection of the general public or protection of the environment;

k) may be applied in non-safety applications such as asset protection;

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

m) uses a safety life cycle (Figure 8) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the safety instrumented systems;

n) requires that a hazard and risk assessment is to be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;

NOTE See Figure 9 for an overview of risk reduction methods.

o) establishes numerical targets for average probability of failure on demand and frequency of dangerous failures per hour for the safety integrity levels;

p) specifies minimum requirements for hardware fault tolerance;

q) specifies techniques/measures required for achieving the specified integrity levels;

r) defines a maximum level of performance (SIL 4) which can be achieved for a safety instrumented function implemented according to this standard;

s) defines a minimum level of performance (SIL 1) below which this standard does not apply;

t) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications (which should be established based on knowledge of the particular application);

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

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

w) requires that the design of a safety instrumented function takes into account human factors;

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

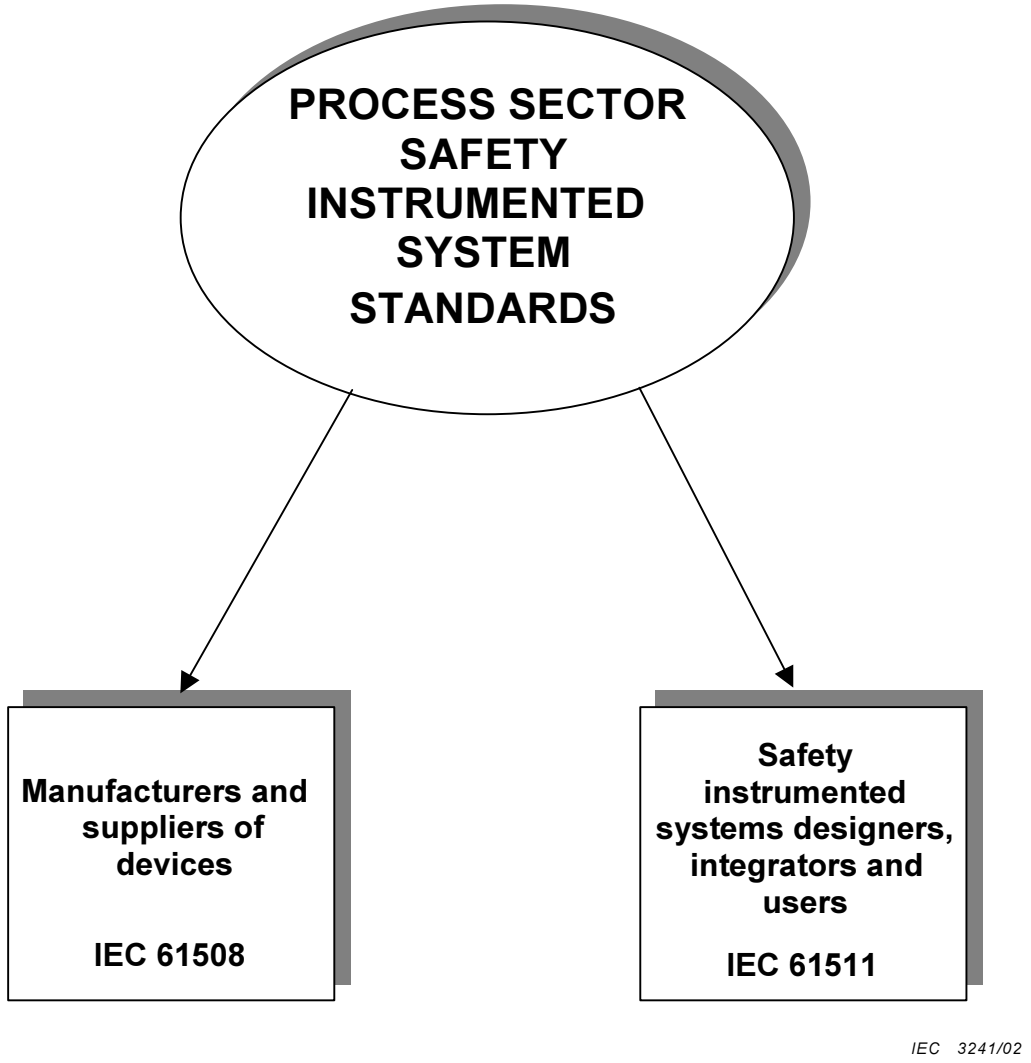


Figure 2 – Relationship between IEC 61511 and IEC 61508

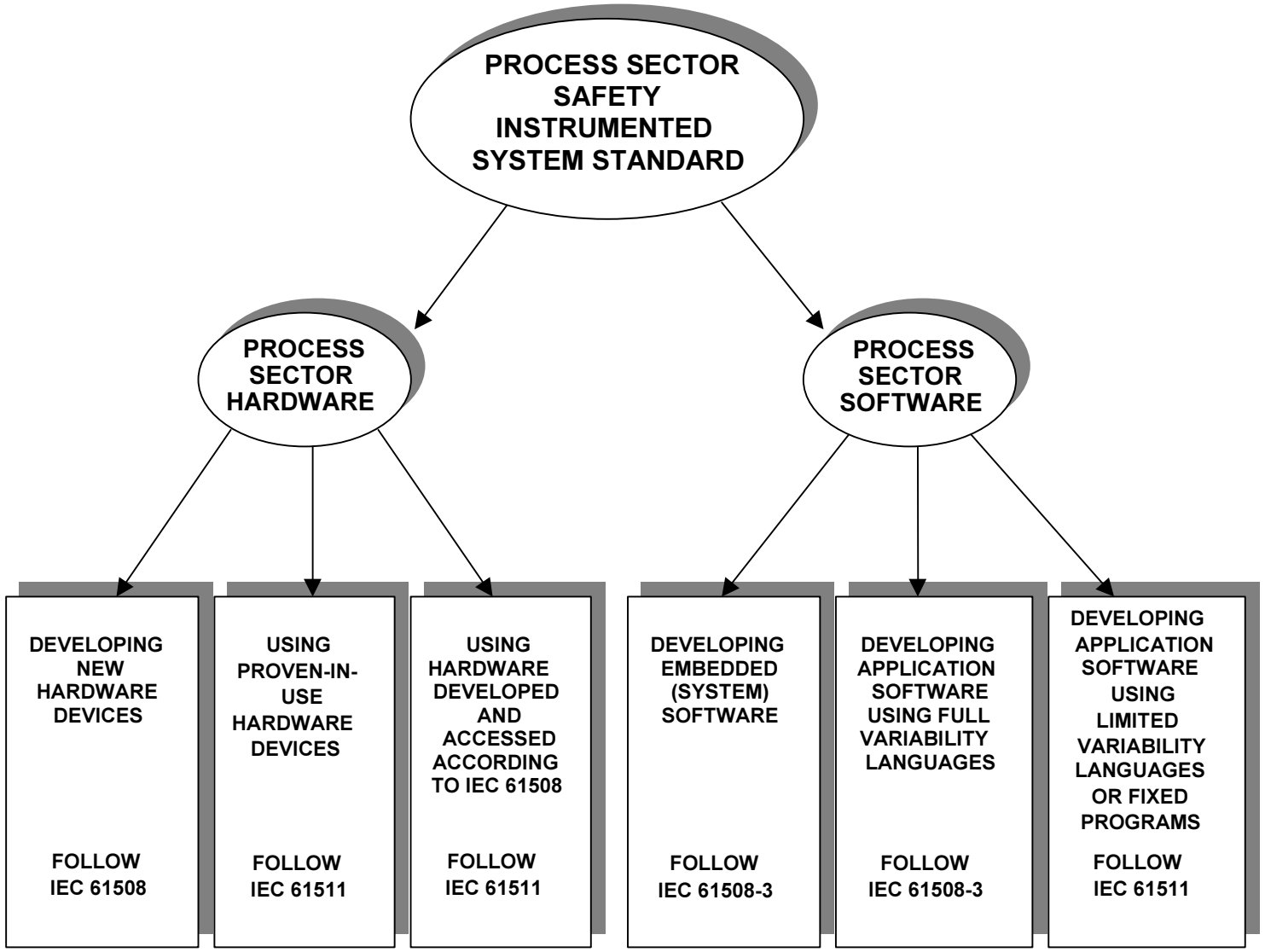


Figure 3 – Relationship between IEC 61511 and IEC 61508 (see clause 1)

