IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable controllers – Part 6: Functional safety

Automates programmables – Partie 6: Sécurité fonctionnelle

IEC 61131-6:2012

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

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

A propos de la CEI

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

A propos des publications CEI

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

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

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

IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable controllers – Part 6: Functional safety

Automates programmables – Partie 6: Sécurité fonctionnelle

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XD
CODE PRIX

ICS 25.040.40; 35.240.50

ISBN 978-2-83220-402-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PROGRAMMABLE CONTROLLERS –

Part 6: Functional safety

FOREWORD

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

International Standard IEC 61131-6 has been prepared by subcommittee 65B: Measurement and control devices, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

FDIS	Report on voting
65B/831/FDIS	65B/850/RVD

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

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

A list of all parts of the IEC 61131 series can be found, under the general title *Programmable controllers*, on the IEC website.

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

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

INTRODUCTION

General

IEC 61131 series consists of the following parts under the general title *Programmable controllers*:

Part 1: General information
Part 2: Equipment requirements and tests
Part 3: Programming languages
Part 4: User guidelines
Part 5: Communications
Part 6: Functional safety
Part 7: Fuzzy control programming
Part 8: Guidelines for the application and implementation of programming languages

This Part of IEC 61131 series constitutes Part 6 of a series of standards on programmable controllers and the associated peripherals and should be read in conjunction with the other parts of the series.

As this document is the FS-PLC product standard, the provisions of this part should be considered to govern in the area of programmable controllers and their associated peripherals.

Compliance with Part 6 of IEC 61131 cannot be claimed unless the requirements of Clause 4 of this part are met.

Terms of general use are defined in Part 1 of IEC 61131. More specific terms are defined in each part.

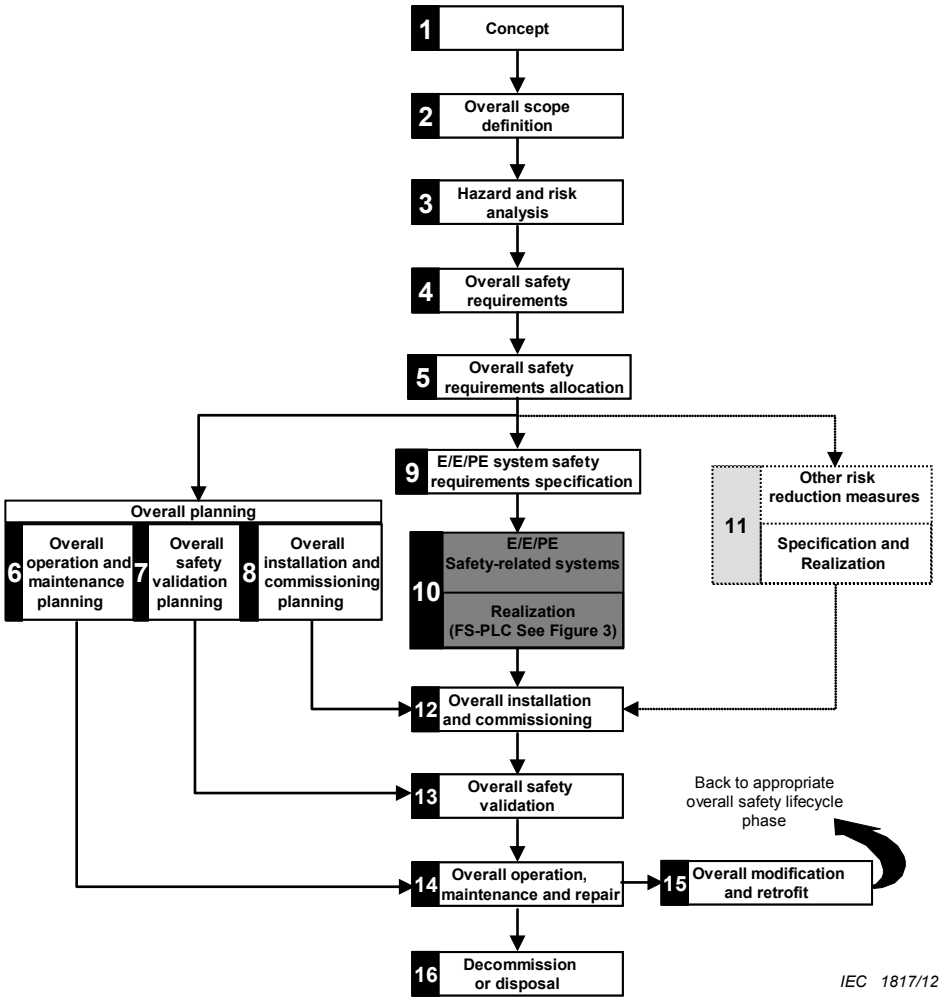
In keeping with 1.1 of IEC 61508-1:2010, this part encompasses the product specific requirements of IEC 61508-1, 61508-2 and 61508-3 as pertaining to programmable controllers and their associated peripherals.

This document's intent is to follow the IEC 61508 series structure, in principle. But some aspects do not have a direct correlation and thus need to be addressed somewhat differently. In part, this is due to addressing hardware, software, firmware, etc. in a single document.

Framework of this part

IEC 61508-1:2010, Figure 2 is included here, and is designated Figure 1. It has been adjusted to show how an FS-PLC fits into the overall E/E/PE safety-related system safety lifecycle. Though Figure 1 box 10 includes sensors, logic subsystem and final elements (e.g. actuators), from the viewpoint of IEC 61508-1, the FS-PLC is given emphasis here by including a reference to Figure 3.

As such, the Realization Phase, Figure 1, box 10, embodies only the logic subsystem, from this part's perspective.



NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.

NOTE 2 The phases represented by box 11 is outside the scope of this standard.

NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 10 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

NOTE 4 See IEC 61508-1, Table 1 for a description of the objectives and scope of the phases represented by each box.

NOTE 5 The technical requirements necessary for the overall operation, maintenance, repair Modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E? PE safety-related system and its elements and components.

Figure 1 – FS-PLC in the overall E/E/PE safety-related system safety lifecycle phases

The areas included in this part are FS-PLC safety lifecycle management, functional safety requirements allocation, and development planning; with the major emphasis on the Realization Phase (Box 10) of the overall safety lifecycle, shown in Figure 1. The assumption of this part is that the FS-PLC is utilized as a logic subsystem for the overall E/E/PE system.

The Figure 1, Realization (box 10), includes:

- the allocation of the FS-PLC safety aspects to FS-PLC hardware, software or firmware, or any combination,
- FS-PLC hardware architectures,
- verification and validation activities at the FS-PLC level,
- FS-PLC modification requirements,
- operation and maintenance information for the FS-PLC user,
- information to be provided by the FS-PLC manufacturer for the user.

PROGRAMMABLE CONTROLLERS –

Part 6: Functional safety

1 Scope

This Part of the IEC 61131 series specifies requirements for programmable controllers (PLCs) and their associated peripherals, as defined in Part 1, which are intended to be used as the logic subsystem of an electrical/electronic/programmable electronic (E/E/PE) safety-related system. A programmable controller and its associated peripherals complying with the requirements of this part is considered suitable for use in an E/E/PE safety-related system and is identified as a functional safety programmable logic controller (FS-PLC). An FS-PLC is generally a hardware (HW) / software (SW) subsystem. An FS-PLC may also include software elements, for example predefined function blocks.

An E/E/PE safety-related system generally consists of sensors, actuators, software and a logic subsystem. This part is a product specific implementation of the requirements of the IEC 61508 series and conformity to this part fulfils all of the applicable requirements of the IEC 61508 series related to FS-PLCs. While the IEC 61508 series is a system standard, this part provides product specific requirements for the application of the principles of the IEC 61508 series to FS-PLC.

This Part of the IEC 61131 series addresses only the functional safety and safety integrity requirements of an FS-PLC when used as part of an E/E/PE safety-related system. The definition of the functional safety requirements of the overall E/E/PE safety-related system and the functional safety requirements of the ultimate application of the E/E/PE safety-related system are outside the scope of this part, but they are inputs for this part. For application specific information the reader is referred to standards such as the IEC 61511 series, IEC 62061, and the ISO 13849 series.

This part does not cover general safety requirements for an FS-PLC such as requirements related to electric shock and fire hazards specified in IEC 61131-2.

This part applies to an FS-PLC with a Safety Integrity Level (SIL) capability not greater than SIL 3.

The objective of this part is:

- to establish and describe the safety life-cycle elements of an FS-PLC, in harmony with the general safety life-cycle identified in IEC 61508-1, -2 and -3;
- to establish and describe the requirements for FS-PLC HW and SW that relate to the functional safety and safety integrity requirements of a E/E/PE safety-related system;
- to establish evaluation methods for a FS-PLC to this part for the following parameters/criteria:
  - a Safety Integrity Level (SIL) claim for which the FS-PLC is capable,
  - a Probability of Failure on Demand (PFD) value,
  - an average frequency of dangerous failure per hour value (PFH),
  - a value for the safe failure fraction (SFF),
  - a value for the hardware fault tolerance (HFT),
  - a diagnostic coverage (DC) value,
  - a verification that the specified FS-PLC manufacturer’s safety lifecycle processes are in place,

  - the defined safe state,
  - the measures and techniques for the prevention and control of systematic faults, and
  - for each failure mode addressed in this part, the functional behaviour in the failed state;
- to establish the definitions and identify the principal characteristics relevant to the selection and application of FS-PLCs and their associated peripherals.

This part is primarily intended for FS-PLC manufacturers. It also includes the critical role of FS-PLC users through the user documentation requirements. Some user guidelines for FS-PLCs may be found in IEC 61131-4.

The requirements of ISO/IEC Guide 51 and IEC Guide 104, as they relate to this part, are incorporated herein.

2 Normative references

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

IEC 60947-5-1:2003, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

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

IEC 61000-4-2:2008, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3:2006, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-4:2012, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5:2005, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6:2008, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-8:2009, *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test*

IEC 61131-1:2003, *Programmable controllers – Part 1: General information*

IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-4:2004, *Programmable controllers – Part 4: User guidelines*

IEC 61326-3-1:2008, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for*

equipment intended to perform safety-related functions (functional safety) – General industrial applications

IEC 61326-3-2:2008, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment*

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

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

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

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

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

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

IEC Guide 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications*

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

EN 50205:2002, *Relays with forcibly guided (mechanically linked) contacts*

3 Terms and definitions

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

3.1
application program
application software
part of the software of a programmable electronic system that specifies the functions that perform a task related to the EUC rather than the functioning of, and services provided by the programmable device itself

[SOURCE: IEC 61508-4:2010, 3.2.7]

3.2
application specific integrated circuit
ASIC
integrated circuit designed and manufactured for specific function, where its functionality is defined by the product developer

[SOURCE: IEC 61508-4:2010, 3.2.15]

3.3
architecture
specific configuration of hardware and software elements in a system

[SOURCE: IEC 61508-4:2010, 3.3.4]

3.4
availability
the probability that an item is able to perform its intended function, expressed as a decimal value between zero and one

EXAMPLE A = 0,9 means that a product is available 90 % of the time.

Note 1 to entry: For $\lambda T << 1$, $A = 1 - \lambda T$, See 3.23.

3.5
average frequency of a dangerous failure per hour
PFH
average frequency of a dangerous failure of an E/E/PE safety-related system to perform the specified safety function over a given period of time

Note 1 to entry: The term “probability of dangerous failure per hour” is not used in this standard but the acronym PFH has been retained but when it is used it means “average frequency of dangerous failure [h]”.

Note 2 to entry: From a theoretical point of view, the PFH is the average of the unconditional failure intensity, also called failure frequency, and which is generally designated *w(t)*. It should not be confused with a failure rate (see Annex B of IEC 61508-6:2010).

Note 3 to entry: When the E/E/PE safety-related system is the ultimate safety layer, the PFH should be calculated from its unreliability $F(T)=1-R(t)$ (see failure rate above). When it is not the ultimate safety-related system its PFH should be calculated from its unavailability $U(t)$ (see PFD, 3.38). PFH approximations are given by $F(T)/T$ and 1/MTTF in the first case and 1/MTBF in the second case.

Note 4 to entry: When the E/E/PE safety-related system implies only quickly repaired revealed failures then an asymptotic failure rate λ_{as} is quickly reached. It provides an estimate of the PFH.

[SOURCE: IEC 61508-4:2010, 3.6.19]

3.6
black channel
parts of a communication channel which are not designed or validated according to the IEC 61508 series

Note 1 to entry: See: 7.4.11.2 of IEC 61508-2:2010.

3.7
channel
element or group of elements that separately implement an element safety function

EXAMPLE A two-channel (or dual-channel) configuration is one with two channels that independently perform the same function.

Note 1 to entry: The term can be used to describe a complete system, or a portion of a system (for example, sensors or final elements).

[SOURCE: IEC 61508-4:2010, 3.3.6]

3.8
common cause failure
CCF
failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure

[SOURCE: IEC 61508-4:2010, 3.6.10]

3.9
cyber security
protection of data in computer and information systems from loss or corruption due to intentional or unintentional activities by unauthorized or malicious individuals

Note 1 to entry: This term concerns the defence against such activities via network or other communication interfaces.

3.10
dangerous failure
FS-PLC
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,

b) decreases the probability that the safety function operates correctly when required

[SOURCE: IEC 61508-4:2010, 3.6.7]

3.11
dangerous fault
fault that can lead to dangerous failure

Note 1 to entry: If a dangerous fault is detected, action is taken to avoid a dangerous failure.

3.12
defined safe state
the state of the FS-PLC, as defined by the FS-PLC manufacturer, when a dangerous failure occurs

Note 1 to entry: Typically, the defined safe state is the default state of each and every FS-PLC output. For digital outputs, this state is considered de-energized unless specifically defined otherwise. For analogue outputs, this state is zero volts or zero amps, unless specifically defined otherwise. For communications ports, this state is defined as no communications, unless specifically defined otherwise.

3.13
detected failure
termination of the ability of a functional unit to perform a required function detected by the diagnostic tests, proof tests, operator intervention or through normal operation

EXAMPLE Physical inspection and manual tests.

3.14
diagnostic coverage
DC

fraction of dangerous failures, detected by automatic on-line diagnostic tests, computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures

Note 1 to entry: The dangerous failure diagnostic coverage is computed using the following equation, where DC is the diagnostic coverage, λ_{DD} is the detected dangerous failure rate and λ_{Dtotal} is the total dangerous failure rate:

$$DC = \Sigma\lambda_{DD} / \Sigma\lambda_{Dtotal}$$

Note 2 to entry: This definition is applicable providing the individual components have constant failure rates.