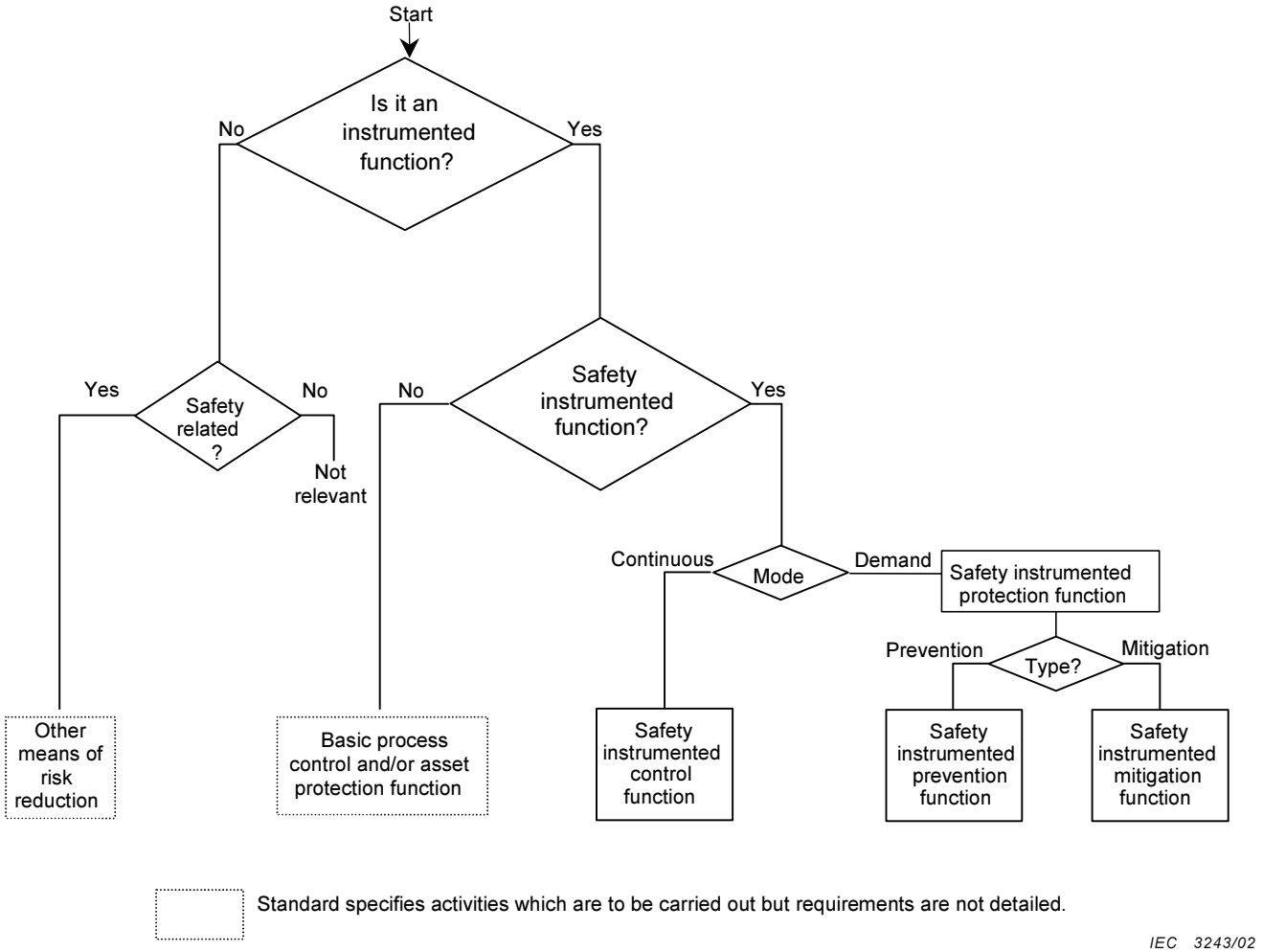


Figure 4 – Relationship between safety instrumented functions and other functions

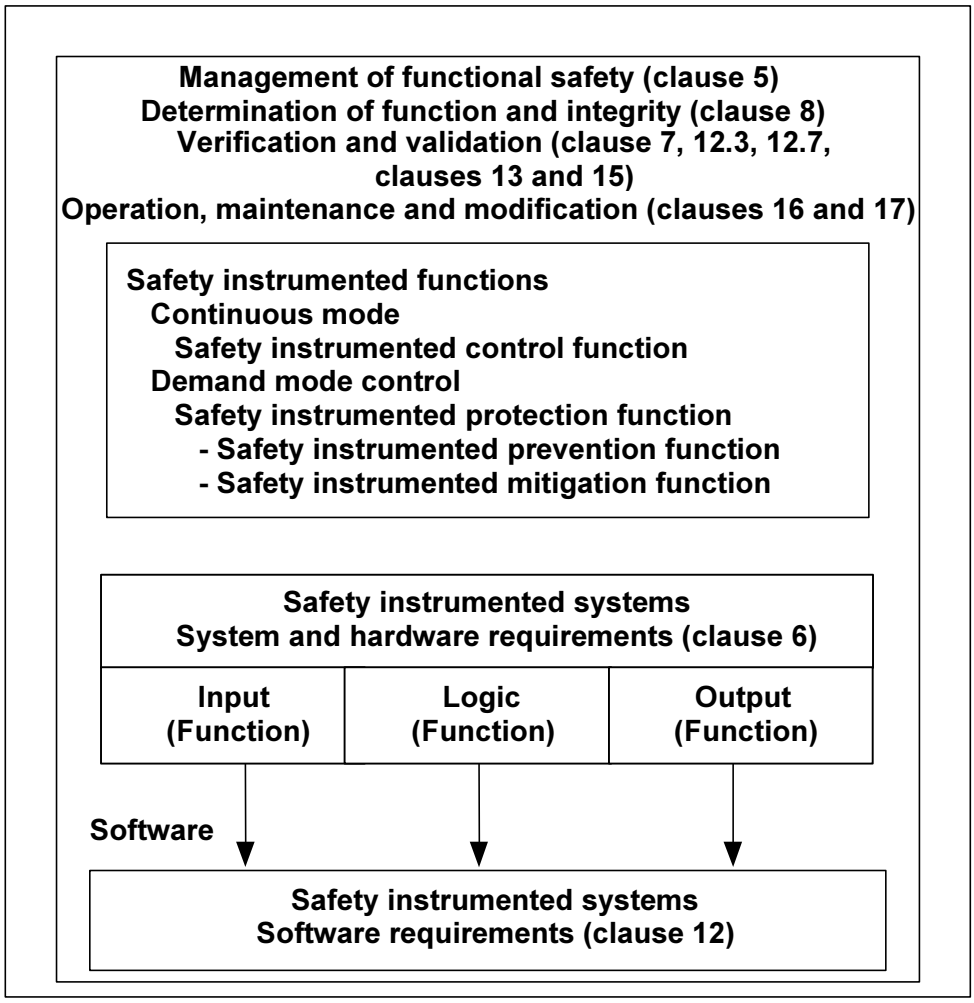


Figure 5 – Relationship between system, hardware, and software of IEC 61511-1

2 Normative references

References to international standards that are struck through in this clause are replaced by references to Australian or Australian/New Zealand Standards that are listed immediately thereafter and identified by shading. Any Australian or Australian/New Zealand Standard that is identical to the International Standard it replaces is identified as such.

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

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

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, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

AS 61508.3, *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*~~

AS IEC 61511.2: *Functional safety—Safety instrumented systems for the process industry sector, Part 2: Guidelines the application of IEC 61511-1*

3 Abbreviations and definitions

3.1 Abbreviations

Abbreviations used throughout IEC 61511 are given in Table 1.

Table 1 – Abbreviations used in IEC 61511

Abbreviation	Full expression
AC/DC	Alternating current/direct current
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
BPCS	Basic process control system
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 testing
FPL	Fixed program language
FTA	Fault tree analysis
FVL	Full variability language
HFT	Hardware fault tolerance
HMI	Human machine interface
H&RA	Hazard and risk assessment
HRA	Human reliability analysis
H/W	Hardware
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISA	Instrumentation, Systems and Automation Society
ISO	International Organization for Standardization
LVL	Limited variability language
MooN	“M” out of “N” (see 3.2.45)
NP	Non-programmable
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of failure on demand
PFD_{avg}	Average probability of failure on demand
PLC	Programmable logic controller
SAT	Site acceptance test
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification
S/W	Software

3.2 Definitions

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

3.2.1
architecture
arrangement of hardware and/or software elements in a system, for example,

(1) arrangement of safety instrumented system (SIS) subsystems;

(2) internal structure of an SIS subsystem;

(3) arrangement of software programs

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

3.2.2
asset protection
function allocated to system design for the purpose of preventing loss 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 an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1

NOTE See Clause A.2.

3.2.4
channel
element or group of elements that independently perform(s) a function

NOTE 1 The elements within a channel could include input/output (I/O) modules, logic systems (see 3.2.40), sensors, final elements.

NOTE 2 A dual channel (i.e., a two-channel) configuration is one with two channels that independently perform the same function.

NOTE 3 The term can be used to describe a complete system or a portion of a system (for example, sensors or final elements).

3.2.5
coding
see “programming”

3.2.6

3.2.6.1
common cause failure
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

3.2.6.2
common mode failure
failure of two or more channels in the same way, causing the same erroneous result

3.2.7
component
one of the parts of a system, subsystem, or device performing a specific function

3.2.8
configuration
see “architecture”

3.2.9
configuration management
discipline of identifying the components of an evolving (hardware and software) system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the life cycle

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 The control system includes input devices and final elements and may be either a BPCS or an 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

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.

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 Two events A and B are dependent, where P(z) is the probability of event z, only if P(A and B) > P(A) $\times$ P(B).

NOTE 2 See 9.5 as an example of dependent failure consideration between layers of protection.

NOTE 3 Dependent failure includes common cause (see 3.2.6).

3.2.13
detected
revealed
overt
in relation to hardware failures and software faults, detected by the diagnostic tests or through normal operation

3.2.14
device
functional unit of hardware or software, or both, capable of accomplishing a specified purpose (for example, field devices; equipment connected to the field side of the SIS I/O terminals; such equipment includes field wiring, sensors, final elements, logic solvers, and those operator interface devices hard-wired to SIS I/O terminals)

3.2.15
diagnostic coverage (DC)
ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests. Diagnostic 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-DC) $\times$ $\lambda_{total\ failure\ rate}$.

NOTE 2 Diagnostic coverage is applied to components or subsystems of a safety instrumented system. For example, the diagnostic coverage is typically determined for a sensor, final element or a logic solver.

NOTE 3 For safety applications the diagnostic coverage is typically applied to the safe and dangerous failures of a component or subsystem. For example, the diagnostic coverage for the dangerous failures of a component or subsystem is DC = $\lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate.

3.2.16
diversity
existence of different means performing a required function

NOTE Diversity may be achieved by different physical methods 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).

3.2.18
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.

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.

3.2.20
failure
termination of the ability of a functional unit to perform a required function

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 3 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 Failures are either random or systematic (see 3.2.62 and 3.2.85).

3.2.21
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

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]

3.2.22
fault avoidance
use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety life cycle of the safety instrumented system

3.2.23
fault tolerance
ability of a functional unit 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]

3.2.24
final element
part of a safety instrumented system which implements the physical action necessary to achieve a safe state

NOTE Examples are valves, switch gear, motors including their auxiliary elements, for example, a solenoid valve and actuator if involved in the safety instrumented function.

3.2.25
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.

3.2.26
functional safety assessment
investigation, based on evidence, to judge the functional safety achieved by one or more protection layers

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

3.2.27
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 A functional safety audit may be carried out as part of a functional safety assessment.

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.

3.2.29
hardware safety integrity
part of the safety integrity of the safety instrumented function relating to random hardware failures in a dangerous mode of failure

NOTE 1 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 that are relevant in this context are the overall dangerous failure rate and the probability of failure to operate on demand.

NOTE 2 See 3.2.86.

NOTE 3 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.30
harm
physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment

NOTE This definition matches ISO/IEC Guide 51.

3.2.31
hazard
potential source of harm

NOTE 1 This definition (without notes) matches 3.4 of ISO/IEC Guide 51.

NOTE 2 The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

3.2.32
human error
mistake
human action or inaction that produces an unintended 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”.

3.2.33
impact analysis
activity of determining the effect that a change to a function or component will have to other functions or components in that system as well as to 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

3.2.35
independent organization
organization which is separate and distinct, by management and other resources, from the organizations 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

3.2.36
independent person
person who is separate and distinct from the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation and does not have direct responsibility for those activities

3.2.37
input function
function which monitors the process and its associated equipment in order to provide input information for the logic solver

NOTE An input function could be a manual function.

3.2.38
instrument
apparatus used in performing an action (typically found in instrumented systems)

NOTE Instrumented systems in the process sector are typically composed of sensors (for example, pressure, flow, temperature transmitters), logic solvers or control systems (for example, programmable controllers, distributed control systems), and final elements (for example, control valves). In special cases, instrumented systems can be safety instrumented systems (see 3.2.72).

3.2.39
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); logic functions provide the transformation from one or more input functions to one or more output functions

NOTE For further guidance, see IEC 61131-3 and IEC 60617-12.

3.2.40
logic solver
that portion of either a BPCS or SIS that performs one or more logic function(s)

NOTE 1 In IEC 61511 the following terms for logic systems are used:

– electrical logic systems for electro-mechanical technology;

– electronic logic systems for electronic technology;

– PE logic system for programmable electronic systems.

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

3.2.40.1
safety configured logic solver
general purpose industrial grade PE logic solver which is specifically configured for use in safety applications in accordance with 11.5

3.2.41
maintenance/engineering interface
maintenance/engineering interface is that hardware and software provided to allow proper SIS maintenance or modification. It 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

3.2.42
mitigation
action that reduces the consequence(s) of a hazardous event

NOTE Examples include emergency depressurization on detection of confirmed fire or gas leak.

3.2.43
mode of operation
way in which a safety instrumented function operates

3.2.43.1
demand mode safety instrumented function
where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS

3.2.43.2
continuous mode safety instrumented function
where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it

NOTE 1 Continuous mode covers those safety instrumented functions which implement continuous control to maintain functional safety.

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.

3.2.44
module
self-contained assembly of hardware components that performs a specific 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

NOTE 1 In the context of IEC 61131-3, 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.

3.2.45
MooN
safety instrumented system, or part thereof, made up of "**N**" independent channels, which are so connected, that "**M**" channels are sufficient to perform the safety instrumented function

3.2.46
necessary risk reduction
risk reduction required to ensure that the risk is reduced to a tolerable level

3.2.47
non-programmable (NP) system
system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software)

NOTE Examples would include hard-wired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

3.2.48
operator interface
means by which information is communicated between a human operator(s) and the SIS (for example, CRTs, indicating lights, push-buttons, horns, alarms); 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.

3.2.50
output function
function which controls the process and its associated equipment according to final actuator information from the logic function

3.2.51
phase
period within the safety life cycle where activities described in this standard take place

3.2.52
prevention
action that reduces the frequency of occurrence of a hazardous event

3.2.53
prior use
see “proven-in-use” (see 3.2.60)

3.2.54
process risk
risk arising from the process conditions caused by abnormal events (including BPCS malfunction)

NOTE 1 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 Process risk analysis is described in IEC 61511-3. 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 Assessment of this risk should include associated human factor issues.

NOTE 4 This term equates to “EUC risk” in IEC 61508-4.

3.2.55
programmable electronics (PE)
electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units

NOTE 1 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

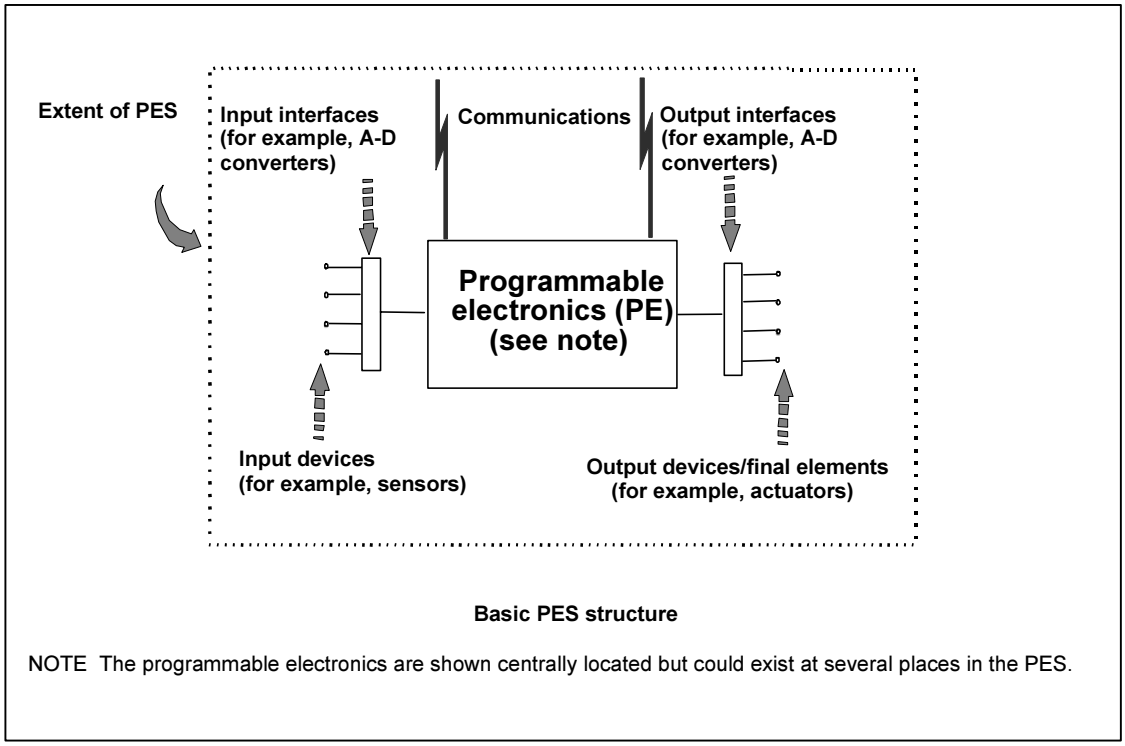
– smart sensors and final elements;

– 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.

3.2.56
programmable electronic system (PES)
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements 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 6)



Basic PES structure

NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.

IEC 3245/02

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

3.2.57
programming
process of designing, writing and testing a set of instructions for solving a problem or processing data

NOTE In this standard, programming is typically associated with PE.

3.2.58
proof test
test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality

3.2.59
protection layer
any independent mechanism that reduces risk by control, prevention or mitigation

NOTE It could be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical engineering mechanism such as a relief valve, a safety instrumented system 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.

3.2.61
quality
totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs

NOTE See ISO 9000 for more details.

3.2.62
random hardware failure
failure, occurring at a random time, which results from a variety of degradation mechanisms in the hardware

NOTE 1 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 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.

3.2.63
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)

NOTE 1 Examples are the use of duplicate functional components and the addition of parity bits.

NOTE 2 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.

3.2.64
risk
combination of the frequency of occurrence of harm and the severity of that harm

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

3.2.65
safe failure
failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state

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.

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

3.2.66
safe state
state of the process when safety is achieved

NOTE 1 In going from a potentially hazardous condition to the final safe state, the process may have to go through a number of intermediate safe-states. 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 2 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.67
safety
freedom from unacceptable risk

NOTE This definition is according to ISO/IEC Guide 51.

3.2.68
safety function
function to be implemented by an SIS, other technology safety related system or external risk, reduction facilities, 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.

3.2.71
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

3.2.72
safety instrumented system (SIS)
instrumented system used to implement one or more safety instrumented functions. 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 3 A SIS may or may not include software.

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.

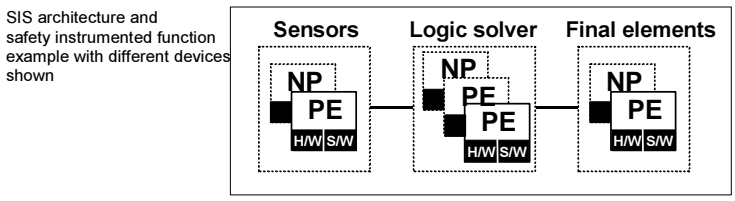


Figure 7 – Example of SIS architecture

3.2.73
safety integrity
average probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all the stated conditions within a stated period of time

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 3 In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) which lead to an unsafe state should be included; for example, hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of a safety instrumented function failing to operate on demand. However, the safety integrity of an SIF also depends on many factors, which cannot be accurately quantified but can only be considered qualitatively.

NOTE 4 Safety integrity comprises hardware safety integrity and systematic safety integrity.

3.2.74
safety integrity level (SIL)
discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest

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

3.2.75
safety integrity requirements specification
specification that contains the safety integrity requirements of the safety instrumented functions that have to be performed by the safety instrumented system(s)

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.

3.2.76
safety life cycle
necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use

NOTE 1 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 this standard.

NOTE 2 The safety life-cycle model used in IEC 61511 is shown in Figure 8.

3.2.77
safety manual
manual which defines how the device, subsystem or system can be safely applied

NOTE This could be a stand-alone document, an instructional manual, a programming manual, a standard document, or included in the user document(s) defining application limitations.

3.2.78
safety requirements specification
specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems

3.2.79
safety software
software in a safety instrumented system with application, embedded or utility software functionality

3.2.80
sensor
device or combination of devices, which measure the process condition (for example, transmitters, transducers, process switches, position switches)

3.2.81
software
intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

NOTE 1 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.

3.2.81.1
software languages in SIS subsystems

3.2.81.1.1
fixed program language (FPL)
in this type of language, the user is limited to adjustment of a few parameters (for example, range of the pressure transmitter, alarm levels, network addresses).

NOTE Typical examples of devices with FPL are: smart sensor (for example, pressure transmitter), smart valve, sequence of events controller, dedicated smart alarm box, small data logging systems.

3.2.81.1.2
limited variability language (LVL)
this type of language is designed to be comprehensible to process sector users, and provides the capability to combine predefined, application specific, library functions to implement the safety requirements specifications. An LVL provides a close functional correspondence with the functions required to achieve the application.

NOTE 1 Typical examples of LVL are given in IEC 61131-3. They include ladder diagram, function block diagram and sequential function chart.

NOTE 2 Typical example of systems using LVL: standard PLC (for example, programmable logic controller for burner management).

3.2.81.1.3
full variability language (FVL)
this type of language is designed to be comprehensible to computer programmers and provides the capability to implement a wide variety of functions and applications

NOTE 1 Typical example of systems using FVL are general purpose computers.

NOTE 2 In the process sector, FVL is found in embedded software and rarely in application software.