[SOURCE: IEC 61508-4:2010, 3.8.6]

3.15
E/E/PE
electrical/electronic/programmable electronic

3.16
element
part of a subsystem comprising a single component or any group of components that performs one or more element safety functions

[SOURCE: IEC 62061:2005, 3.2.6, modified]

Note 1 to entry: An element may comprise hardware and/or software.

[SOURCE: IEC 61508-4:2010, 3.4.5, modified]

3.17
element safety function
that part of a safety function which is implemented by an element

[SOURCE: IEC 61508-4:2010, 3.5.3, modified]

3.18
embedded SW
embedded software
embedded firmware
FW
software controlling the operation of the FS-PLC or one of its subsystems

Note 1 to entry: The embedded software is supplied by the FS-PLC manufacturer installed in the FS-PLC. The user has no direct access to embedded software. The FS-PLC manufacturer develops or writes embedded software to control his FS-PLC. This may, for example, control the communication subsystem or the interpretation of the program developed by the user in the engineering tools.

Note 2 to entry: Another term for embedded software.

Note 3 to entry: Firmware can be either safety related or non-safety related.

3.19
engineering tools
software for developing the application program

EXAMPLE: The engineering tools software is supplied by the FS-PLC manufacturer to be installed on a personal computer workstation. Within this SW package the user develops or writes his application program to control his process. This application program is then downloaded into the FS-PLC, where it determines control of the user's FS-PLC, attached equipment and thus process.

Note 1 to entry: Application programs and software can be either safety related or non-safety related.

3.20
equipment under control
EUC
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

Note 1 to entry: The EUC control system is separate and distinct from the EUC.

[SOURCE: IEC 61508-4:2010, 3.2.1]

3.21
equipment under test
EUT
representative configuration(s), as defined by the manufacturer, used for type tests

3.22
failure
termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required

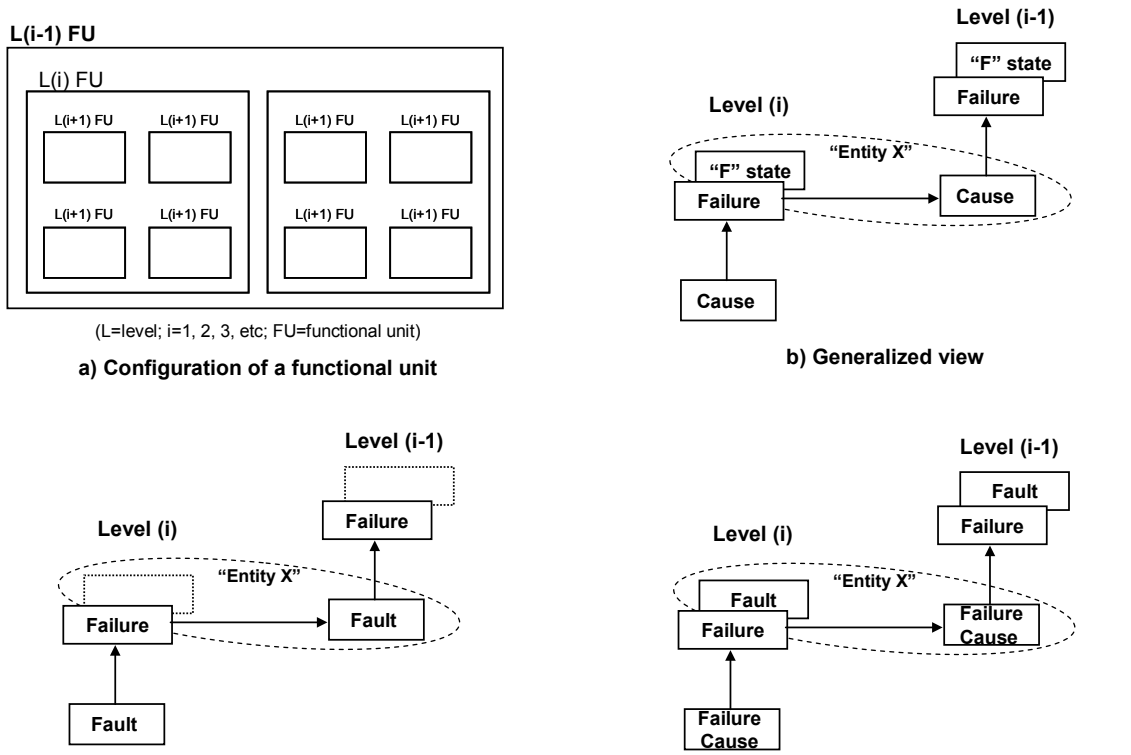
Note 1 to entry: This is based on IEC 60050-191:1990, 191-04-01 with changes to include systematic failures due to, for example, deficiencies in specification or software.

SEE: Figure 2 for the relationship between faults and failures.

Note 2 to entry: Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

Note 3 to entry: Failures are either random (in hardware) or systematic (in hardware or software), see 3.42 and 3.56.

[SOURCE: IEC 61508-4:2010, 3.6.4]



NOTE 1 As shown in a), a functional unit is able to be viewed as a hierarchical composition of multiple levels, each of which might in turn be called a functional unit. In level (i), a "cause" might manifest itself as an error (a deviation from the correct value or state) within this level (i) functional unit, and, if not corrected or circumvented, might cause a failure of this functional unit, as a result of which it falls into an "F" state where it is no longer able to perform a required function (see b)). This "F" state of the level (i) functional unit might in turn manifest itself as an error in the level (i-1) functional unit and, if not corrected or circumvented, might cause a failure of this level (i-1) functional unit.

NOTE 2 In this cause and effect chain, the same thing ("Entity X") is able to be viewed as a state ("F" state) of the level (i) functional unit into which it has fallen as a result of its failure, and also as the cause of the failure of the level (i-1) functional unit. This "Entity X" combines the concept of "fault" in IEC 61508 series and ISO/IEC 2382-14, which emphasizes its cause aspect as illustrated in c), and that of "fault" in IEC 60050-191, which emphasizes its state aspect as illustrated in d). The "F" state is called fault in IEC 60050-191, whereas it is not defined in IEC 61508 series and ISO/IEC 2382-14.

NOTE 3 In some cases, a failure or an error might be caused by an external event such as lightning or electrostatic noise, rather than by an internal fault. Likewise, a fault (in both vocabularies) may exist without a prior failure. An example of such a fault is a design fault.

Figure 2 – Failure model

3.23
failure rate
reliability parameter (λ(*t*)) of an entity (single components or systems) such that *λ(t).dt* is the probability of failure of this entity within [*t, t+dt*] provided that it has not failed during [0, *t*]

Note 1 to entry: Mathematically, λ(*t*) is the conditional probability of failure per unit of time over [*t, t+dt*]. It is in strong relationship with the reliability function (i.e. probability of no failure from 0 to *t*) by the general formula $R(t) = \exp(-\int_0^t \lambda(\tau)d\tau$. Reversely it is defined from the reliability function by $\lambda(t) = -\frac{dr(t)}{dt}\frac{1}{r(t)}$.

Note 2 to entry: Failure rates and their uncertainties can be estimated from field feedback by using conventional statistics. During the "useful life" (i.e. after burn-in and before wear-out), the failure rate of a simple items is more or less constant, $\lambda(t) \equiv \lambda$.

Note 3 to entry: The average of λ(*t*) over a given period [0, *T*], $\lambda_{avg}(T) = (\int_0^T \lambda(\tau)d\tau)/T$, is not a failure rate because it cannot be used for calculating *R*(*t*) as shown in Note 1 to entry. Anyway it may be interpreted as the average frequency of failure over this period (i.e. the PFH, see Annex B of IEC 61508-6:2010).

Note 4 to entry: The failure rate of a series of items is the sum of the failure rates of each items.

Note 5 to entry: The failure rate of redundant systems is generally non constant. Nevertheless when all failures are quickly revealed, independent and quickly repaired λ(*t*) converges quickly to an asymptotic value λ_{as} which is the equivalent failure rate of the systems. It should not be confused with the average failure rate described in Note 3 to entry which doesn't necessarily converge to an asymptotic value.

[SOURCE: IEC 61508-4:2010, 3.6.16]

3.24
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

[SOURCE: ISO/IEC 2382-14:1997, 14.01.10]

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines “fault” as a state characterised by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources. See Figure 2 for an illustration of these two points of view.

[SOURCE:IEC 61508-4:2010, 3.6.1]

3.25
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

[SOURCE: ISO/IEC 2382-14:1997, 14.04.06]

Note 1 to entry: The definition in IEC 60050-191:1990, 191-15-05 refers only to sub-item faults. See the Note 1 to entry in 3.24.

[SOURCE: IEC 61508-4:2010, 3.6.3]

Note 2 to entry: Faults and errors to be considered include those involving interfaces to the FS-PLC.

3.26
FS-PLC functional safety requirements specification
specification containing the safety function requirements and associated safety integrity levels for the FS-PLC

3.27
functional safety
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12]

Note 1 to entry: Functional safety is, in essence, the ability of a safety-related system to achieve or maintain a safe state.

3.28
HW
hardware
FS-PLC electrical, mechanical or other physical devices which are connected together to perform functions

3.29
high complexity safety-related subsystem
part of a E/E/PE safety-related system for which:

the failure mode of at least one component is not well defined, or

the behaviour of the subsystem under fault conditions cannot be completely determined, or

there is insufficient field failure data to show that the claimed failure rates are met

EXAMPLE A FS-PLC. This is derived from type B subsystem as described in IEC 61508-2:2010, 7.4.4.1.3.

Note 1 to entry: Refer to Type A (9.4.3.2.2) and Type B (9.4.3.2.3) systems.

3.30
logic subsystem
a logic subsystem is defined as that portion of a E/E/PE safety-related system that performs the function logic but excludes sensors and final elements

EXAMPLE An FS-PLC is a logic subsystem.

3.31
mean repair time
MRT
expected overall repair time

Note 1 to entry: MRT encompasses the times (b), (c) and (d) of the times for MTTR (see 3.34).

[SOURCE: IEC 61508-4:2010, 3.6.22]

3.32
mean time between failures
MTBF
a statistically based parameter (usually expressed in hours) that allows comparisons to be made between the reliability of different products

Note 1 to entry: Mathematically, it is the reciprocal of a repairable product's failure rate.

Note 2 to entry: MTBF is an arithmetic mean determined from a large number of units over a long period of time.

Note 3 to entry: For a complex product like a PLC, the average failure rate approximates a constant failure rate with an exponential Reliability function: $R(t) = e^{-\lambda t}$

Note 4 to entry: MTBF = MTTF + MTTR.

SEE: NOTE 2 to entry of 3.33.

3.33
mean time to failure
MTTF
a statistically based parameter (usually expressed in hours) that allows comparisons between the reliability of different non-repairable products

Note 1 to entry: For a non-repairable product with a constant failure rate, MTTF is the reciprocal of the product's failure rate.

Note 2 to entry: MTTF is an arithmetic mean determined from a large number of units over a long period of time.

Note 3 to entry: Although the two terms MTBF and MTTF are sometimes used interchangeably, they are properly used to refer to repairable and non-repairable products respectively. MTBF should be used only for products that are normally repaired and returned to service.

3.34
mean time to restoration
MTTR

expected time to achieve restoration

Note 1 to entry: MTTR encompasses:

the time to detect the failure (a); and,

the time spent before starting the repair (b); and,

the effective time to repair (c); and,

the time before the component is put back into operation (d).

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

[SOURCE: IEC 61508-4:2010, 3.6.21]

3.35
mode of operation
way in which a safety function operates, which may be either low demand, high demand or continuous mode

Note 1 to entry: The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state (see 7.4.6 of IEC 61508-2:2010).

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.1
low demand mode
where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.2
high demand mode
where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.3
continuous mode
where the safety function retains the EUC in a safe state as part of normal operation

[SOURCE: IEC 61508-4:2010, 3.5.14]

3.36
MooN
M out of N
architecture made up of “N” independent channels, which are so connected, that at least “M” channels are required to perform the safety function

3.37
process safety time
worst case
period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring

[SOURCE: IEC 61508-4:2010, 3.6.20]

3.38
probability of dangerous failure on demand
PFD
safety unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system

Note 1 to entry: The [instantaneous] unavailability (as per IEC 60050-191) is the probability that an item is not in state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided. It is generally noted by U (*t*).

Note 2 to entry: The [instantaneous] availability does not depend on the states (running or failed) experienced by the item before t. It characterizes an item which only has to be able to work when it is required to do so, for example, an E/E/EP safety-related system working in low demand mode.

Note 3 to entry: If periodically tested, the PFD of an E/E/PE safety-related system is, in respect of the specified safety function, represented by a saw tooth curve with a large range of probabilities ranging from low, just after a test, to a maximum just before a test.

[SOURCE: IEC 61508-4:2010, 3.6.17]

3.39
programmable HW
HW that can be altered or modified, either in functionality or performance, by embedded software

EXAMPLES FPGA, flash memory devices, and microprocessor based products.

3.40
proof test
periodical test
periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition

Note 1 to entry: The effectiveness of the proof test will be dependent both on failure coverage and repair effectiveness. In practice detecting 100 % of the hidden dangerous failures is not easily achieved for other than low-complexity E/E/PE safety-related systems. This should be the target. As a minimum, all the safety functions which are executed are checked according to the E/E/PE safety-related systems functional safety requirements specification. If separate channels are used, these tests are done for each channel separately. For complex elements an analysis may need to be performed in order to demonstrate that the probability of hidden dangerous failure not detected by proof tests is negligible over the whole life duration of the E/E/EP safety-related system.

Note 2 to entry: A proof test needs some time to be achieved. During this time the E/E/EP safety-related system may be inhibited partially or completely. The proof test duration can be neglected only if the part of the E/E/EP safety-related system under test remains available in case of a demand for operation or if the EUC is shut down during the test.

Note 3 to entry: During a proof test, the E/E/EP safety-related system may be partly or completely unavailable to respond to a demand for operation. The Mean Time To Repair (MTTR) can be neglected for SIL calculations only if the EUC is shut down during repair or if other risk measures are put in place with equivalent effectiveness.