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

3.2.81.2
software program type

3.2.81.2.1
application software
software specific to the user application. In general, it contains logic sequences, permissives, limits and expressions that control the appropriate input, output, calculations, decisions necessary to meet the safety instrumented functional requirements. See fixed and limited variability language

3.2.81.2.2
embedded software
software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user. Embedded software is also referred to as firmware or system software. See 3.2.81.1.3, full variability language

3.2.81.2.3
utility software
software tools for the creation, modification, and documentation of application programs. These software tools are not required for the operation of the SIS

3.2.82
software life cycle
activities occurring during a period of time that starts when software is conceived and ends when the software is permanently disused

NOTE 1 A software life cycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and modification phase.

NOTE 2 Software cannot be maintained; rather, it is modified.

3.2.83
subsystem
see “system”

3.2.84
system
set of elements, which interact according to a design; 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 A person can be part of a system.

NOTE 2 This definition differs from IEV 351-01-01.

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).

3.2.85
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE 1 Corrective maintenance without modification would usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

NOTE 3 This definition (up to note 2) matches IEV 191-04-19.

NOTE 4 Examples of systematic failure causes including human error in

– the safety requirements specification;

– the design, manufacture, installation and operation of the hardware;

– the design and/or implementation of the software.

3.2.86
systematic safety integrity
that part of the safety integrity of safety instrumented function relating to systematic failures (see note 3 of 3.2.73) in a dangerous mode of failure

NOTE 1 Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity).

NOTE 2 See also 3.2.29.

3.2.87
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)

NOTE The numerical values for the target failure measures are given in Tables 3 and 4.

3.2.88
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.

3.2.89
tolerable risk
risk which is accepted in a given context based on the current values of society

NOTE See IEC 61511-3.

[ISO/IEC Guide 51]

3.2.90
undetected
unrevealed
covert
in relation to hardware and software faults not found by the diagnostic tests or during normal operation

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

3.2.91
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

3.2.92
verification
activity of demonstrating for each phase of the relevant 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 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.

3.2.93
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 The watchdog confirms that the software system is operating correctly by the regular resetting of an external device (for example, hardware electronic watchdog timer) by an output device controlled by the software.

NOTE 2 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 a safe state. The watchdog is used to increase the on-line diagnostic coverage of the PE logic solver (see 3.2.15 and 3.2.40).

4 Conformance to this International Standard

To conform to this International Standard, it shall be shown that each of the requirements outlined in Clauses 5 through 19 has been satisfied to the defined criteria and therefore the clause objective(s) has(have) been met.

5 Management of functional safety

5.1 Objective

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

NOTE This clause is solely aimed at the achievement and maintenance of the functional safety of safety instrumented systems 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 safety shall be identified together with the means for evaluating its 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 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 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 be addressed when considering the competence of persons, departments, organizations or other units involved in 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 (for example, electrical, electronic or programmable electronic);

c) engineering knowledge, training and experience appropriate to the sensors and final elements;

d) safety engineering knowledge (for example, process safety analysis);

e) knowledge of the legal and safety regulatory requirements;

f) adequate management and leadership skills appropriate to their role in safety life-cycle activities;

g) understanding of the potential consequence of an event;

h) the safety integrity level of the safety instrumented functions;

i) the novelty and complexity of the application and the technology.

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 economical reasons.

5.2.4 Planning

Safety planning shall take place to define the activities that are required to be carried out along with the persons, department, organization or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire safety life cycle (see Clause 6).

NOTE The safety planning may be incorporated in

– a section in the quality plan entitled “safety plan”; or

– a separate document entitled “safety 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 safety instrumented system arising from

y) hazard analysis and risk assessment;

z) assessment and auditing activities;

aa) verification activities;

bb) validation activities;

cc) post-incident and post-accident activities.

5.2.5.2 Any supplier, providing products or services to an organization, having overall responsibility for one or more phases of the 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 establish the adequacy of the quality management system.

5.2.5.3 Procedures shall be implemented to evaluate the performance of the safety instrumented system against its safety requirements including procedures for

- identification and prevention of systematic failures which could jeopardize safety;
- assessing whether dangerous failure rates of the safety instrumented system 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 the demand rate on the safety instrumented functions during actual operation to verify the assumptions made during risk assessment when the integrity level requirements were determined.

5.2.6 Assessment, auditing and revisions

5.2.6.1 Functional safety assessment

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

5.2.6.1.2 The membership of the assessment team shall include at least one senior competent person not involved in the project design team.

NOTE 1 When the assessment team is large, consideration should be given to having more than one senior competent individual on the team who is independent from the project team.

NOTE 2 The following should be considered when planning a functional safety assessment:

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

5.2.6.1.3 The stages in the safety life cycle at which the functional safety assessment activities are to be carried out shall be identified during safety planning.

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

NOTE 2 Consideration should be given to carrying out functional safety assessment activities at the following stages (see Figure 8).

– Stage 1 - After the hazard and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification has been developed.
– Stage 2 - After the safety instrumented system has been designed.
– Stage 3 - After the installation, pre-commissioning and final validation of the safety instrumented system 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 safety instrumented system.

NOTE 3 The number, size and scope of functional safety assessment activities should depend upon the specific circumstances. The factors in this decision are likely to include

– size of project;
– degree of complexity;
– safety integrity level;
– duration of project;
– consequence in the event of failure;
– degree of standardization of design features;
– safety regulatory requirements;
– previous experience with a similar design.

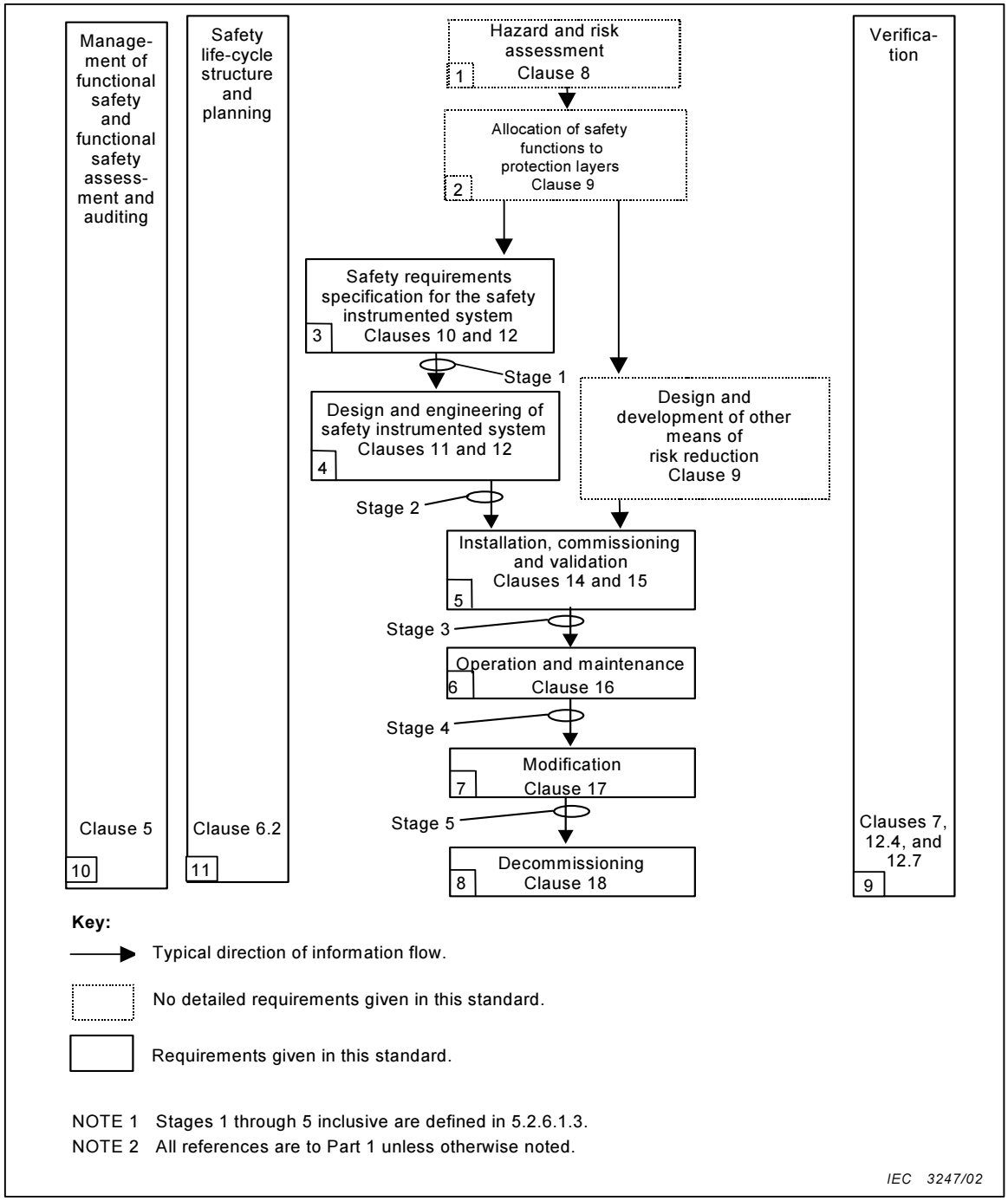


Figure 8 – SIS safety life-cycle phases and functional safety assessment stages

5.2.6.1.4 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 assessment team shall confirm, prior to the identified hazards being present, that

- the hazard and risk assessment has been carried out (see 8.1);
- the recommendations arising from the hazard and risk assessment that apply to the safety instrumented system have been implemented or resolved;
- project design change procedures are in place and have been properly implemented;

- the recommendations arising from the previous functional safety assessment have been resolved;
- the safety instrumented system is designed, constructed and installed in accordance with the safety requirement specification, any differences having been identified and resolved;
- the safety, operating, maintenance and emergency procedures pertaining to the safety instrumented system are in place;
- the safety instrumented system validation planning is appropriate and the validation activities have been completed;
- the employee training has been completed and appropriate information about the safety instrumented system has been provided to the maintenance and operating personnel;
- plans or strategies for implementing further functional safety assessments are in place.

5.2.6.1.5 Where development and production tools are used for any safety life-cycle activity, they shall themselves be subject to a functional safety assessment.

NOTE 1 The degree to which such tools should need to be addressed will depend upon their impact on the safety 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 of tools includes, but is not limited to, traceability to calibration standards, operating history and defect list.

5.2.6.1.6 The results of the functional safety assessment shall be available together with any recommendation coming from this assessment.