[SOURCE: IEC 61508-4:2010, 3.8.5]

3.41
proper function verification procedure
PFVP
methodology to test an FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

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

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or,

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

[SOURCE: IEC 61508-4:2010, 3.6.8]

3.46
safe fault
fault that cannot lead to dangerous failure

3.47
safe failure fraction
SFF
property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.

Note 1 to entry: This ratio is represented by the following equation:

$SFF = (\Sigma\lambda_{Savg} + \Sigma\lambda_{Ddavg})/(\Sigma\lambda_{Savg} + \Sigma\lambda_{Ddavg} + \Sigma\lambda_{Duavg})$

when the failure rates are based on constant failure rates the equation can be simplified to:

$SFF = (\Sigma\lambda_{S} + \Sigma\lambda_{Dd})/(\Sigma\lambda_{S} + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$

[SOURCE: IEC 61508-4:2010, 3.6.15]

3.48
safe state
state of the EUC when safety is achieved

Note 1 to entry: In going from a potentially hazardous condition to the final safe state, the EUC may have to go through a number of intermediate safe states. For some situations a safe state exists only so long as the EUC is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

[SOURCE: IEC 61508-4:2010, 3.1.13]

3.49
safety function response time
worst case elapsed time following actuation of a safety sensor, before the corresponding safe state of the safety actuator(s) is achieved in the presence of errors or failures in the safety function channel.

[SOURCE: IEC 61784-3:2010, 3.1.1.36, modified]

3.50
safety integrity
probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

Note 1 to entry: The higher the level of safety integrity, the lower the probability that the safety-related system will fail to carry out the specified safety functions or will fail to adopt a specified state when required.

Note 2 to entry: There are four levels of safety integrity (see IEC 61508-4:2010, 3.5.8).

Note 3 to entry: In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) that 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 average frequency of failure in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, safety integrity also depends on many factors that cannot be accurately quantified but can only be considered qualitatively.

Note 4 to entry: Safety integrity comprises hardware safety integrity (see IEC 61508-4:2010, 3.5.7) and systematic safety integrity (see IEC 61508-4:2010, 3.5.6).

Note 5 to entry: This definition focuses on the reliability of the safety-related systems to perform the safety functions (see IEC 60050-191:1990, 191-12-01 for a definition of reliability).

[SOURCE: IEC 61508-4:2010, 3.5.4]

3.51
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

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

Note 4 to entry: This specification scheme is only applicable to the safety-related system.

Note 5 to entry: The target failure measures for the four safety integrity levels are specified in Table 1 and Table 2 of this part.

3.52
SIL capability
maximum SIL for a FS-PLC which can be achieved in relation to architectural constraints and systematic safety integrity

[SOURCE: adapted from IEC 62061:2005, 3.2.24]

3.53
safety-related system
designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and
- is intended to achieve, on its own or with other E/E/PE safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions

Note 1 to entry: The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the other risk reduction measures (see IEC 61508-4:2010, 3.4.2), the necessary risk reduction in order to meet the required tolerable risk (see IEC 61508-4:2010, 3.1.7). See also Annex A of IEC 61508-5:2010.

Note 2 to entry: Safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on receipt of commands. The failure of a safety-related system would be included in the events leading to the determined hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems and safety-related protection systems.

Note 3 to entry: Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and independent systems dedicated to safety.

Note 4 to entry: A safety-related system may

a) be designed to prevent the harmful event (i.e. if the safety-related systems perform their safety functions then no harmful event arises);

b) be designed to mitigate the effects of the harmful event, thereby reducing the risk by reducing the consequences;

c) be designed to achieve a combination of a) and b).

Note 5 to entry: A person can be part of a safety-related system (see IEC 61508-4:2010, 3.4.1). For example, a person could receive information from a programmable electronic device and perform a safety action based on this information, or perform a safety action through a programmable electronic device.

Note 6 to entry: A safety-related system includes all the hardware, software and supporting services (for example, power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system).

Note 7 to entry: A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic.

[SOURCE: IEC 61508-4:2010, 3.4.1]

3.54
software
SW
intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

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

Note 2 to entry: This definition without Note to entry 1 differs from ISO/IEC 2382-1 (see bibliography), and the full definition differs from ISO 9000-3, by the addition of the word data.

[SOURCE: IEC 61508-4:2010, 3.2.5]

3.55
subsystem
a part of a FS-PLC comprising a single component or an array of components that performs one or more functions

Note 1 to entry: In this part, the term subsystem is used differently that as defined in IEC 61508-4.

3.56
systematic failure
failure, related in a deterministic way to a certain cause, that can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

[SOURCE: IEC 60050-191:1990, 191-04-19]

Note 1 to entry: Corrective maintenance, without modification, will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

EXMPLES Examples of causes of systematic failures include human error in

- the functional safety requirements specification;
- the design, manufacture, installation, operation of the hardware;
- the design, implementation, etc. of the software.

Note 3 to entry: In this standard, failures in a safety-related system are categorized as random hardware failures or systematic failures.

[SOURCE: IEC 61508-4:2010, 3.6.6]

3.57
useful lifetime
worst case
minimum elapsed time between the installation of the FS-PLC and the point in time when component failure rates of the FS-PLC can no longer be predicted, with any accuracy

EXAMPLE For example, the point in time when the initial beta-factor calculations as defined in IEC 61508-6:2010 Annex D are no longer valid.

3.58
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: Adapted from ISO 8402 by excluding the notes.

Note 2 to entry: In this standard there are three validation phases:

overall safety validation (see IEC 61508-1:2010, Figure 2),

E/E/PE safety-related system validation (see IEC 61508-1:2010, Figure 3),

software validation (see IEC 61508-1:2010, Figure 4).

Note 3 to entry: Validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the functional safety requirements specification for that safety-related system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software functional safety requirements specification.

[SOURCE: IEC 61508-4:2010, 3.8.2]

3.59
verification
confirmation by examination and provision of objective evidence that the requirements have been fulfilled

Note 1 to entry: Adapted from ISO 8402 by excluding the notes.

Note 2 to entry: In the context of this standard, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall, FS-PLC), by analysis, mathematical reasoning and/or tests, that, for the specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

EXAMPLE Verification activities include

- reviews on outputs (documents from all phases of the safety lifecycle) 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.

[SOURCE: IEC 61508-4:2010, 3.8.1]

Note 3 to entry: In this standard the verification phase includes all activities which are related to the FS-PLC development and the proof that the developed FS-PLC fulfils its specification.

4 Conformance to this standard

This part encompasses the product specific requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-3. While IEC 61508 series is a system standard, this part provides product specific requirements with more precise information for the application of the principles of IEC 61508 series to an FS-PLC.

Conformance to this standard is only applicable when a programmable controller and its associated peripherals, as defined in IEC 61131-1, are intended to be used as the logic subsystem of an E/E/PE safety-related system and is identified as a functional safety PLC (FS-PLC). This FS-PLC may also include software elements, for example as predefined function blocks.

To conform to this standard it shall be demonstrated that the FS requirements of each clause and subclause of this part has been satisfied.

An FS-PLC must first meet the applicable requirements of Part 2 before being considered compliant with this part. There is no equivalent requirement for compliance with Part 3.

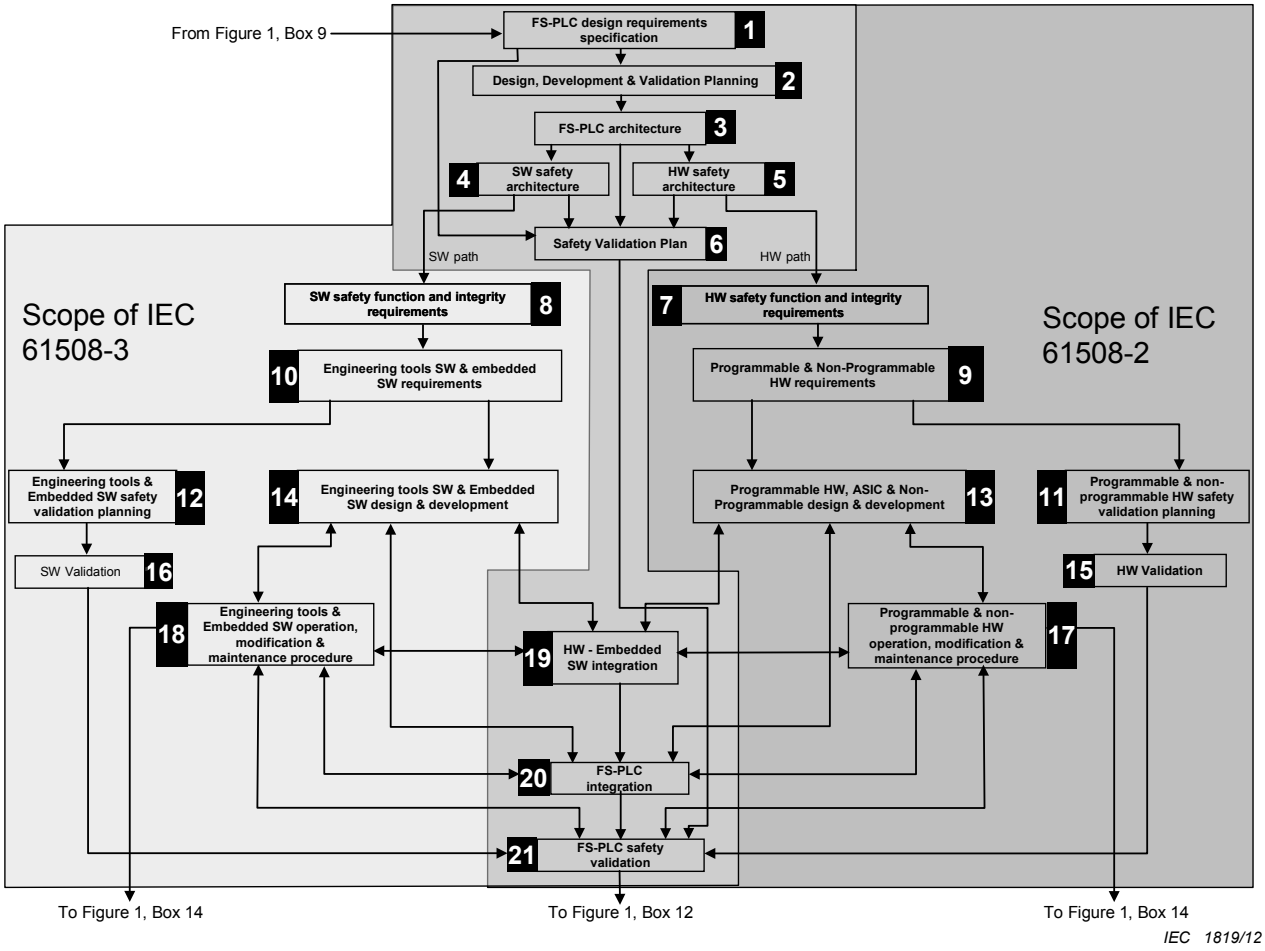
Conformance to these clauses and subclauses is the responsibility of the manufacturer of the FS-PLC.

5 FS-PLC safety lifecycle

5.1 General

In order to deal in a systematic manner with all the activities necessary to achieve the required FS-PLC logic function(s) and SIL capability for the FS-PLC, 5.1 adopts an FS-PLC safety lifecycle, see Figure 3, as a technical framework.

Figure 3 is based on Figure 2, 3 and 4 from IEC 61508-1:2010, Figure 2 and 4 from IEC 61508-2:2010 and Figure 2, 3, 4 and 5 from IEC 61508-3:2010.



NOTE 1 The “From Figure 1 or To Figure 1 box 9, 12 or 14” references are to Figure 1 of this part.

NOTE 2 This figure describes the typical tasks associated with the development of an FS-PLC. It does not represent a fixed step-by-step procedure in the development of an FS-PLC.

Figure 3 – FS-PLC safety lifecycle (in realization phase)

For all the phases of the FS-PLC safety lifecycle, shown in Figure 3, Clauses 5 to 16 define the requirements for the FS-PLC, as derived from IEC 61508-2 and IEC 61508-3. Figure 3 deviates from the IEC 61508-1, IEC 61508-2 and IEC 61508-3 source figures not in substance but to make some clarifications and distinctions.

The requirements of Clauses 5 to 16 encompass all the FS-PLC safety requirement specifications: HW (incl. ASIC, FPGA etc.) and SW. Figure 3 shows the flow as FS-PLC architectural decisions are made and requirements are then divided between FS-PLC HW safety requirement specifications and FS-PLC SW safety requirement specifications.

On the FS-PLC SW side, two types of SW tasks are shown (engineering tools and embedded SW). While these are considered SW, there are some distinct differences in their impact and relationships to the HW development side, toolsets, methods, etc.

On the FS-PLC HW side, three types of HW tasks are shown (programmable HW, ASIC and non-programmable HW). While these are considered HW, there are some distinct differences in their impact and relationships to the SW development side, toolsets, methods, etc.

Boxes 17, 18, 19 and 20 of Figure 3 depict a progressive integration of the SW and HW parts of the FS-PLC.

The first level of integration takes place between the programmable HW and the embedded SW targeted to the HW. This is shown clearly in the source IEC 61508 figures.

The second level of integration takes place when all parts of the FS-PLC are available; programmable HW and its embedded SW, non-programmable HW and engineering tools. While implied in the source IEC 61508 figures, it is clarified in Figure 3.

Only after this second level of integration can the FS-PLC safety validation be completed.

5.2 FS-PLC functional safety SIL capability requirements

5.2.1 General

Prior to entering the realization phase, the functional safety and safety integrity requirements, defining the FS-PLC logic functions and their SIL capability, shall be stated. Then, there needs to be an allocation of the functional safety and SIL capability requirements to either hardware, software or both. This leads to detailed requirements for hardware and software as specified in Clauses 9 and 10, respectively.

The hardware and software lifecycle phases applied in this part are:

- FS-PLC design requirements specification [box 1 of Figure 3; Clause 6]
- Design, development and validation plan [box 2 of Figure 3; Clause 7]
- FS-PLC architecture [box 3 of Figure 3; Clause 8]
- SW safety architecture [box 4 of Figure 3]
- HW safety architecture [box 5 of Figure 3]
- Safety validation plan [box 6 of Figure 3; Clause 11]
- HW safety function and safety integrity requirements [box 7 of Figure 3]
- SW safety function and safety integrity requirements [box 8 of Figure 3]
- Programmable & non-Programmable HW requirements [box 9 of Figure 3]
- Engineering tools and embedded SW requirements [box 10 of Figure 3; Subclause 10.3]
- Programmable & non-programmable HW safety validation planning [box 11 of Figure 3]
- Engineering tools & embedded SW safety validation planning [box 12 of Figure 3; Subclause 10.4]
- Programmable & Non-Programmable HW design & development [box 13 of Figure 3]
- Engineering tools & Embedded SW design & development [box 14 of Figure 3; Clause 10]
- HW Validation [box 15 of Figure 3; Subclause 9.7]
- SW Validation [box 16 of Figure 3]
- Programmable & non-programmable HW operation & modification procedure [box 17 of Figure 3; Clause 15]
- Engineering tools & embedded SW operation & modification procedure [box 18 of Figure 3]
- HW - Embedded SW integration [box 19 of Figure 3; Subclause 9.5]
- FS-PLC integration [box 20 of Figure 3]
- FS-PLC safety validation [box 21 of Figure 3; Clause 11]

5.2.2 Data security

5.2.2.1 General

Security threat and hazard analysis are normally necessary for safety-related applications to protect against intentional attacks or unintentional changes. Security can be achieved by establishing appropriate security policies and measures such as physical (for example mechanical, electronic) or organizational measures.

Where safety related communications are part of the FS-PLC there is the possibility of inadvertent changes to the parameters of network devices. Safety related communication devices shall have protections against inadvertent changes.

Where applicable, the requirements for overall security defined in IEC 62443 shall be followed.

5.2.2.2 Security assumptions for ensuring functional safety and SIL capability

The basic security policy for the security environment(s) of the FS-PLC, according to the complexity of the equipment, should address the following security services:

- logical access controls to, and between, the FS-PLC, including human-machine interfaces. Such logical control is restricted to a known community of users who are approved by management to access one or more of the devices. Commonly, logical access is restricted to a small group of users who install, maintain and administer those services and granted on a role basis to selectively access, change and/or use specified information.
- management controls so that within a particular security environment there is a common approach to the management and administration of the security policy, with a single authority having overall responsibility.
- physical controls to limit unauthorized access to the FS-PLC (including backup materials, cabling, connections).

Where applicable, the FS-PLC manufacturer shall provide guidelines on how these shall be accomplished.

Based on the security threat and hazard analysis, appropriate measures shall be applied. For example:

a) control of communication writes,
b) mechanical or logical key switch access,
c) guidelines to limit physical access, for example by means of locked enclosures,
d) guidelines of limited access via networks,
e) integral password protection,
f) tamper-proof seals,
g) change management detection and tracking.

5.3 Quality management system

A quality management system shall be used for development and manufacturing of FS-PLCs that:

- is a precondition for HW (incl. ASIC, FPGA etc.) / SW design and development and manufacturing of the FS-PLC,
- describes requirements for HW (incl. ASIC, FPGA etc.) / SW development and manufacturing processes,
- ensures that FS-PLCs comply to the requirements defined in this standard and all referenced normative standards,

- ensures well documented results of HW (incl. ASIC, FPGA etc.) / SW development and test,
- ensures reproducible, well documented steps of HW (incl. ASIC, FPGA etc.) / SW development and manufacturing,
- includes change management/revision control and configuration management systems.

NOTE An example of requirements for a quality management system is described in ISO 9001.

5.4 Management of FS-PLC safety lifecycle

5.4.1 Objectives

The first objective of the requirements of 5.4 is to specify the responsibilities in the management of functional safety of those who have responsibility for an FS-PLC, or for one or more phases of the FS-PLC system and software safety lifecycles.

The second objective of the requirements of 5.4 is to specify the activities to be carried out by those with responsibilities in the management of functional safety.

NOTE The organizational measures dealt with in 5.4 provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of functional safety of the FS-PLC. The technical requirements necessary for maintaining functional safety is specified as part of the information provided by the manufacturer. See Clause 16.

5.4.2 Requirements and procedures

5.4.2.1 Requirements

5.4.2.1.1 General

An organisation with responsibility for an FS-PLC realisation, or for one or more phases of the overall, FS-PLC system or software safety lifecycle, shall appoint one or more persons to take overall responsibility for:

- the FS-PLC and for its lifecycle phases;
- coordinating the safety-related activities carried out in those phases;
- the interfaces between those phases and other phases carried out by other organisations;
- carrying out the requirements of 5.4.2.1.2 to 5.4.2.1.11 and 5.4.2.2.2;
- coordinating functional safety assessments (see 5.4.2.1.11 b) and Clause 14) – particularly where those carrying out the functional safety assessment differ between phases – including communication, planning, and integrating the documentation, judgements and recommendations;
- ensuring that functional safety is achieved and demonstrated in accordance with the objectives and requirements of this standard.

It is permitted to delegate the responsibility for safety-related activities or safety lifecycle phases to other persons, particularly those with relevant expertise. However, this delegation is to reside with one or with a small number of persons with sufficient management authority.

5.4.2.1.2 Policy and strategy for achieving functional safety

The policy and strategy for achieving functional safety shall be specified, together with the means for evaluating their achievement, and the means by which they are communicated within the organization.

5.4.2.1.3 Identification of responsibility

All persons, departments and organizations responsible for carrying out activities in the applicable overall FS-PLC system or software safety lifecycle phases (including persons responsible for verification and functional safety assessment and, where relevant, licensing authorities or safety regulatory bodies) shall be identified, and their responsibilities shall be fully and clearly communicated to them.

5.4.2.1.4 Information communication

Procedures shall be developed for defining what information is to be communicated between relevant parties and how that communication will take place.

NOTE See Clause 5 of IEC 61508-1:2010 for documentation requirements.

5.4.2.1.5 Follow-up

Procedures shall be developed for ensuring prompt follow-up and satisfactory resolution of recommendations relating to the FS-PLC, including those arising from:

a) functional safety assessment (see Clause 14);

b) verification activities (see Clause 13);

c) validation activities (see Clause 11);

d) configuration management (see Clause 15).

5.4.2.1.6 Field failure and user information analysis

Procedures shall be developed for analysing available field failure and user information, including:

- recognising systematic faults that could jeopardise functional safety;
- assessing whether the failure rates during operation and maintenance are in accordance with the requirements specified during the life cycle phase overall scope definition.

5.4.2.1.7 Internal quality audits

Requirements for periodic internal quality audits of the FS-PLC design and manufacturing processes shall be specified, including:

a) the frequency of the internal quality audits;

b) the level of independence of those carrying out the audits;

c) the necessary documentation, corrective actions and follow-up activities.

5.4.2.1.8 Modification

Procedures shall be developed for:

a) initiating modifications to the FS-PLC;

b) obtaining approval and authority for modifications.

5.4.2.1.9 Maintaining information

Procedures shall be developed for maintaining accurate information on faults and failures of the FS-PLC.

5.4.2.1.10 Configuration management

Procedures shall be developed for configuration management of the FS-PLC, including in particular:

a) the point, in respect to specific phases, at which formal configuration control is to be implemented;

b) the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);

c) the procedures for preventing unauthorized items from entering service.

5.4.2.1.11 Software configuration management

Procedures shall be developed for software configuration management of the FS-PLCs during the relevant FS-PLC safety lifecycle phases. In particular, the following shall be specified:

a) the administrative and technical controls throughout the software functional safety lifecycle, in order to manage software changes and thus ensure that the specified requirements for software functional safety continue to be satisfied,

b) a guarantee that all necessary operations have been carried out to demonstrate that the required software functional safety integrity has been achieved,

c) a means for accurately maintaining, with unique identification, all configuration items which are necessary to meet the safety integrity requirements of the FS-PLC,

d) configuration items including at least the following:

- functional safety analysis and requirements,
- software specification and design documents,
- software source code modules,
- test plans and results,
- pre-existing software and SW packages which are to be incorporated into the FS-PLC,
- all tools and development environments which are used to create, test or carry out any action on the software of the FS-PLC.

e) change-control procedures:

- to prevent unauthorized modifications,
- to document modification requests,
- to analyse the impact of a proposed modification,
- to approve or reject the modification request;
- to document the details of, and the authorisation for, all approved modifications,
- to establish configuration baseline at appropriate points in the software development,
- to document the (partial) integration testing which justifies the baseline and
- to guarantee the composition of, and the building of, all software baselines (including the rebuilding of earlier baselines).

Management decision and authority is needed to guide and enforce the use of administrative and technical controls.

f) a procedure that ensures that appropriate methods are implemented to load application software and data into FS-PLC,

Specific target location systems as well as general systems are to be considered if possible.

g) documentation of the following information to permit a subsequent configuration audit:

- configuration status,
- release status,
- justification for, and approval of, all modifications
- details of the modification.

h) formal documentation of the release of functional safety-related software. Master copies of the software and all associated documentation and version of data in service shall be kept to document maintenance and modification throughout the operational lifetime of the released software.

NOTE For further information on configuration management, see ISO/IEC 12207, IEEE 828-2005, IEEE 1042-1987.

5.4.2.2 Individuals managing functional safety

5.4.2.2.1 Individuals and specification of activities

Those individuals who have responsibility for one or more phases of the FS-PLC system or software safety lifecycles shall, in respect of those phases for which they have responsibility and in accordance with the procedures defined in 5.4.2.1 and its subclauses, specify all management and technical activities that are necessary to ensure the achievement, demonstration and maintenance of functional safety of the FS-PLC, including:

a) the selected measures and techniques used to meet the requirements of a specified clause or subclause;

b) the functional safety assessment activities, and the way in which the achievement of functional safety will be demonstrated to those carrying out the functional safety assessment (see Clause 14);

Appropriate procedures for functional safety assessment shall be used to define

- the selection of an appropriate organisation, person or persons, at the appropriate level of independence;
- the drawing up, and making changes to, terms of reference for functional safety assessments;
- the change of those carrying out the functional safety assessment at any point during the lifecycle of a system;
- the resolution of disputes involving those carrying out functional safety assessments.

5.4.2.2.2 Procedures and individuals

Procedures shall be available to ensure that all persons with responsibilities defined in accordance with 5.4.2.1 and 5.4.2.1.3 (i.e. including all persons involved in any FS-PLC system or software lifecycle activity, including activities for verification, management of functional safety and functional safety assessment), shall have the appropriate competence (i.e. training, technical knowledge, experience and qualifications) relevant to the specific duties that they have to perform. Such procedures shall include requirements for the refreshing, updating and continued assessment of competence.

5.4.2.2.3 Competence and individuals

The appropriateness of competence shall be considered in relation to the particular application, taking into account all relevant factors including:

a) the responsibilities of the person;

b) the level of supervision required;

c) the safety integrity levels of the FS-PLC – the higher the safety integrity levels, the more rigorous shall be the specification of competence;

d) the novelty of the design, design procedures or application – the newer or more untried these are, the more rigorous shall be the specification of competence;

e) previous experience and its relevance to the specific duties to be performed and the technology being employed – the greater the required competence, the closer the fit shall be between the competences developed from previous experience and those required for the specific activities to be undertaken;

f) the type of competence appropriate to the circumstances (for example qualifications, experience, relevant training and subsequent practice, and leadership and decision-making abilities);

g) engineering knowledge appropriate to the application area and to the technology;

h) safety engineering knowledge appropriate to the technology;

i) knowledge of the legal and safety regulatory framework;

j) relevance of qualifications to specific activities to be performed.

The competence of all persons with responsibilities defined in accordance with 5.4.2.1 and 5.4.2.1.3 shall be documented.

5.4.2.3 Suppliers

Suppliers providing products or services to an organization having overall responsibility for the FS-PLC or software safety lifecycles (see 5.4.2.1), shall deliver products or services as specified by that organization and shall have an appropriate quality management system.

Suppliers shall have a quality management system and in addition an appropriate functional safety management system.

5.4.2.4 Software functional safety planning

The functional safety planning shall define the strategy for the software procurement, development, integration, verification, validation and modification to the extent required by the safety integrity level of the safety functions implemented by the FS-PLC.

NOTE 1 The philosophy of this approach is to use the functional safety planning as an opportunity to customize this standard to take account of the required safety integrity for each safety function implemented by the FS-PLC.

When the software is intended to implement FS-PLC safety functions of different safety integrity levels, all of the software shall be treated as belonging to the highest safety integrity level, unless adequate independence between the FS-PLC safety functions of the different safety integrity levels can be shown in the implementation. The justification for independence shall be documented.

NOTE 2 See for IEC 61508-3:2010, 6.2.2 for additional topics.

5.4.3 Execution and monitoring

The activities specified as a result of 5.4.2 and its subclauses shall be implemented and monitored.

5.4.4 Management of functional safety

Activities relating to the management of functional safety shall be applied at the relevant phases of the FS-PLC and software safety lifecycles in accordance with the targeted SIL capability and IEC 61508.

6 FS-PLC design requirements specification

6.1 General

The first objective of this phase is to allocate the FS-PLC functional safety and the safety integrity requirements, contained in the design requirement specification. These are the FS-PLC focused functional safety and integrity requirements of the E/E/PE safety-related system for the intended application(s).

The second objective of this phase is to allocate a safety integrity level capability to the FS-PLC, based on the designated E/E/PE safety-related system function the FS-PLC is designed and specified to provide.

6.2 Design requirements specification contents

The FS-PLC design requirements specification shall contain:

a) allocation of safety requirement(s) to HW, SW or a combination thereof with sufficient detail for the design and development of the FS-PLC,

NOTE 1 Examples of FS-PLC safety functions are putting an output into a manufacturer-defined safe state or maintaining a manufacturer-defined safe state.

b) the intended SIL capability of the FS-PLC;

c) specification of the safe state or safe states of the FS-PLC;

d) specify the limitations of operation of the FS-PLC in low demand and high demand/continuous modes of operation;

NOTE 2 Where the FS-PLC is used in different configurations, different SIL capability limits can apply to the different configurations.

e) a description of all the measures and techniques necessary to achieve the required functional safety. The description shall include:

1) the time it takes an FS-PLC to process an external signal(s) to activate a specified function(s), e.g. FS-PLC safety function under normal and fault conditions, input-to-output, calculation to be delivered to output, external write to output, network communications, performance;

NOTE 3 The worst case response time for the FS-PLC safety function contributes to the worst case response time of the overall E/E/PE safety-related system safety function. See IEC 61784-3.