5.2.6.1.7 All relevant information shall be made available to the functional safety assessment team upon their request.

5.2.6.2 Auditing and revision

5.2.6.2.1 Procedures shall be defined and executed for auditing compliance with requirements including

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

5.2.6.2.2 Management of modification procedures shall be in place to initiate, document, review, implement and approve changes to the safety instrumented system other than replacement in kind (i.e. like for like).

5.2.7 SIS configuration management

5.2.7.1 Requirements

5.2.7.1.1 Procedures for configuration management of the SIS during the SIS and software safety life-cycle phases shall be available; in particular, the following should be specified:

- the stage at which formal configuration control is to be implemented;
- the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);
- the procedures for preventing unauthorized items from entering service.

6 Safety life-cycle requirements

6.1 Objectives

The objectives of this clause are:

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

NOTE The overall approach of this standard is shown in Figures 8, 10, and 11. It should be stressed that this approach is for illustration and is only meant to indicate the typical safety life-cycle activities from initial conception through decommissioning.

6.2 Requirements

6.2.1 A safety life-cycle incorporating the requirements of this standard shall be defined during safety planning.

6.2.2 Each phase of the 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

Safety life-cycle phase or activity		Objectives	Require-ments	Inputs	Outputs
Figure 8 box number	Title		Clause or subclause		
1	Hazard and risk assessment	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	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 safety instrumented function, the associated safety integrity level	9	A description of the required safety instrumented function(s) 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 safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety	10	Description of allocation of safety requirements (see clause 9)	SIS safety requirements; software safety requirements
4	SIS design and engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity	11 and 12.4	SIS safety requirements Software safety requirements	Design of the SIS in conformance with the SIS safety requirements; planning for the SIS integration test

Table 2 *(continued)*

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 safety instrumented functions and the required safety integrity	12.3, 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 results of SIS integration tests Results of the installation, commissioning and validation activities
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	SIS requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities
Safety life-cycle phase or activity		**Objectives**	**Requirements Clause or subclause**	**Inputs**	**Outputs**
Figure 8 box number	**Title**				
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modification
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remain appropriate	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	7, 12.7	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase
10	SIS functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the SIS	5	Planning for SIS functional safety assessment SIS safety requirement	Results of SIS functional safety assessment

6.2.3 For all safety life-cycle phases, safety planning shall take place to define the criteria, techniques, measures and procedures to

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

7 Verification

7.1 Objective

The objective of this clause is to demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases (Figure 8) of the safety life cycle identified by the verification planning.

7.1.1 Requirements

Verification planning shall define all activities required for the appropriate phase (Figure 8) of the safety life cycle. It shall conform to this standard by providing 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;
- how to handle non-conformances;
- tools and supporting analysis.

7.1.1.1 Verification shall be performed according to the verification planning.

7.1.1.2 The results of the verification process shall be available.

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 safety integrity level required.

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

8 Process hazard and risk assessment

8.1 Objectives

The objectives of the requirements of this clause are:

- to determine the hazards and hazardous events of the process and associated equipment;
- to determine the sequence of events leading to the hazardous event;
- to determine the process risks associated with the hazardous event;
- to determine any requirements for risk reduction;
- to determine the safety functions required to achieve the necessary risk reduction;
- to determine if any of the safety functions are safety instrumented functions (see Clause 9).

NOTE 1 Clause 8 of this standard is addressed to process engineers, hazard and risk specialists, safety managers as well as instrument engineers. The purpose is to recognize the multi-disciplinary approach typically required for the determination of safety instrumented functions.

NOTE 2 Where reasonably practicable, processes should be designed to be inherently safe. When this is not practical, risk reduction methods such as mechanical protection systems and safety instrumented systems may need to be added to the design. These systems may act alone or in combination with each other.

NOTE 3 Typical risk reduction methods found in process plants are indicated in Figure 9 (no hierarchy implied).

8.2 Requirements

8.2.1 A hazard and risk assessment shall be carried out on the 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 consequences and likelihood of the event;
- consideration of conditions such as normal operation, start-up, shutdown, maintenance, process upset, emergency shutdown;
- the determination of requirements for additional risk reduction necessary to achieve the required 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 and equipment failure rates, 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 safety instrumented function(s) (see Clause 9).

NOTE 1 In determining the safety integrity requirements, account will need to be taken of the effects of common cause between systems that create demands and the protection systems that are designed to respond to those demands. An example of this would be where demands can arise through control system failure and the equipment used within the protection systems is similar or identical to the equipment used within the control system. In such cases, a demand caused by a failure of equipment in the control system may not be responded to effectively if a common cause has rendered similar equipment in the protection system 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 will not necessarily have been completed. In such cases, it will be necessary to reconsider the requirements for safety integrity and safety instrumented function once the design of the safety instrumented system and other layers of protection 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 SIL of safety instrumented functions are illustrated in IEC 61511-3.

8.2.2 The dangerous failure rate of a BPCS (which does not conform to IEC 61511) that places a demand on a protection layer shall not be assumed to be better than 10^{-5} per hour.

8.2.3 The hazard and risk assessment 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 have to be assigned as numerical value. Graphical approaches (see IEC 61511-3) can also be used.

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

9 Allocation of safety functions to protection layers

9.1 Objectives

The objectives of the requirements of this clause are to

- allocate safety functions to protection layers;
- determine the required safety instrumented functions;
- determine, for each safety instrumented function, the associated safety integrity level.

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

9.2 Requirements of the allocation process

9.2.1 The allocation process shall result in

- the allocation of safety functions 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.

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

9.2.2 The required safety integrity level of a safety instrumented function shall be derived by taking into account the required risk reduction that is to be provided by that function.

NOTE See IEC 61511-3 for guidance.

9.2.3 For each safety instrumented function operating in demand mode, the required SIL shall be specified in accordance with either Table 3 or Table 4. 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 safety instrumented function operating in continuous mode of operation, the required SIL shall be specified in accordance with Table 4.

Table 3 – Safety integrity levels: probability of failure on demand

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**Target average probability of failure on demand**	**Target 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 – Safety integrity levels: frequency of dangerous failures of the SIF

CONTINUOUS MODE OF OPERATION	
Safety integrity level (SIL)	**Target frequency of dangerous failures to perform the safety instrumented function (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 See 3.2.43 for further explanation.

NOTE 2 The safety integrity level is defined numerically so as to provide an objective target to compare alternative 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 frequency of dangerous failures per hour for a continuous mode safety instrumented function is determined by considering the risk (in terms of hazard rate) caused by failure of the safety instrumented function acting in continuous mode together with the failure rate of other equipment that leads to the same risk, taking into consideration contributions from 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).

9.3 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.

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

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

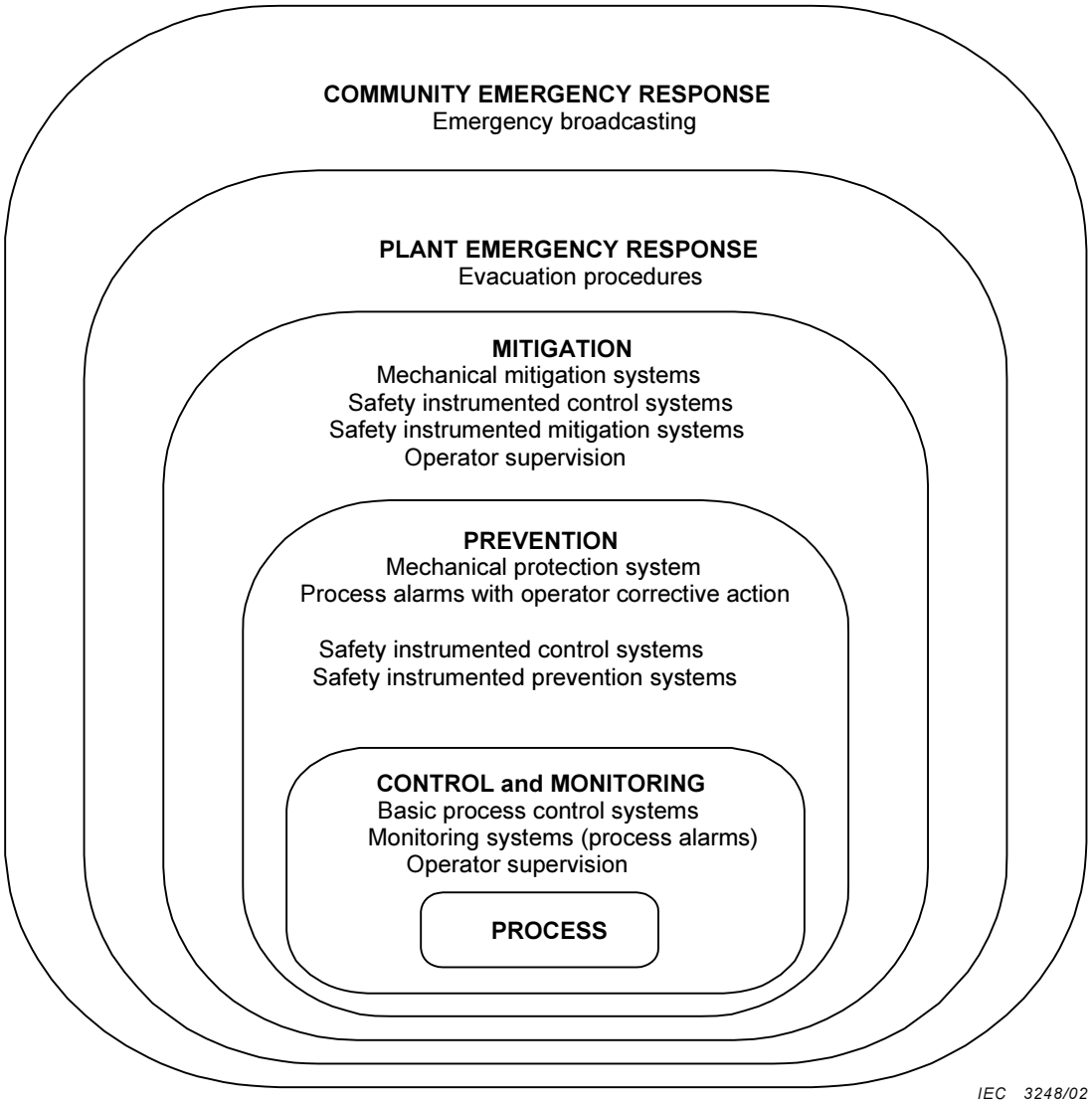


Figure 9 – Typical risk reduction methods found in process plants

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

NOTE When considering how much risk reduction credit to be given to a BPCS, consideration should be given to the fact that a part of the BPCS may also be an initiating source for an event.