2) all information relevant to functional safety which may have an influence on the E/E/PE safety-related system design;

3) all interfaces with the FS-PLC;

4) external fault diagnostic tests;

NOTE 4 For example, the detection of shorted or open loads in the de-energized case for digital outputs.

5) all relevant modes of operation of the FS-PLC;

6) all required modes of behaviour of the FS-PLCs – in particular, behaviour on the detection of faults;

7) the significance of all hardware/software interactions – where relevant, any required constraints between the hardware and the software shall be identified and documented;

NOTE 5 Where these interactions are not known before finishing the design, only general constraints are stated.

8) limiting and constraint conditions for the FS-PLCs and any associated subsystems, for example timing constraints;

9) any specific requirements related to the procedures for starting-up and restarting the FS-PLCs;

10) the target hardware random failure rates for each failure effect to be considered during failure mode and effect analysis;

11) any requirements, constraints, functions and facilities for proof testing of the FS-PLC part of the E/E/PE safety-related system to be undertaken;

NOTE 6 Typically, the proof test interval for an FS-PLC is the useful Lifetime.

12) the electromagnetic immunity limits and performance criteria in accordance with requirements in 12.5;

NOTE 7 Based on agreement between the FS-PLC manufacturer and the user, higher limits are used for certain applications, e.g. light curtain applications in accordance with 61496-1.

13) the requirements for the control of errors on any external safety related digital communications;

14) the measures to be provided to restrict operation by unauthorised persons (key switches, locked cabinets, network access, passwords, etc.);

15) critical application-independent alarms and events, e.g. system degradation, scan overrun, power-fail restart;

16) cyber security – manufacturer to specify whether the FS-PLC may be connected to a non-secure network and any specific measures necessary for cyber security;

NOTE 8 For guidance on security risks analysis, see IEC 62443 series.

17) a description of the HMI, libraries, engineering tools, etc. where they are safety related;

18) the quality assurance/quality control measures in place;

19) the techniques and measures of Table B.1 of IEC 61508-2:2010 that are used.

6.3 Target failure rate

Based on a targeted SIL for the FS-PLC and its demand mode, a PFD (see Table 1) or PFH (see Table 2) for the FS-PLC is determined.

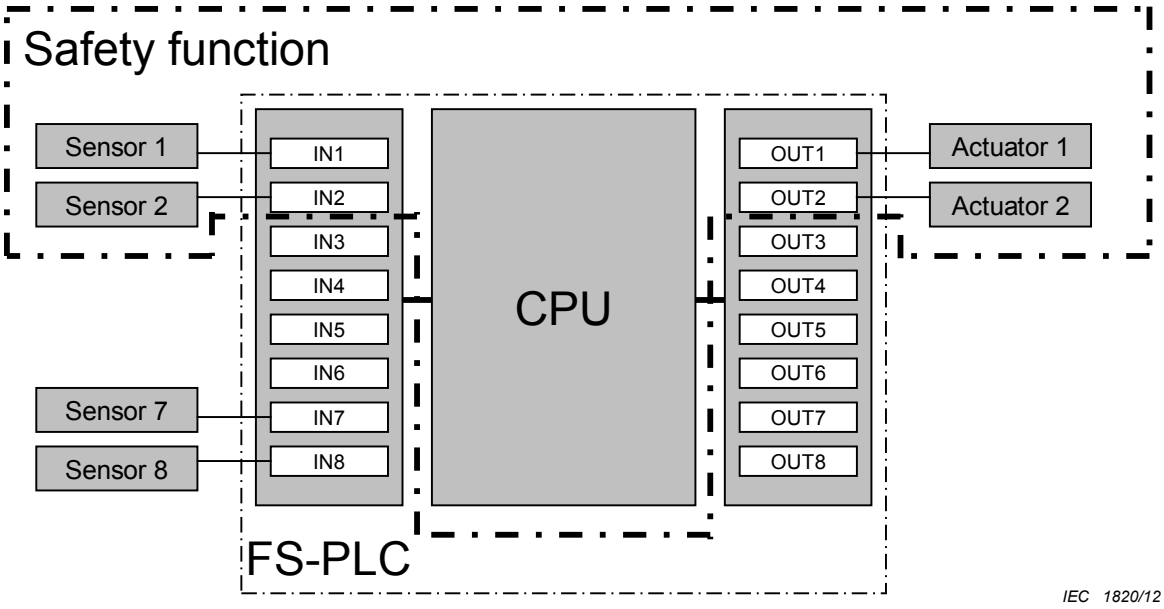


Figure 4 – Relevant parts of a safety function

Relevant parts of a safety function are illustrated in Figure 4.

Table 1 – Safety integrity levels for low demand mode of operation

SIL of safety-related system	PFD of the safety function	PFD of the FS-PLC contribution
4[a]	$\geq 10^{-5}$ to $< 10^{-4}$	$< k\ 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$< k\ 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$< k\ 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$< k\ 10^{-1}$
NOTE Typically $0 < k < 0{,}15$		
[a] This part applies to FS-PLC with a SIL capability not greater than SIL 3. For SIL 4 capability, additional FS-PLC safety function requirements of 61508 series shall be applied.		

Table 2 – Safety integrity levels for high demand or continuous mode of operation

SIL of safety-related system	PFH of the safety function	PFH of the FS-PLC contribution
4[a]	$\geq 10^{-9}$ to $< 10^{-8}$	$< k\ 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$< k\ 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$< k\ 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$< k\ 10^{-5}$
NOTE Typically $0 < k < 0{,}15$		
[a] This part applies to FS-PLC with a SIL capability not greater than SIL 3. For SIL 4 capability, additional FS-PLC safety function requirements of 61508 series shall be applied.		

The safety integrity requirement for the FS-PLC shall be specified in terms of PFD or PFH, only for random hardware failures. Where the safety integrity requirement is specified in terms of PFD, then the necessary proof test interval to achieve that PFD shall also be defined.

NOTE The PFD or PFH of a safety-related system is the sum of the PFD or PFH values for the sensors, the logic subsystem, and the actuators as part of a safety function. For illustration see Figure 4.

Systematic failures of an FS-PLC shall be addressed by techniques and measures in 9.4.6.

The FS-PLC's allocation of this PFD or PFH shall be specified by the FS-PLC manufacturer. This allocation is recommended to be less than or equal to 15 % (a "*k*" factor of 0,15 in the above tables), of the E/E/PE safety-related system's PFD or PFH.

The intent is to permit the allocation of the remainder, of the PFD or PFH, to the sensors and actuators.

A PFD or PFH allocation for the FS-PLC above the 15 % level is allowed based on a more rigorous analysis of the application and an agreement between the manufacturer and independent assessor in consultation with the user.

The FS-PLC safety function requirements and safety integrity requirements for the E/E/PE safety-related system function that the FS-PLC is designed and specified to provide, shall be documented in the FS-PLC design requirements specification.

7 FS-PLC design, development and validation plan

7.1 General

The FS-PLC safety function requirements and safety integrity requirements, for the E/E/PE safety-related system function the FS-PLC is designed and specified to provide, and specified in Clause 6, shall be planned for here.

7.2 Segmenting requirements

The objective of this phase is to segment the FS-PLC system functional safety and integrity requirements into SW functional safety and integrity requirements and HW functional safety and integrity requirements according to the documented architecture selected.

After partitioning of the FS-PLC system functional safety and integrity requirements into:

- SW functional safety and integrity requirements,
- HW functional safety and integrity requirements, and

- documentation of the assessments plans.

Clauses 9 and 10 define the FS-PLC HW (in realization phase) and the FS-PLC SW (in realization phase).

A development plan shall include an assessment plan and a set of HW and SW related design plans addressing appropriate items from Annex B of IEC 61508-2:2010.

8 FS-PLC architecture

8.1 General

The objective of Clause 8 is to specify the FS-PLC HW and SW safety architecture.

Based on the FS-PLC system functional safety requirements specification, various architectures may be evaluated to achieve the needs set forth in the functional safety requirements specification. Trade-offs will be made to determine and define where and how to execute the required FS-PLC safety functions necessary. These decisions will then set the overall FS-PLC architecture as well as the underlying SW and HW architectures.

The SW and HW architectural requirements shall be documented in the SW and HW functional safety requirements documents respectively.

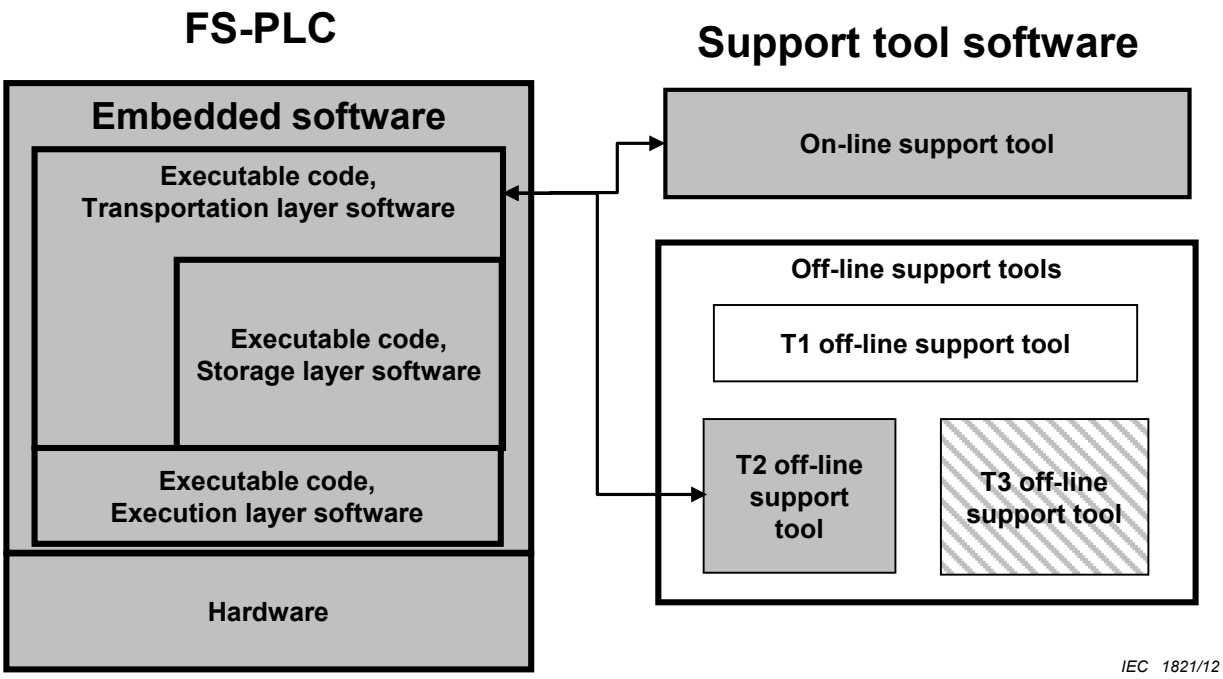


Figure 5 – FS-PLC to engineering tools relationship

The grey blocks, in Figure 5, are FS-PLC related areas and must be addressed. The white block is not a safety related part of FS-PLC, i.e. interference free. The cross-hatched block indicates the possibility of this item being considered safety-related based on criticality analysis. If the latter is safety-related, it shall be addressed.

The example items, in Figure 5, in white and cross-hatched blocks are for illustrative purposes only and may or may not be determined to be safety related in the application.

8.2 Architectures and subsystems

FS-PLC subsystems may incorporate multiple architectures.

An FS-PLC shall use a MooN architecture designation consisting of N channels, any one of which can contribute to processing of the FS-PLC logic function. At least M channels are required to perform the FS-PLC logic function. The system executes the FS-PLC logic function if M channels are functioning properly. (N-M) defines the fault tolerance of the system, where (N-M+1) channel failures would result in the failure of the FS-PLC logic function. See Annex B for examples.

8.3 Data communication

An FS-PLC system generally has two types of data communication. One is the safety related communication, and the other is non-safety related communication.

Functional safety related communication using fieldbuses shall comply with IEC 61784-3.

Safety related communication using other than fieldbuses shall comply with the requirement in IEC 61508-2:2010, 7.4.11.

For non-safety related communication, refer to IEC 61131-2.

Measures shall be taken to prevent any foreseeable data communication, whether valid or invalid, from a) adversely affecting the correct operation of a safety-related function, or b) preventing the maintenance of or achievement of a defined safe state.

9 HW design, development and validation planning

9.1 HW general requirements

The requirements of 8.3 are derived from the hardware specific requirements contained in the FS-PLC functional safety requirement specification.

9.2 HW functional safety requirements specification

The FS-PLC HW functional safety requirements shall be as specified in and/or derived from the FS-PLC functional safety requirements specification.

Where non safety-related functions are performed within the same FS-PLC as safety-related functions, adequate measures shall be in place to prevent safety-related functions from being adversely affected by non safety-related functions.

The FS-PLC HW functional safety requirements shall be expressed and structured in such a way that they are:

- clear, precise, unambiguous, verifiable, testable, maintainable and feasible; and
- written to aid comprehension by those who are likely to utilize the information at any stage of the FS-PLC safety lifecycle.

9.3 HW safety validation planning

NOTE This phase of the lifecycle of a FS-PLC is normally carried out in parallel with the HW design and development, see 9.4.

Hardware validation planning is accomplished by specifying the steps that are to be used to demonstrate compliance to the FS-PLC HW functional safety requirements specification (see Clause 6).

The functional safety validation plan shall include the procedures to be followed to assure that each safety function is correctly implemented and has the required SIL capability, a description of the test parameters and test environment and pass/fail criteria.

Type test are specified in Clause 12.

9.4 HW design and development

9.4.1 General

The FS-PLC shall be designed to meet the requirements of the HW functional safety requirements specification.

The HW designed and the documentation written during the design and documentation lifecycle phase of the FS-PLC shall meet all of the following:

a) the requirements for HW SIL capability (SIL 1, 2, or 3) based on the HW fault tolerance and safe failure fraction approach (Route 1_H of 7.4.4 and 7.4.4.2 of IEC 61508-2:2010) comprising,

   the architectural constraints on HW safety integrity of 9.4.3, 9.4.3.1.2 and

   the requirements for the probability of dangerous HW failures of 9.4.3.2.4;

b) the requirements for systematic safety integrity comprising,

   the requirements for the avoidance of systematic failures of 9.4.5, and

   the requirements for the control of systematic faults of 9.4.6.

c) the requirements for FS-PLC behaviour upon detection of a fault of 9.4.2.

d) independence of safety related and non-safety related functions unless all FS-PLC HW will be treated as safety related. The independence shall be such that failures in the non-safety parts shall not cause dangerous failures in the safety part. The method of achieving this independence and the justification of the method shall be documented.