9.4.3 If a risk reduction factor greater than 10 is claimed for the BPCS, then it shall be designed to the requirements within this standard.

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

9.5.1 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.

NOTE For a definition of dependent failure, see 3.2.12.

9.5.2 The assessment shall consider the following:

- independency 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?).

10 SIS safety requirements specification

10.1 Objective

The objective of this clause is to specify the requirements for the safety instrumented function(s).

10.2 General requirements

10.2.1 The safety requirements shall be derived from the allocation of safety instrumented functions and from those requirements identified during safety planning.

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

– clear, precise, verifiable, maintainable and feasible; and

– written to aid comprehension by those who are likely to utilize the information at any phase of the life cycle.

10.3 SIS safety requirements

10.3.1 These requirements shall be sufficient to design the SIS and shall include the following:

- a description of all the safety instrumented functions necessary to achieve the required functional safety;
- requirements to identify and take account of common cause failures;
- a definition of the safe state of the process for each identified safety instrumented function;
- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system);
- the assumed sources of demand and demand rate on the safety instrumented function;
- requirement for proof-test intervals;
- response time requirements for the SIS to bring the process to a safe state;
- the safety integrity level and mode of operation (demand/continuous) for each safety instrumented function;
- a description of SIS process measurements and their trip points;
- a description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves;
- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives;
- requirements for manual shutdown;
- requirements relating to energize or de-energize to trip;
- requirements for resetting the SIS after a shutdown;
- maximum allowable spurious trip rate;
- failure modes and desired response of the SIS (for example, 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 within each mode;
- the application software safety requirements as listed in 12.2.2;
- requirements for overrides/inhibits/bypasses including how they will be cleared;
- the specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors;
- the mean time to repair 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;
- the extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radiofrequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;
- identification to normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these modes of operation;
- definition of the requirements for any safety instrumented function necessary to survive a major accident event, for example, 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.

11 SIS design and engineering

11.1 Objective

The objective of the requirements of this clause is to design one or multiple SIS to provide the safety instrumented function(s) and meet the specified safety integrity level(s).

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 this clause.

11.2.2 Where the SIS is to implement both safety and non-safety instrumented function(s) then all the hardware and software 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.

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 safety instrumented functions of different safety integrity levels, then the shared or common hardware and software shall conform to the highest safety integrity level 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.

11.2.4 If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.

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

NOTE 2 Devices of the SIS may also be used for functions of the basic process control system if it can be shown that a failure of the basic process control system does not compromise the safety instrumented functions of the safety instrumented system.

11.2.5 Requirements for operability, maintainability 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).

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 task assigned to operators and maintenance staff. The design of all human-machine interfaces shall follow good human factors practice and shall accommodate the likely level of training or awareness that operators should receive.

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

11.2.8 Manual means (for example, emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the safety requirement specifications.

11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependence 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 shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, 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 for 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 because if the shared component fails, a demand will be created immediately to which the SIS may not be capable of responding . For that reason, additional analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.

11.2.11 For subsystems that on loss of power do not fail to the safe state, all of the following requirements shall be met and action taken according to 11.3:

- loss of circuit integrity is detected (for example, end-of-line monitoring);
- 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.

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.

11.4 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.

11.5 Requirements for selection of components and subsystems

11.5.1 Objectives

11.5.1.1 The first objective of the requirements of this clause is to specify the requirements for the selection of components or subsystems which are to be used as part of a safety instrumented system.

11.5.1.2 The second objective of the requirements of this clause is to specify the requirements to enable a component or subsystem to be integrated in the architecture of a SIS.

11.5.1.3 The third objective of the requirements of this clause is to specify acceptance criteria for components and subsystems in terms of associated safety instrumented functions and safety integrity.

11.5.2 General requirements

11.5.2.1 Components and subsystems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with 11.4 and 11.5.3 to 11.5.6, as appropriate.

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.

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 based on prior use

11.5.3.1 Appropriate evidence shall be available that the components and subsystems are suitable for use in the safety instrumented system.

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.

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

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;
- demonstration of the performance of the components or subsystems in similar operating profiles and physical environments;

  NOTE In the case of field devices (for example, sensors and final elements) fulfilling a given function, this function 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 to satisfy this requirement.

- the volume of the operating experience.

  NOTE 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 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 is included in the list where relevant.

11.5.4 Requirements for selection of FPL programmable components and subsystems (for example, field devices) based on prior use

11.5.4.1 The requirements of 11.5.2 and 11.5.3 apply.

11.5.4.2 Unused features of the components and subsystems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.

11.5.4.3 For the specific configuration and operational profile of the hardware and software, the evidence of suitability shall consider

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

11.5.4.4 For SIL 3 applications, a 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 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 safety instrumented system, 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 the selection of LVL programmable components and subsystems (for example, logic solvers) based on prior use

11.5.5.1 The following requirements may only be applied to PE logic solvers used in safety instrumented systems which implement SIL 1 or SIL 2 safety instrumented functions.

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 as experienced previously, and the operational profile and physical environment of the component or subsystem when used within the safety instrumented system, 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 safety instrumented system 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 safety instrumented function;
- the complexity and functionality of the component or subsystem.

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 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 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 safety instrumented system, 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; 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;
  - it has been tested 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 nor dynamic reconfiguration;
  - documented fault-insertion 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 the selection of FVL programmable components and subsystems (for example, logic solvers)

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

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. Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, cooking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse lines.

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

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

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.

11.6.4 Smart sensors shall be write-protected to prevent inadvertent modification from a remote location, unless appropriate safety review allows the use of read/write. The review should take into account human factors such as failure to follow procedures.

11.7 Interfaces

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).

11.7.1 Operator interface requirements

11.7.1.1 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.

11.7.1.2 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. 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 be a repeat confirmation step.

11.7.1.3 Bypass switches shall be protected by key locks or passwords to prevent unauthorized use.

11.7.1.4 The SIS status information that is critical to maintaining the SIL 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.

11.7.1.5 The SIS operator interface design shall be such as to prevent changes to SIS application software. Where safety information needs to be transmitted from the BPCS to the SIS, then systems should be used which can selectively allow writing from the BPCS to specific SIS variables. Equipment or procedures should be applied to confirm that the proper selection has been transmitted and received by the SIS and does not compromise the safety functionality of the SIS.

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.

11.7.2 Maintenance/engineering interface requirements

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

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

- SIS operating mode, program, data, means of disabling alarm communication, test, bypass, maintenance;
- SIS diagnostic, voting and fault handling services;
- add, delete, or modify application software;
- 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.

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

11.7.2.4 Enabling and disabling the read-write access shall be carried out only by a configuration or programming process using the maintenance/engineering interface with appropriate documentation and security measures.

11.7.3 Communication interface requirements

11.7.3.1 The design of the 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 a safe state.

11.7.3.2 The SIS shall be able to communicate with the BPCS and peripherals with no impact on the SIF.

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

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

NOTE An alternate medium (for example, fibre optics) may 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. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line testing 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 safety requirement specifications.
- The operator shall be alerted to the bypass of any portion of the SIS via an alarm and/or operating procedure.

11.8.4 Forcing of inputs and outputs in PE SIS shall not be used as a part of

- application software;
- operating procedure(s);
- 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

11.9.1 The probability of failure on demand of each safety instrumented function shall be equal to, or less than, the target failure measure as specified in the safety requirement specifications. This shall be verified 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.

11.9.2 The calculated probability of failure of each safety instrumented function due to hardware failures shall take into account

a) the architecture of the SIS as it relates to each safety instrumented function under consideration;

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

c) the estimated rate of failure of each subsystem, due to random hardware faults, in any modes which would cause a dangerous failure of the SIS which are undetected by the diagnostic 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 susceptibility of the SIS to common cause failures;

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

f) the intervals at which proof tests are undertaken;

g) the repair times for detected failures;

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

i) the estimated rate of dangerous failure of any human 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).

NOTE 1 Modelling methods are available and the most appropriate method is a matter for the analyst and should depend on the circumstances. Available methods include (see IEC 61508-6, Annex B)

– simulation;

– cause consequence analysis;

– fault-tree analysis;

– Markov models;

– reliability block diagrams.

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.

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.

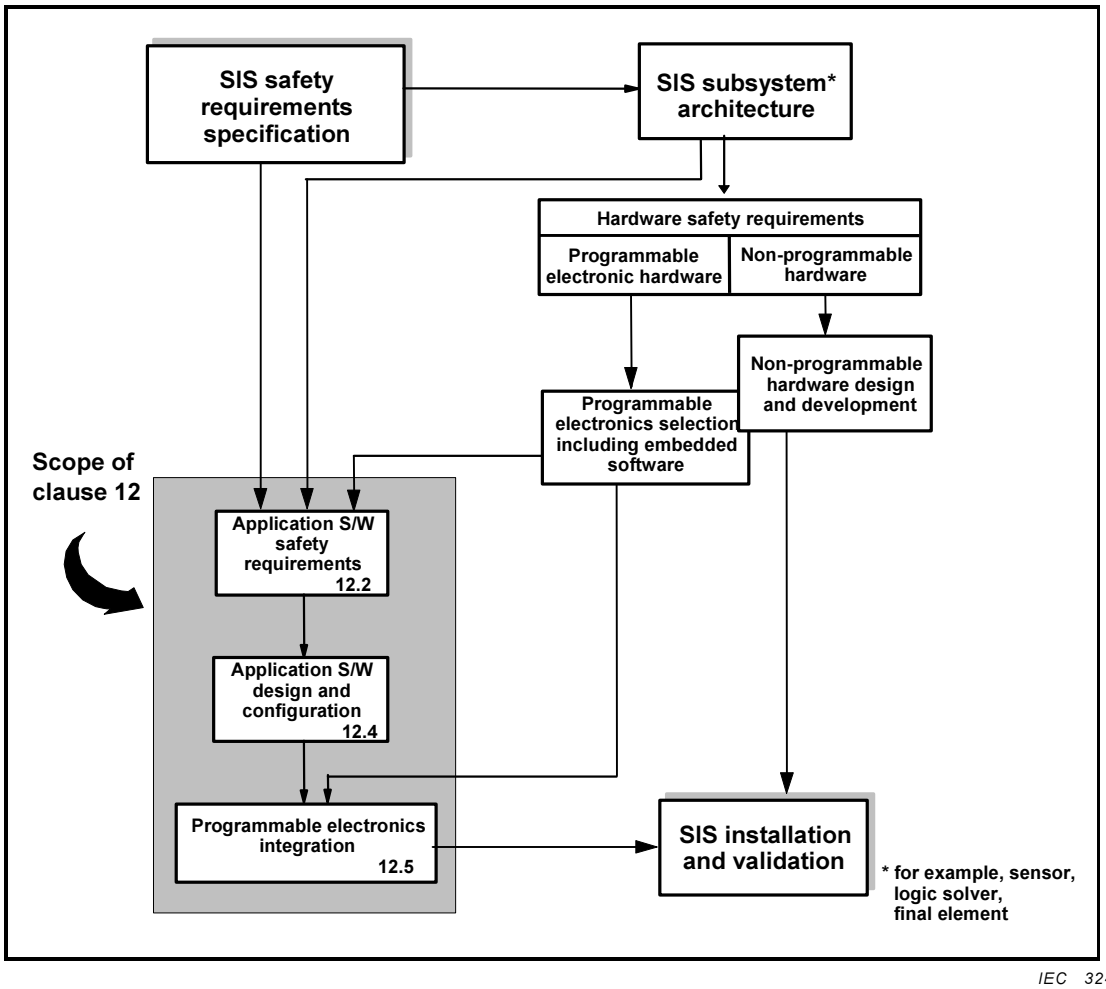


Figure 10 – Application software safety life cycle and its relationship to the SIS safety life cycle

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.