9.4.2 Requirements for FS-PLC behaviour on detection of a fault

The detection of a dangerous fault during operation of the FS-PLC shall result in either:

a) the transition of all outputs, by built-in measures, e.g. HW or embedded SW, that could be affected by the fault to a defined safe state within the fault reaction time specified by the manufacturer, or

b) the fault being notified (alarmed) to the application measures, e.g. application program within the fault reaction time specified by the manufacturer such that the application measures, e.g. application program, can cause appropriate action to be taken to maintain safety.

NOTE What action is appropriate is dependent on the application and this is determined by the user rather than the FS-PLC manufacturer.

As a minimum the faults shown in Table 3 shall be detected and notified (alarmed) to the application program unless either

- the fault cannot occur in the FS-PLC by design, or
- the omission of the fault is justified by a written technical assessment.

Table 3 – Faults to be detected and notified (alarmed) to the application program

Faults to be detected and notified (alarmed) to the application program
scan time overrun – scan time is greater than a preset maximum value
input or output points are disabled or maintenance overrides are in place
fault detection is disabled
over temperature condition
failure of a diagnostic to execute
attempted write access via an unauthorized channel
degraded system operational modes – redundant modules/channels are off-line or faulted
loss of system or field power, including redundant sources
loss or delay of external safety-related communications
divide by zero or other logical error detected

9.4.3 HW safety integrity

9.4.3.1 HW fault tolerance

9.4.3.1.1 General

During design of the FS-PLC, the hardware fault tolerance related to functional safety shall be defined. The HW fault tolerance in combination with the safe failure fraction allows a specification of the maximum safety integrity (SIL 1, 2, or 3) that can be claimed in accordance with Route 1_H as described in IEC 61508-2.

9.4.3.1.2 Highest safety integrity level claimable

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware fault tolerance and safe failure fraction of the subsystems that carry out that safety function. Table 4 and Table 5 specify the highest safety integrity level that can be claimed for an FS-PLC safety function which uses a subsystem taking into account the hardware fault tolerance and safe failure fraction of that subsystem. The requirements of Table 4 and Table 5 shall be applied to each subsystem carrying out an FS-PLC safety function and hence every part of the FS-PLC. Subclauses 9.4.3.2.2 to 9.4.3.2.4 specify which one of Table 4 or Table 5 apply to any particular subsystem. Subclauses 9.4.3.2.5 and 9.4.3.2.6 specify how the highest safety integrity level that can be claimed for an FS-PLC safety function is derived. With respect to these requirements:

a) a hardware fault tolerance of N means that N+1 faults could cause a loss of the FS-PLC safety function. In determining the hardware fault tolerance no account shall be taken of other measures that may control the effects of faults such as diagnostics, and

b) where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault;

c) in determining hardware fault tolerance, certain faults may be excluded based on the physical behaviour of the component's dominant failure mode. Any such fault exclusions shall be justified and documented;

NOTE 1 ISO 13849-2:2003 gives examples for fault exclusion based on different technologies.

d) the safe failure fraction of a subsystem is defined as the ratio of the average rate of safe failures plus dangerous detected failures of the subsystem to the total average failure rate of the subsystem.

NOTE 2 The architectural constraints have been included in order to achieve a sufficiently robust architecture, taking into account the level of subsystem complexity. The hardware safety integrity level for the FS-PLC system, derived through applying these requirements, is the maximum that is permitted to be claimed even though, in some

cases, a higher safety integrity level could theoretically be derived if a solely mathematical approach had been adopted for the FS-PLC system.

NOTE 3 The architecture and subsystem derived to meet the hardware fault tolerance requirements is that used within specified operating conditions. The fault tolerance requirements may be relaxed while the FS-PLC system is being repaired on-line. However, the key parameters relating to any relaxation must have been previously evaluated (for example mean time to restoration compared to the probability of a demand).

Table 4 – Hardware safety integrity – low complexity (type A) subsystem

	Hardware fault tolerance		
SFF	**0**	**1**	**2**
<60 %	SIL 1	SIL 2	SIL 3
60 % to <90 %	SIL 2	SIL 3	SIL 4 [a]
90 % to <99 %	SIL 3	SIL 4[a]	SIL 4 [a]
≥99 %	SIL 3	SIL 4 [a]	SIL 4 [a]

[a] This part applies to FS-PLC with a SIL capability not greater than SIL 3. Special requirements apply for SIL 4 capability. See IEC 61508 series.

NOTE Table derived from IEC 61508-2:2010, Table 2.

Table 5 – Hardware safety integrity – high complexity (type B) subsystem

	Hardware fault tolerance		
SFF	**0**	**1**	**2**
<60 %	Not allowed	SIL 1	SIL 2
60 % to <90 %	SIL 1	SIL 2	SIL 3
90 % to <99 %	SIL 2	SIL 3	SIL 4 [a]
≥99 %	SIL 3	SIL 4 [a]	SIL 4 [a]

[a] This part applies to FS-PLC with a SIL capability not greater than SIL 3. Special requirements apply for SIL 4 capability. See IEC 61508 series.

NOTE Table derived from IEC 61508-2:2010, Table 3.

9.4.3.1.3 Requirements for FS-PLC behaviour on detection of a fault

The detection of a dangerous fault in a FS-PLC shall result in a specified action to either:

a) achieve or maintain the manufacturer-defined safe state, or

b) if the FS-PLC has a hardware fault tolerance of one or more then to repair the faulty part within the mean repair time (MRT) specified in the application, where continued operation is permitted, or if the FS-PLC has a hardware fault tolerance of zero and is in low demand mode then to repair the faulty part within the mean repair time (MRT) specified in the application. Continued operation during the repair of the FS-PLC requires additional risk reduction measures to be taken by the user.

9.4.3.1.4 Independent watchdog timers

All subsystems that utilize a microprocessor shall include a watchdog timer function which:

– is separated from and operated independently of the state of the microprocessor,

– is not affected by a common cause mechanism that may prevent the wrong watchdog reset by resetting the microprocessor.

The following types of watchdog reset mechanisms should be avoided:

a) the use of a range of memory or I/O addresses, only a single address should be used,

b) allowing both read and write operations, only one should be used,

c) using an address that might easily be accessed if the microprocessor is stuck in a loop,

d) using only a maximum time-out value, a window should be specified with a minimum and maximum value.

9.4.3.2 HW subsystem decomposition

9.4.3.2.1 General

NOTE 1 The reader is reminded that the term subsystem used in this part is defined differently than as defined in IEC 61508-4. See 3.55.

Subclause 9.4.3.1 defines requirements for safe failure fraction (SFF) and fault tolerance depending on safety integrity level and subsystem type.

Two subsystem types, defined in 9.4.3.2.2 and 9.4.3.2.3, are further explained by the following supplemental information:

Type A subsystems (low complexity) are typically built of discrete components (e.g. resistors, capacitors, diodes, transistors) for which the fault modes and their effect on the subsystem, are predictable and well-defined.

Type B subsystems (high complexity) typically include one or more complex or programmable components (e.g. microprocessors, ASICs, FS-PLC modules) which have poorly-defined fault modes with unpredictable effects on the subsystem. (For such components, in the absence of better data, it may be assumed that 50 % of all faults lead to a safe effect and 50 % lead to a dangerous effect.)

NOTE 2 Integrated circuits of low complexity are those for which all of the failure modes and fault effects are known.

When evaluating an FS-PLC, the FS-PLC shall first be decomposed into subsystems. Each subsystem must fulfil the requirements of Table 4 or Table 5, with regard to SFF and fault tolerance necessary to achieve the specified SIL.

If two subsystems are dependent and one subsystem provides the diagnostics for the other subsystem, the subsystem providing the diagnostics must first meet the requirements of Table 4 or Table 5. The subsystem providing the diagnostics can then be combined with the second subsystem to fulfil the requirements of Table 4 or Table 5 for both subsystems together.

NOTE 3 Example; FS-PLC I/O modules are typically composed of a microprocessor and an I/O part as shown in Figure 6. The processor element controls the I/O and often executes the diagnostics as well. In such a case the processor element shall be treated as a Type B subsystem and the I/O could be either a Type B or Type A subsystem depending on the subsystem components.

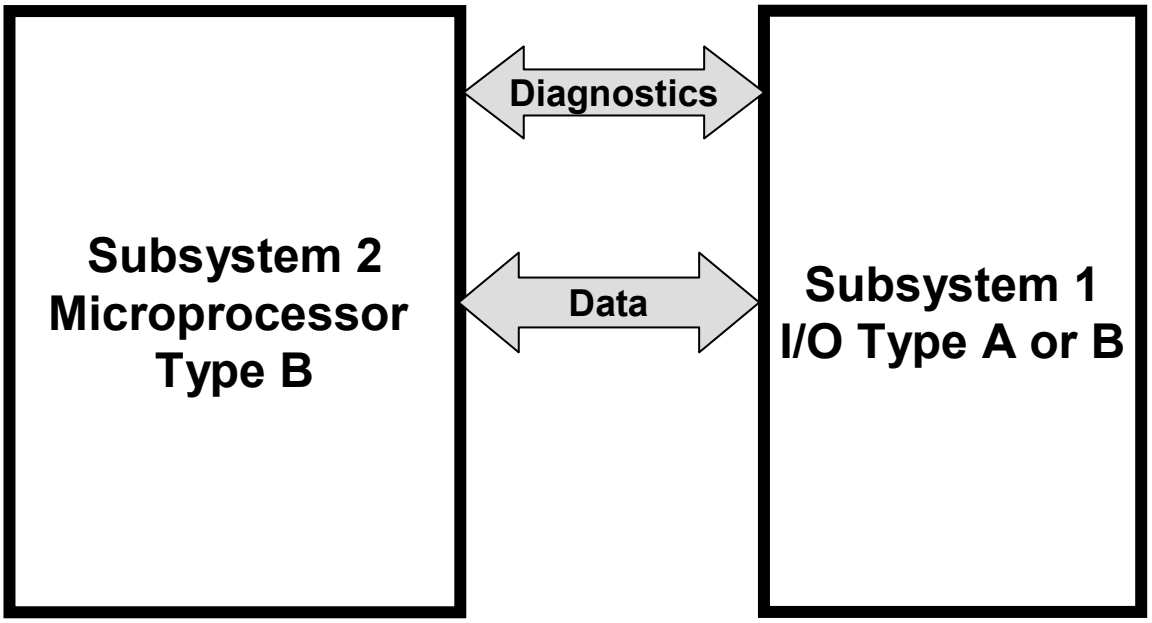


Figure 6 – HW subsystem decomposition

Consider the case of an I/O module, which is composed of two subsystems, one a Type A or B, designated Subsystem 1 and one a Type B, designated Subsystem 2. It is intended this I/O module achieve SIL 3.

Assume Subsystem 1 has a fault tolerance of 1 and a SFF of 55 %, by itself. Assume Subsystem 2 has a fault tolerance of 1 and a SFF of 95 %, by itself.

If Subsystem 1 takes advantage of the processor element of Subsystem 2, to conduct diagnostics, it can achieve a high DC and SFF (near 100 %).

However, when combining diagnostics, a number of items must be considered. Because the subsystems 1 and 2 form a series, both must have a SFF > 90 %. This means that the diagnostics of subsystem 1 must be ≥ 90 % if it contains type B components and > 60 % when it contains only type A components. Claiming type A will be difficult as the control lines for the diagnostics come from a type B subsystem, so the interface of these two subsystems must have a diagnostic coverage of 90 %. To claim a certain diagnostic coverage this has to be in line with Annex B of IEC 61508-2:2010.

Table 5 would require an SFF of at least 90 % for the I/O module to achieve SIL 3.

Before Subsystem 1 utilized the processor of Subsystem 2, for diagnostics, the combination of Subsystems 1 and 2 could not achieve a SFF greater than 90 %. With Subsystem 1 utilizing the processor of Subsystem 2, for diagnostics, the combination of Subsystems 1 and 2 can now achieve a SFF greater than 90 %, and hence the I/O module can achieve SIL 3.

9.4.3.2.2 Type A subsystem

A subsystem can be regarded as type A if, for the components required to achieve the FS-PLC portion of the safety function

a) the failure modes of all constituent components are well defined; and
b) the behaviour of the subsystem under fault conditions can be completely determined; and
c) there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 9.4.8).

9.4.3.2.3 Type B subsystem

A subsystem shall be regarded as type B if, for the components required to achieve the FS-PLC portion of the safety function,

a) the failure mode of at least one constituent component is not well defined; or

b) the behaviour of the subsystem under fault conditions cannot be completely determined; or

c) there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures (see 9.4.8).

NOTE 1 This means that if at least one of the components of a subsystem itself satisfies the conditions for a type B subsystem then that subsystem is regarded as type B rather than type A.

NOTE 2 The FS-PLC is a complex (type B) subsystem. At the same time the FS-PLC can be composed of subsystems that are type A or type B.

9.4.3.2.4 Architectural constraints on type A and type B subsystems

Table 4 and Table 5 specify a SFF that is required to fulfil the specification for a SIL 1, 2 or 3 claim, based on the hardware fault tolerance. The architectural constraints of either Table 4 or Table 5 shall apply to each subsystem carrying out the FS-PLC portion of the safety function, so that:

a) the hardware fault tolerance requirements shall be achieved for the whole of the FS-PLC system;

b) Table 4 applies for every type A subsystem forming part of the FS-PLC system;

c) Table 5 applies for every type B subsystem forming part of the FS-PLC system;

d) both Table 4 and Table 5 will be applicable to the FS-PLC system comprising both type A and type B subsystems, since the requirements in Table 4 shall apply for the type A subsystems and the requirements in Table 5 shall apply for the type B subsystems.

9.4.3.2.5 Serial combinations of subsystems

In an FS-PLC system where a number of element safety functions are implemented through a serial combination of elements (such as in Figure 7), the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by the element that has achieved the lowest safety integrity level for the achieved safe failure fraction for a hardware fault tolerance of 0. To illustrate the method assume an architecture as indicated in Figure 7, and see example below.