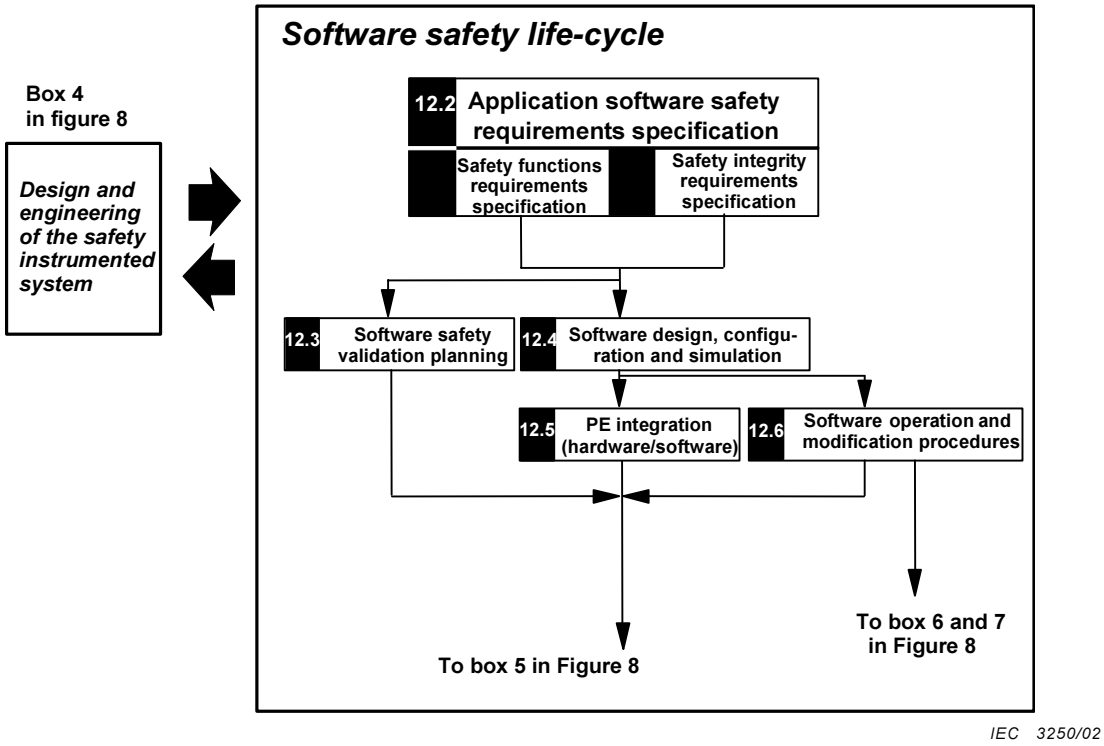


Figure 11 – Application software safety life cycle (in realization phase)

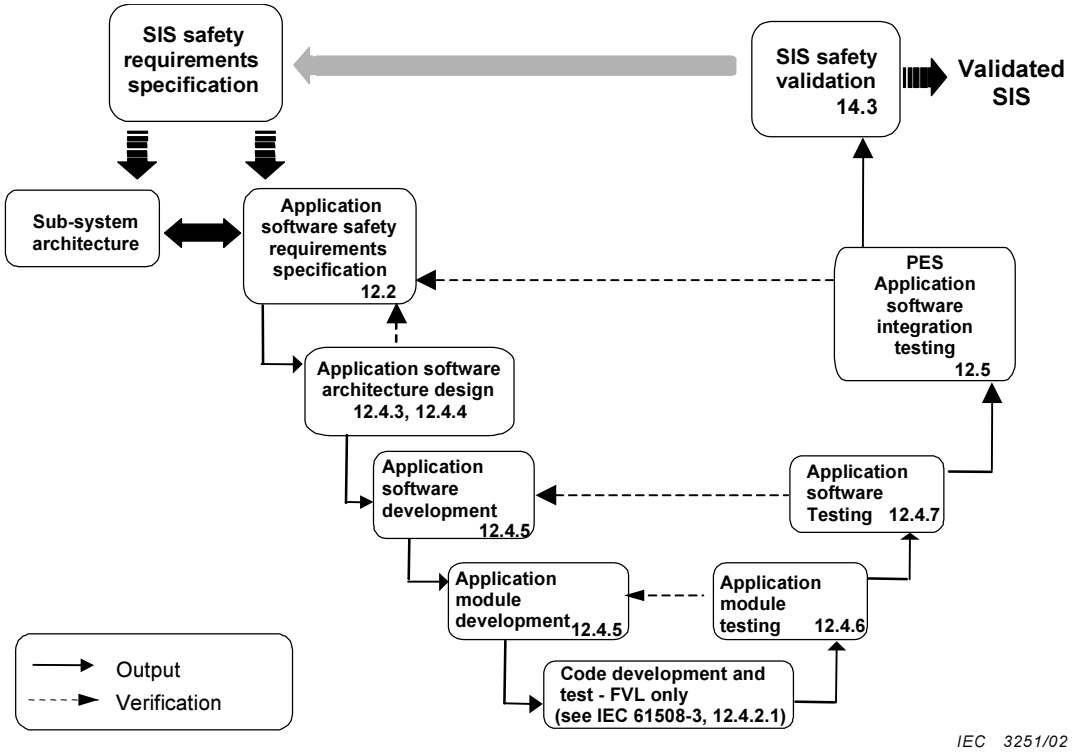


Figure 12 – Software development life cycle (the V-model)

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.

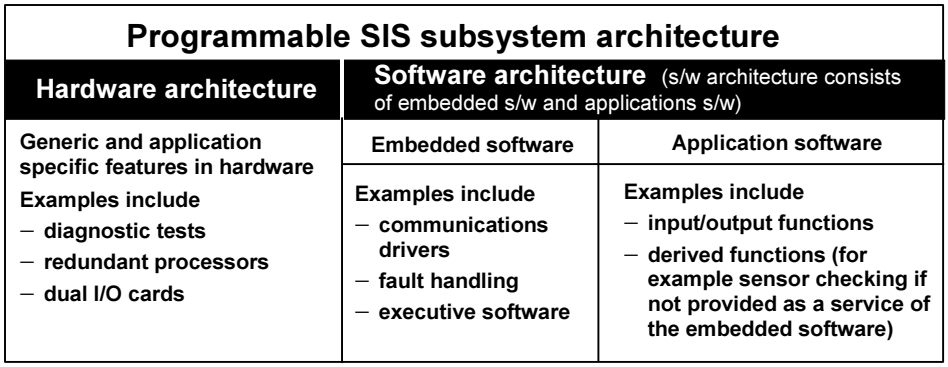


Figure 13 – Relationship between the hardware and software architectures of SIS

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.

13 Factory acceptance testing (FAT)

NOTE This clause is informative.

13.1 Objectives

13.1.1 The objective of a factory acceptance test (FAT) is to test the logic solver and associated software together to ensure it satisfies the requirements defined in the safety requirement specification. By testing the logic solver and associated software prior to installing in a plant, errors can be readily identified and corrected.

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

13.2 Recommendations

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

NOTE 1 Close co-operation between the logic solver supplier and design contractor may 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 subsystems of an SIS 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 specify the following

- Types of tests to be performed including black-box system functionality tests (i.e., 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); performance tests (timing, reliability and availability, integrity, safety targets and constraints), environmental tests (including EMC, life- and stress-testing), interface testing, testing in degraded and/or fault modes, exception testing, application of the SIS maintenance and operating manuals.
- Test cases, test description and test data.

  NOTE It is very important to make clear who is responsible for developing the test case and who is going to be responsible for carrying out the test and witnessing the test.
- Dependence on other systems/interfaces.
- Test environment and tools.
- Logic solver 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.

NOTE For tests that cannot be physically demonstrated, these are normally resolved by a formal argument as to why the SIS achieves the requirement, target or constraint.

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

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

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

- the version of the test planning being used;
- the safety instrumented function 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 be documented, stating

a) the test cases;

b) the test results; and

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

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

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

a) the extent of impact on each safety instrumented function; and

b) the extent of re-test which should be defined and implemented.

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

14 SIS installation and commissioning

14.1 Objectives

14.1.1 The objectives of the requirements of this clause are to

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

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 safety instrumented system components shall be properly installed according to the design and installation plan(s) (see 14.2.1).

14.2.3 The safety instrumented system 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;
- all field devices are operational;
- logic solver and input/outputs are operational;
- the interfaces to other systems and peripherals are operational.

14.2.4 Appropriate records of the commissioning of the SIS shall be produced, stating the test results 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 on safety 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

15.1.1 The objective of the requirements of this clause is to validate, through inspection and testing, that the installed and commissioned safety instrumented system and its associated safety instrumented functions achieve the requirements as stated in the safety requirement specification.

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

15.2 Requirements

15.2.1 Validation planning of the SIS shall define all activities required for validation. The following items shall be included**.**

- The validation activities including validation of the safety instrumented system(s) with respect to the safety requirements specification including implementation and resolution of resulting recommendations.
- Validation of all relevant modes of operation 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;
- the procedures, measures and techniques to be used for validation;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities and levels of independence for validation activities;
- reference to information against which validation shall be carried out (for example, cause and effect chart).

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

15.2.2 Additional validation planning for the safety application software shall include the following.

d) Identification of the safety software which needs to be validated for each mode of process operation before commissioning commences.

e) Information on the technical strategy for the validation including
   - manual and automated techniques;
   - static and dynamic techniques;
   - analytical and statistical techniques.

f) In accordance with b), the measures (techniques) and procedures that shall be used for confirming that each safety instrumented function conforms with the specified requirements for the software safety instrumented functions (see 12.2) and the specified requirements for software safety integrity (see 12.2).

g) The required environment in which the validation activities are to take place (for example, for tests this would include calibrated tools and equipment).

h) The pass/fall 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; and

   – other acceptance criteria, for example, memory usage, timing and value tolerances.

i) The policies and procedures for evaluation the results of the validation, particularly failures.

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

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 safety instrumented system and its associated safety instrumented functions shall be carried out in accordance with the safety instrumented system validation planning. Validation activities shall include, but not be limited to, the following:

- the safety instrumented system performs under normal and abnormal operating modes (for example, start-up, shutdown) as identified in the safety requirement specification;
- confirmation that adverse interaction of the basic process control system and other connected systems do not affect the proper operation of the safety instrumented system;
- the safety instrumented system properly communicates (where required) with the basic process control system or any other system or network;
- sensors, logic solver, and final elements perform in accordance with the safety requirement specification, including all redundant channels;

  NOTE If a factory acceptance test (FAT) was performed on the logic solver as described in Clause 13, credit may be taken for validation of the logic solver by the FAT.

- safety instrumented system documentation is consistent with the installed system;
- confirmation that the safety instrumented function performs as specified on invalid process variable values (for example, out of range);
- the proper shutdown sequence is activated;
- the safety instrumented system provides the proper annunciation and proper operation display;
- computations that are included in the safety instrumented system are correct;
- the safety instrumented system reset functions perform as defined in the safety requirement specification;
- bypass functions operate correctly;
- start-up overrides operate correctly;
- manual shutdown systems operate correctly;
- the proof-test intervals are documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- confirmation that the safety instrumented system performs as required on loss of utilities (for example, electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the safety instrumented system returns to the desired state;
- confirmation that the EMC immunity, as specified in the safety requirements specification (see 10.3), has been achieved.

15.2.5 The software validation shall show that all of the specified software safety requirements (see 12.2) are correctly performed, and the software does not jeopardize the safety requirements under SIS fault conditions and in degraded modes of operation or by executing software 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 SIS validation shall be produced which provides

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

15.2.7 When discrepancies occur between expected and actual results, the analysis made and the decisions taken on whether to continue the validation or to issue a change request and return to an earlier part of the development life cycle, shall be available as part of the results of the safety validation.

15.2.8 After the safety instrumented system validation and prior to the identified hazards being present, the following activities shall be carried out.

- All bypass functions (for example, 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 (for example, fluids) shall be removed.
- All forces shall be removed and if applicable all force enables shall be removed.

16 SIS operation and maintenance

16.1 Objectives

16.1.1 The objectives of the requirements of this clause are:

- to ensure that the required SIL of each safety instrumented function is maintained during operation and maintenance;
- to operate and maintain the SIS so that the designed functional safety is maintained.

16.2 Requirements

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

- routine and abnormal operation activities;
- proof testing, preventive and breakdown maintenance activities;

- the procedures, measures and techniques to be used for operation and maintenance;
- verification of adherence to operations and maintenance procedures;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities.

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

- the routine actions 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;
- the actions and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (for example, when a system needs to be bypassed for testing or maintenance, what additional mitigation steps need to be implemented);
- the information which needs to be maintained on system failure and demand rates on the SIS;
- the information which needs to be maintained showing results of audits and tests on the SIS;
- 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 Considerations include
  - procedures for reporting failures;
  - procedures for analysing systematic failures.
- ensuring that test equipment used during normal maintenance activities is properly calibrated and maintained.

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

16.2.4 Operators shall be trained on the function and operation of the SIS in their area. This training shall ensure the following:

- they understand how the SIS functions (trip points and the resulting action that is taken by the SIS);
- the hazard the SIS is protecting against;
- the operation of all bypass 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 This may include “system reset” and “system restart”.
- expectation on activation of any diagnostic alarms (for example, what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS).

16.2.5 Maintenance personnel shall be trained as required to sustain full functional performance of the SIS (hardware and software) to its targeted integrity.

16.2.6 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 actions taken following a demand on the system;
- the failures of equipment forming part of the SIS established during routine testing or actual demand;
- the cause of the demands;
- the cause of false trips.

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.

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

- functional safety audits;
- tests on the SIS.

16.2.8 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 be used to determine the undetected failures that need to be tested:

– examination of fault trees;

– failure mode and effect analysis;

– reliability centred maintenance.

16.3 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 safety requirement specification**.**

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

16.3.1.3 The frequency of the proof tests shall be as decided using the PFD_{avg} calculation.

NOTE Different parts of the SIS may require different test intervals, for example, the logic solver may 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.

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, hardware degradation, and software reliability.

16.3.1.6 Any change to the application logic requires full proof testing. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were correctly implemented.

16.3.2 Inspection

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

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;

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 (for example, loop number, tag number, equipment number, and SIF number);

e) results of the tests and inspection (for example, “as-found” and “as-left” conditions).

17 SIS modification

17.1 Objectives

17.1.1 The objectives of the requirements of this clause are:

- that modifications to any safety instrumented system are properly planned, reviewed and approved prior to making the change; and
- 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 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 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 safety instrumented system, 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 which may be affected.

17.2.3 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 impact safety then there shall be a return to the first phase of the safety life cycle affected by the modification.

17.2.4 Modification activity shall not begin without proper authorization.

17.2.5 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 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;
- appropriate configuration history;
- tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.

17.2.6 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

18.1.1 The objectives of the requirements of this clause are:

- to ensure that prior to decommissioning any safety instrumented system from active service, a proper review is conducted and required authorization is obtained; and
- to ensure that the required safety instrumented functions remain operational during decommissioning activities.

18.2 Requirements

18.2.1 Prior to carrying out any decommissioning of a safety instrumented system, 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 which 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 hazard and risk assessment sufficient to determine the breadth and depth that subsequent safety life-cycle phases shall need to be re-taken. The assessment shall also consider

- functional safety during the execution of the decommissioning activities; and
- the impact of decommissioning a safety instrumented system 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 the relevant requirements of this standard including re-verification and re-validation.

18.2.5 Decommissioning activities shall not begin without proper authorization.

19 Information and documentation requirements

19.1 Objectives

19.1.1 The objectives of the requirements of this clause are:

- to ensure that the necessary information is available and documented in order that all phases of the safety life cycle can be effectively performed; and
- to ensure that the necessary information is available and documented in order that verification, validation and functional safety assessment 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 this standard shall be available.

19.2.2 The documentation should

- describe the installation, system or equipment and the use of it;
- be accurate;
- be easy to understand;
- suit the purpose for which it is intended; and
- be available in an accessible and maintainable form.

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 requirements of this standard.

19.2.6 The documentation shall have a revision index (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 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 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 hazard and risk assessment and the related assumptions;
b) the equipment used for safety instrumented functions 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) design, implementation, test and validation.

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

Annex A
(informative)

Differences

This annex illustrates the key differences between IEC 61511 and IEC 61508.

IEC 61511 has some differences from IEC 61508. These differences are discussed in Clauses A.1 and A.2 and are based on the comparison of this version of IEC 61511 to IEC 61508.

A.1 Organizational differences

IEC 61508	IEC 61511	Comment
Part 1	Part 1	IEC 61508-1, -2, -3, and -4 have been combined into IEC 61511-1
Part 2	Part 1	Included in IEC 61511-1
Part 3	Part 1	Included in IEC 61511-1
Part 4	Part 1	Included in IEC 61511-1
Part 5	Part 3	Included in IEC 61511-3
Part 6	Part 2	Guidelines for IEC 61511-1
Part 7	All parts	Informative references included in each part as annexes (where required)

A.2 Terminology

IEC 61508-4	IEC 61511-1	Comment
E/E/PE safety related system	SIS	IEC 61508 refers to E/E/PE safety related systems while IEC 61511 refers to safety instrumented systems
PES	SIS	IEC 61508 “PES” includes sensors and final control elements, while IEC 61511 uses the term SIS.
Process control system	Basic process control system	Basic process control system is a global term for the process sector
EUC	Process	IEC 61508 refers to EUC (equipment under control) while IEC 61511 refers to process
Safety function	Safety instrumented function (SIF)	IEC 61508 safety function implemented by E/E/PES, other technology safety related system, or external risk reduction facilities. IEC 61511 SIF is implemented solely by SIS

Bibliography

IEC 60050(191): 1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

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

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

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

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, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations*

IEC 61508-6:2000, *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 61511-3: 2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

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

ISO/IEC 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, *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*

———————

Standards Australia

Standards Australia is an independent company, limited by guarantee, which prepares and publishes most of the voluntary technical and commercial standards used in Australia. These standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth government, Standards Australia is recognized as Australia's peak national standards body. For further information on Standards Australia visit us at

www.standards.org.au

Australian Standards

Australian Standards are prepared by committees of experts from industry, governments, consumers and other relevant sectors. The requirements or recommendations contained in published Standards are a consensus of the views of representative interests and also take account of comments received from other sources. They reflect the latest scientific and industry experience. Australian Standards are kept under continuous review after publication and are updated regularly to take account of changing technology.

International Involvement

Standards Australia is responsible for ensuring that the Australian viewpoint is considered in the formulation of international Standards and that the latest international experience is incorporated in national Standards. This role is vital in assisting local industry to compete in international markets. Standards Australia represents Australia at both ISO (The International Organization for Standardization) and the International Electrotechnical Commission (IEC).

Electronic Standards

All Australian Standards are available in electronic editions, either downloaded individually from our web site, or via On-Line and DVD subscription services. For more information phone 1300 65 46 46 or visit Standards Web Shop at

www.standards.com.au

GPO Box 5420 Sydney NSW 2001
Administration Phone (02) 8206 6000 Fax (02) 8206 6001 Email mail@standards.com.au
Customer Service Phone 1300 65 46 46 Fax 1300 65 49 49 Email sales@standards.com.au
Internet www.standards.org.au

ISBN 0 7337 5913 0

Printed in Australia