EXAMPLE (see Figure 7) Assume an architecture where a number of subsystem safety functions are performed by a single channel of subsystems 1, 2 and 3 as in Figure 7 and the subsystems meet the requirements of Table 4 and Table 5 as follows:

– subsystem 1 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1;

– subsystem 2 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;

– subsystem 3 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1;

– both subsystem 1 and subsystem 3 restrict the maximum SIL that can be claimed, for the achieved hardware fault tolerance and safe failure fraction to just SIL 1.

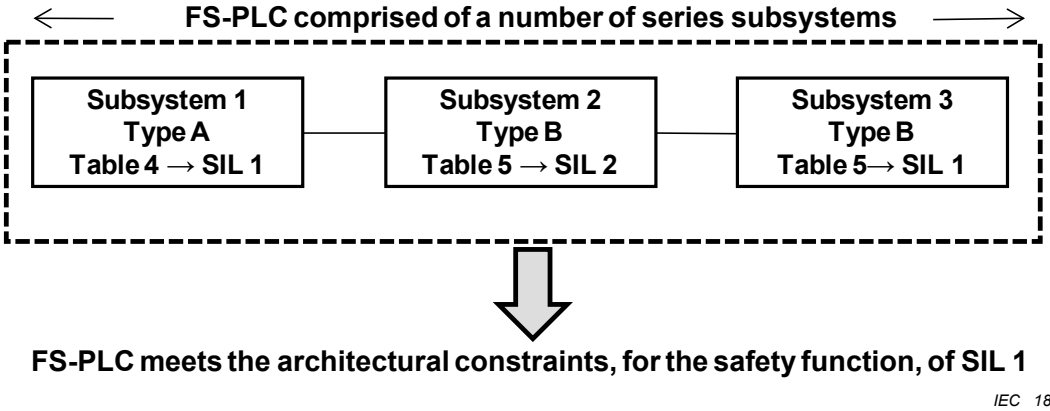


Figure 7 – Example: determination of the maximum SIL for specified architecture

9.4.3.2.6 Parallel combinations of subsystems

In a FS-PLC system where its safety function is implemented through multiple channels of subsystems (such as in Figure 8), the maximum hardware safety integrity level that can be claimed for its safety function under consideration shall be determined by:

a) grouping the serial combination of elements for each channel and then determining the maximum safety integrity level that can be claimed for the safety function under consideration for each channel (see 9.4.3.2.5); and

b) selecting the channel with the highest safety integrity level that has been achieved for the safety function under consideration and then adding 1 safety integrity level to determine the maximum safety integrity level for the overall combination of the subsystem.

c) At the minimum the following requirements shall be fulfilled:

- the safety function shall be performed in each subsystem,
- common cause failure analysis shall be performed according to the claimed SIL,
- the voter at the output of the subsystems shall be designed according to the claimed SIL,
- failure reaction of the combined system shall meet the requirements of IEC 61508-2:2010, 7.4.8,
- the DC of the FS-PLC shall fulfil the requirements of the SIL of the combined system,
- the software/firmware used in the FS-PLC shall fulfil the requirements of the SIL of the combined system.

d) Assumptions:

- a systematic fault of that subsystem does not cause a failure of the specified safety function but does so only in combination with a second systematic fault of another subsystem,
- sufficient independence exists between the two subsystems (justified by common cause failure analysis).

EXAMPLE The grouping and analysis of these combinations may be carried out in various ways. To illustrate one possible method, assume an architecture in which a particular FS-PLC safety function is performed by two subsystems, X and Y, where subsystem X consists of subsystems 1, 2, 3 and 4, and subsystem Y consists of a single subsystem 5, as shown in Figure 8. The use of parallel channels in subsystem X ensures that subsystems 1 and 2 implement the part of the FS-PLC safety function required of subsystem X independently from subsystem 3 and 4, and vice-versa. The FS-PLC safety function will be performed:

– in the event of a fault in either subsystem 1 or subsystem 2, the combination of subsystems 3 and 4 is able to perform the required part of the FS-PLC safety function; or

– in the event of a fault in either subsystem 3 or subsystem 4, the combination of subsystems 1 and 2 is able to perform the required part of the FS-PLC safety function.

The determination of the maximum safety integrity level that can be claimed, for the safety function under consideration, is detailed in the following steps.

For subsystem X, with respect to the specified FS-PLC safety function under consideration, each subsystem meets the requirements of Table 4 and Table 5 as follows:

- subsystem 1 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 3;
- subsystem 2 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;
- subsystem 3 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;
- subsystem 4 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1.

Subsystems are combined to give a maximum hardware safety integrity level for the FS-PLC safety function under consideration, for subsystem X as follows:

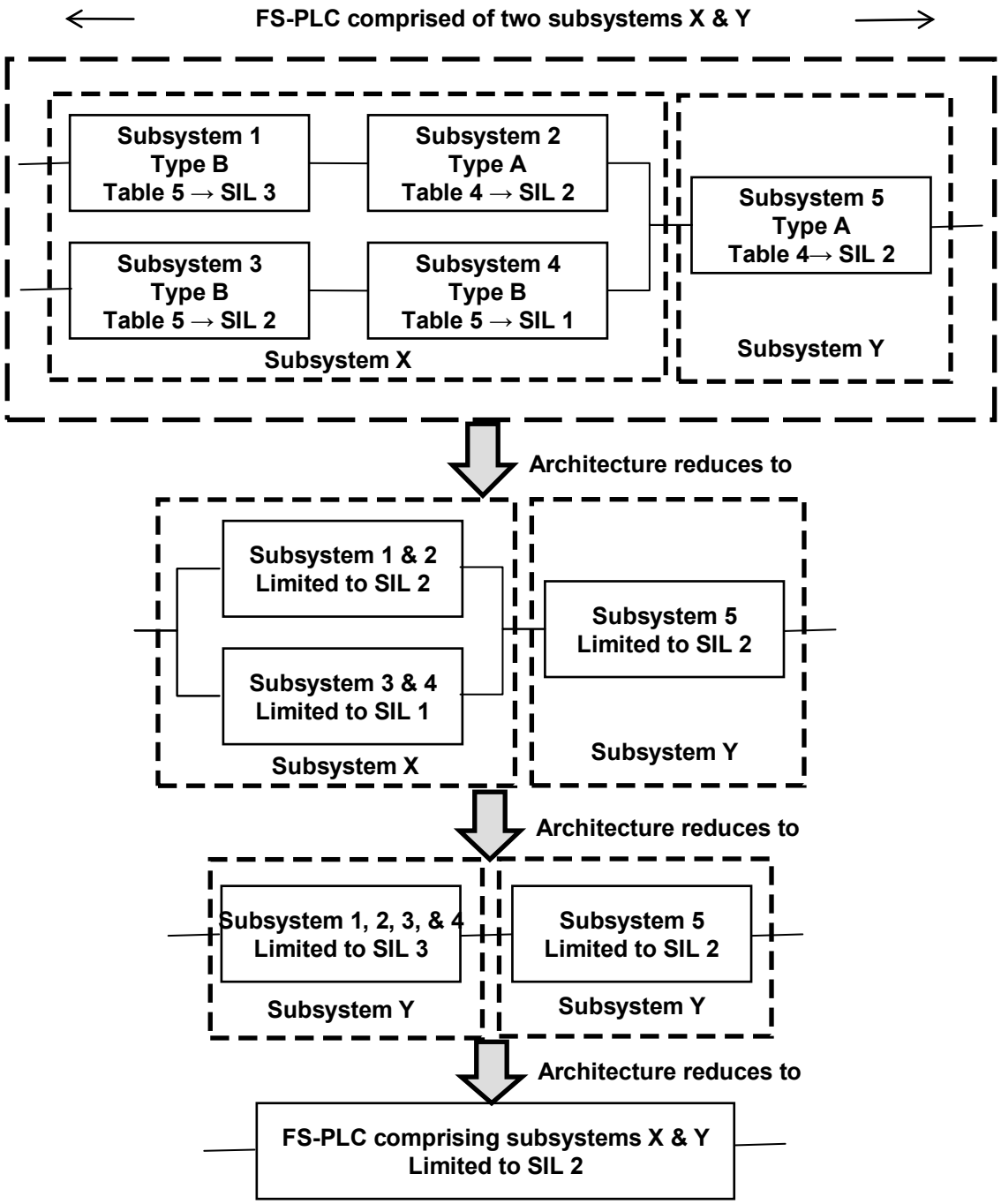
a) Combining subsystems 1 and 2: The hardware fault tolerance and safe failure fraction achieved by the combination of subsystems 1 and 2 (each separately meeting the requirements for SIL 3 and SIL 2 respectively) meet the requirements of SIL 2 (determined by subsystem 2; see 9.4.3.2.5);

b) Combining subsystems 3 and 4: The hardware fault tolerance and safe failure fraction achieved by the combination of subsystems 3 and 4 (each separately meeting the requirements for SIL 2 and SIL 1 respectively) meet the requirements of SIL 1 (determined by subsystem 4 see 9.4.3.2.5);

c) Further combining the combination of subsystems 1 and 2 with the combination of subsystems 3 and 4: the maximum safety integrity level that can be claimed for the FS-PLC safety function under consideration is determined by selecting the channel with the highest safety integrity level that has been achieved and then adding 1 safety integrity level to determine the maximum safety integrity level for the overall combination of subsystems. In this case the subsystem comprises two parallel channels with a hardware fault tolerance of 1. The channel with the highest safety integrity level, for the FS-PLC safety function under consideration was that comprising subsystems 1 and 2 which achieved the requirements for SIL 2. Therefore, the maximum safety integrity level for the subsystem for a hardware fault tolerance of 1 is (SIL 2 + 1) = SIL 3 (see 9.4.3.2.6).

For subsystem Y, subsystem 5 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2.

For the complete FS-PLC (comprising two subsystems X and Y that have achieved the requirements, for the safety function under consideration, of SIL 3 and SIL 2 respectively), the maximum safety integrity level that can be claimed for an FS-PLC is determined by the subsystem that has achieved the lowest safety integrity level (9.4.3.1.2). Therefore, for this example, the maximum safety integrity level, that can be claimed for the FS-PLC, for the safety function under consideration, is SIL 2.



FS-PLC meets the architectural constraints, for the safety function, of SIL 2

IEC 1824/12

NOTE 1 Subsystems 1 and 2 implement the part of the safety function required of subsystem X independently from elements 3 and 4, and vice versa.

NOTE 2 The subsystems implementing the FS-PLC safety function will be across the entire FS-PLC system in terms of ranging from the inputs to logic solving to outputs.

NOTE 3 For details on interpreting this figure, see the example described above.

NOTE 4 Type A only applies to a subsystem of an FS-PLC. Type B can apply to subsystem of FS-PLC or to FS-PLC itself.

Figure 8 – Example of limitation on hardware safety integrity for a multiple-channel safety function

9.4.4 Random HW failures

9.4.4.1 General

The probability of dangerous failure due to random HW failures shall be equal or less than the target failure measure as specified in the functional safety requirements specification.

Random hardware failures for a design shall be identified and analyzed by failure modes and effects analysis (FMEA), fault tree analysis, or other acceptable methods (see Annex A). The failure rates for each component shall be estimated from a recognized reliability database. Each failure shall be classified into one of the following categories, using a diagnostics coverage analysis:

- safe detected,
- safe un-detected,
- dangerous detected,
- dangerous undetected
- no effect.

All reliability calculations shall use one single source for the component reliability data. Data from multiple sources can be used only if it can be shown that the data was developed under common conditions. For further information see Annex D.

Once these failure rates are determined, a reliability model for the FS-PLC must be established and a calculation method must be selected. This is a prerequisite to determining the PFD or PFH value of the subsystems and the FS-PLC. Annex B of IEC 61508-6:2010 addresses the PFD and PFH calculations and shall be utilized for various architectures of an FS-PLC; e.g. 1oo1, 1oo2, 1oo2D (with diagnostics), 2oo2, and 2oo3, etc.

For complex systems like a FS-PLC reliability calculation based on reliability block diagrams or a Markov model is recommended.

NOTE When suitable data is available, the failure is apportioned between the predominant failure modes: short, open, change of value, etc.

9.4.4.2 HW common cause failures

Where the FS-PLC architecture includes multiple channels, for example 1oo2 or 2oo3 architectures, then common cause failures shall be considered.

A common cause failure is a failure which is the result of one or more events which cause a coincident or near-coincident failure of two or more separate channels in a multiple channel system, potentially resulting in the loss of the safety function. Common cause failures may result from a systematic fault (for example, a design or specification mistake) or an external stress leading to a hardware failure, (for example an excessive temperature).

Common cause failure rates shall be estimated using a recognised method. Typically, such methods apply a proportion of the hardware random failure rate for one channel as a common cause failure rate for the multiple channel system. The value of the proportion – the Beta factor – is determined by a scoring system based on the degree of independence of the channels and the possibility of detecting faults before they affect all channels.

The suitability of the method chosen for assessing common cause failures in the FS-PLC design shall be justified.

NOTE Annex E gives one possible method for assessing common cause failures. More discussion is given in Annex D of IEC 61508-6:2010.

9.4.4.3 HW diagnostic coverage (DC)

The diagnostic coverage of a FS-PLC system can be calculated as follows:

- create a reliability model of the FS-PLC using suitable subsystems
- carry out a Failure Mode and Effects Analysis (FMEA) for each component of each subsystem
- categorize each failure mode according to whether it leads to a safe failure effect or a dangerous effect as defined by the safe state and intended applications of the FS-PLC as declared by the manufacturer

  NOTE 1 Where data is not available for high complexity components, it can be assumed that 50 % of the random hardware failures are safe and 50 % are dangerous. This assumption can also be applied to subsystems but is typically not used.

- calculate the failure rate of safe failures (λ_S) and the failure rate of dangerous failures (λ_D), for each subsystem
- estimate the failure rate of dangerous failures which will be detected by diagnostic tests (λ_{DD}), for each subsystem
- calculate the failure rate of dangerous failures which will not be detected by diagnostic tests (λ_{DU}), for each subsystem

  NOTE 2 $\lambda_D = \lambda_{DD} + \lambda_{DU}$.

- calculate the diagnostic coverage (DC mean value) and safe failure fraction (SFF mean value) for each subsystem:

  $DC = \Sigma \lambda_{DD} / \Sigma \lambda_D = \Sigma \lambda_{DD} / [\Sigma \lambda_{DU} + \Sigma \lambda_{DD}]$

- when one of these failure rates is not constant, its average over the period shall be estimated and used in DC and SFF calculations.

Diagnostic coverage for the same subsystem by two or more diverse methods can be used to claim a higher diagnostic coverage than typically permitted by IEC 61508 series. The diverse methods must be independent and not have common cause failure modes.

Table 6 lists the faults or failures that shall, as a minimum, be detected in order to achieve the indicated diagnostic coverage.

See Annex A of IEC 61508-2:2010 for a more comprehensive listing of the techniques and measures that, when applicable, shall be incorporated into an FS-PLC for controlling random hardware, systematic, environmental, and operational failures. Annex A of IEC 61508-2:2010 also goes further into explaining these techniques and measures.

Table 6 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction

Component	See Table(s) IEC 61508-2:2010 Annex A	Requirements for diagnostic coverage claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Electromechanical devices	A.2	Does not energize or de-energize; Welded contacts	Does not energize or de-energize; Individual contacts welded	Does not energize or de-energize Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent) No positive opening (for position switches this failure is not assumed if they are built and tested according to IEC 60947-5-1, or equivalent)
Discrete hardware	A.3, A.7, A.9			
Digital I/O		Stuck-at[b]	DC fault model[c]	DC fault model[c]; Drift[d] and oscillation
Analogue I/O		Stuck-at[b]	DC fault model[c]; Drift and oscillation	DC fault model[c]; Drift and oscillation
Power supply		Stuck-at[b]	DC fault model[c]; Drift and oscillation	DC fault model[c]; Drift and oscillation
Bus	A.3 A.7 A.8			
General		Stuck-at[b] of the addresses	Time out Wrong address decoding	Time out Wrong address decoding
Memory management unit (MMU)		Stuck-at[b] of data or addresses	Change of addresses caused by soft-errors in the MMU registers[d e]	Change of addresses caused by soft-errors in the MMU registers[d e]
Direct memory access (DMA)		No or continuous access	DC fault model[c] for data and addresses; Change of information caused by soft-errors in the DMA registers Wrong access time	All faults which affect data in the memory; Wrong access time
Bus-arbitration[a]		Stuck-at[b] of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration

Component	See Table(s) IEC 61508-2:2010 Annex A	Requirements for diagnostic coverage claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
CPU/Processor	A.4, A.10			DC fault[c] model for data and addresses;
Register, internal RAM		Stuck-at[b] for data and addresses	DC fault[c] model for data and addresses Change of information caused by soft-errors	Dynamic cross-over for memory cells; Change of information caused by soft-errors
Coding and execution including flag register		Wrong coding or no execution	Wrong coding or wrong execution	No, wrong or multiple addressing No definite failure assumption
Address calculation		Stuck-at[b]	DC fault model[c] Change of information caused by soft-errors	No definite failure assumption
Program counter, stack pointer		Stuck-at[b]	DC fault model[c] Change of information caused by soft-errors	DC fault model[c] Change of information caused by soft-errors
Interrupt handling **Interrupt**	A.4	No or continuous interrupts[f]	No or continuous interrupts[f]; cross-over of interrupts	No or continuous interrupts[f]; cross-over of interrupts
Reset circuitry	A.4	Stuck-at[b] Individual components do not initialize to reset state	DC fault model[c] Drift and oscillation Individual components do not initialize to reset state	DC fault model[c] Drift and oscillation Individual components do not initialize to reset state
Read-only memory/Invariable memory	A.5	Stuck-at[b] for data and addresses	DC fault[c] model for data and addresses	All faults which affect data in the memory
Read-write memory/Variable memory	A.6	Stuck-at[b] for data and addresses	DC fault[c] model for data and addresses; Change of information caused by soft-errors	DC fault[c] model for data and addresses; Dynamic cross-over for memory cells; No, wrong or multiple addressing; Change of information caused by soft-errors
Clock (quartz, oscillator, PLL)	A.11	Sub- or super-harmonic Period jitter	Incorrect frequency Period jitter	Incorrect frequency Period jitter
Communication and mass storage	A.12	Wrong data or addresses;	All faults which affect data in memory;	All faults which affect data in

Component	See Table(s) IEC 61508-2:2010 Annex A	Requirements for diagnostic coverage claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
		No transmission	Wrong data or addresses; Wrong transmission time; Wrong transmission sequence	memory; Wrong data or addresses; Wrong transmission time; Wrong transmission sequence

NOTE For ASICs, this table and Tables A.2 to A.18 of IEC 61508-2:2010 apply where relevant.

a Bus-arbitration is the mechanism for deciding which device has control of the bus.

b "Stuck-at" is a fault category which can be described with continuous "0" or "1" or "on", e.g. at the pins of a component.

c "DC fault model" (DC = direct current) includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines. For integrated circuits short circuit between any two connections (pins) is considered.

d The soft-error rate (SER) for low energized semiconductors is known to be more than one order of magnitude higher (50x..500x) than the hard-error rate (permanent damage of the device). See reference to IEC 61508-7:2010, A.5.

e Causes of soft errors are: alpha particles from package decay, neutrons, external EMI noise and internal cross-talk. The effect of soft-errors can only be mastered by safety integrity measures at runtime. Safety integrity measures effective for random hardware failures may not be effective for soft-errors. Example: RAM tests, such as walk-path, galpat, etc. are not effective, whereas monitoring techniques using Parity and ECC with recurring read of the memory cells or techniques using redundancy (and comparison or voting) can be.

f No interrupt means that no interrupt is carried out when an interrupt(s) should take place. Continuous interrupts means that continuous interrupts are carried out when they should not take place.

9.4.4.4 HW safe failure fraction (SFF)

For complex subsystems or elements, a division of failures into 50 % safe and 50 % dangerous is generally accepted for, for example, subsystems or elements without diagnostic(s).

“No effect” components shall not be included in the calculation, e.g. LEDs, multiple filter capacitors.

Table 6 sets out the faults or failures to be detected during operation or to be analysed in the derivation of the safe failure fraction.

9.4.4.5 SIL capability calculations

In order to claim a specific SIL capability for a FS-PLC, both the qualitative techniques and measures specified in Annex B of IEC 61508-2:2010 and the quantitative values calculated using the equations of Annex B of IEC 61508-6:2010 shall be satisfied.

Incorporating these specific techniques and measures during the FS-PLC lifecycle addresses systematic failures. Doing the calculations of IEC 61508-6:2010, Annex B addresses random hardware failures.

The following focuses on the quantitative calculations of a SIL capability for a FS-PLC. This sequence of actions by the FS-PLC manufacturer simplifies the SIL calculation process:

a) determine the SIL specified for the intended field of application(s) – “the target SIL”,

b) determine whether the intended application(s) will require a low demand on the FS-PLC safety function or a high/continuous demand on the FS-PLC safety function or both – a low demand will require a PFD calculation while a high/continuous demand will require a PFH calculation,

c) specify the architecture for the FS-PLC,

d) establish that percentage of the PFD or PFH associated with the system SIL that will be allocated to the FS-PLC (see 6.3),

e) establish a Mean Time to Restoration (MTTR) and Mean Repair Time (MRT) for the FS-PLC when a failure occurs,

f) recommend one or more proof test intervals (T_1) for the FS-PLC,

g) determine the dangerous failure rates for the FS-PLC - both detected (λ_{DD}) and undetected (λ_{DU}) - based on hardware component failure rates (see 9.4.4.3) and associated calculations (see Annex B of IEC 61508-6:2010),

h) calculate the percentages of the common cause failures that are detected (β_D) and are not detected (β) See Annex E. (see also Annex D of IEC 61508-6:2010),

i) use the above parameters to calculate PFD and/or PFH per Annex B of IEC 61508-6:2010,

j) verify that the calculated value(s) meets the appropriate allocated ranges from Tables B.2, B.3, B.4, B.5, B.10, B11, B.12 and B.13 of IEC 61508-6:2010.

9.4.5 HW requirements for the avoidance of systematic failures

Techniques and measures to avoid systematic failures during hardware development described in Annex B of IEC 61508-2:2010 shall be used.

9.4.6 HW requirements for the control of systematic faults

9.4.6.1 General

Systematic faults are faults that are related to a cause which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.

9.4.6.2 Control of systematic faults

For controlling systematic faults, the FS-PLC design shall possess design features that make the FS-PLC safety-related systems tolerant against:

- any residual design faults in the hardware, unless the possibility of hardware design faults can be excluded (see Table A.15 of IEC 61508-2:2010);
- environmental stresses, including electromagnetic disturbances (see Table A.16 of IEC 61508-2:2010);
- mistakes made by the operator of the EUC (see Table A.17 of IEC 61508-2:2010);
- any residual design faults in the software;
- errors and other effects arising from any data communication process (see 8.3).

9.4.6.3 Maintainability and testability

Maintainability and testability shall be considered during the design and development activities in order to facilitate implementation of these properties in the final safety-related systems incorporating the FS-PLC.

9.4.6.4 Human interfaces

The design of the FS-PLC shall take into account human capabilities and limitations and be suitable for the actions assigned to operators and maintenance staff. The design of all

interfaces shall follow good human-factor practice and shall accommodate the likely level of training or awareness of operators, for example in mass production applications where the operator has limited training.

NOTE The design goal is that foreseeable critical mistakes made by operators or maintenance staff are prevented or eliminated by design wherever possible, or that the secondary confirmation exists before completion.

9.4.7 HW classification of faults

Faults lead to failures. The goal is to detect and alarm faults before they might result in a failure with dangerous effect. A key concept is to detect a fault before multiple faults occur, as multiple fault scenarios can become impossible to analyze.

Unless explicitly identified, multiple fault scenarios are not considered in fault analysis, e.g. Fault Tree Analysis (FTA), Failure Modes Effects Analysis (FMEA).

In general there are five different types of failures which shall be considered for the analysis of an FS-PLC. The classification of these five failures is dependent on the safety function of the FS-PLC and its architecture.

The first fault type (no effect fault) has no effect on the safety function of the FS-PLC (example; annunciation indicator). It shall not be included in any PFD and PFH, etc, calculations, and shall not contribute to the SFF.

If a failure does not affect the FS-PLC safety function it is classified as a “no effect failure”. A “no effect failure” does not contribute to the safe failure fraction (SFF) calculation.

The remaining four fault types are considered with regard to the safety function of the FS-PLC. These shall be included in PFD and PFH, etc, calculations.

The purpose of Figure 9 is to help or guide the designer of the FS-PLC to properly categorize faults for failure analysis, e.g. FMEA, FTA.

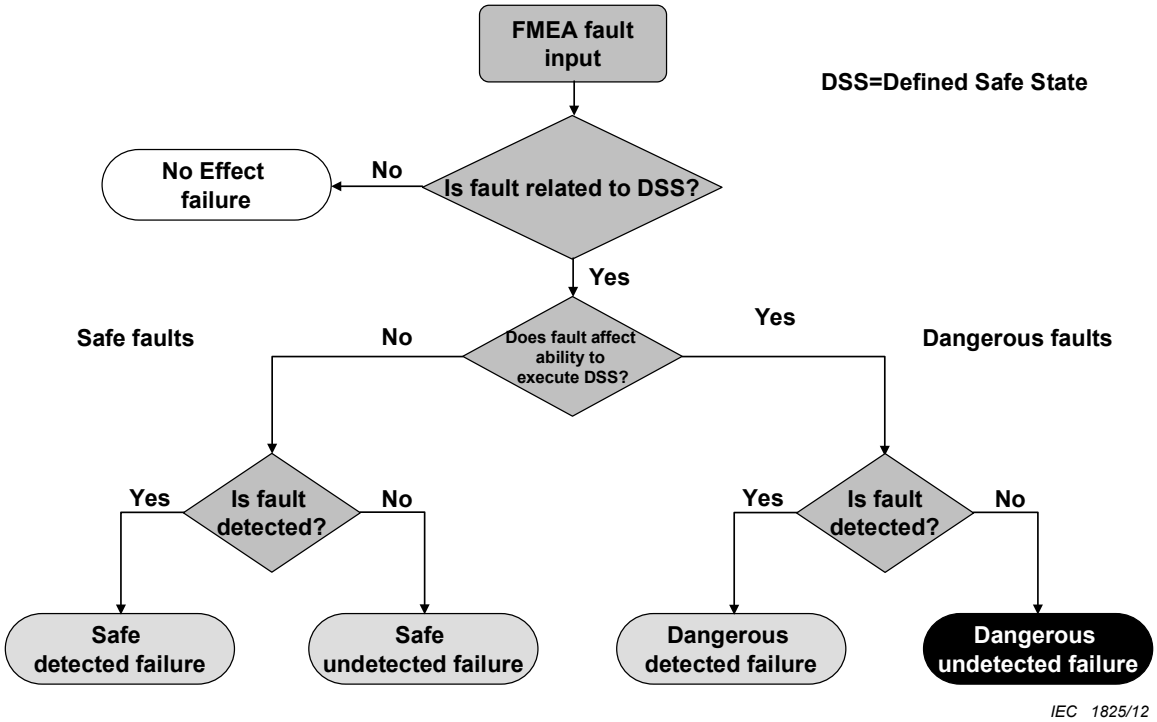


Figure 9 – Fault classification and FS-PLC behaviour

Diagnostic means are assumed to be available to detect and to react to dangerous and/or safe fault(s).

If a failure unintentionally executes the FS-PLC safety function it is a safe undetected failure. On the other hand if the failure does not unintentionally execute the FS-PLC safety function but is detected by diagnostic measures it is assumed that the diagnostic leads to adequate reaction of the system in accordance with 7.4.8 of IEC 61508-2:2010 or that the failure will be repaired (safe detected failure). In case of high demand operation mode the diagnosed failure shall lead to automatic execution of the FS-PLC safety function or to a safe state. In case of low demand mode a notice to the operator is sufficient to enable repair of the system.

If the system does not unintentionally execute the FS-PLC safety function or does not reach a safe state the failure is classified as a dangerous undetected failure. Also a dangerous failure could be diagnosed (dangerous detected fault). Depending on the operation mode, see 9.4.3.1.3 for specified actions.

9.4.8 HW implementation

The FS-PLC shall be implemented according to the FS-PLC HW design.

During the design and development process, the following information shall be compiled by the FS-PLC manufacturer and shall be available for assessment:

a) a specification of those functions and interfaces which can be used by safety functions, e.g. application constraints, communication limitations;

b) estimates of random hardware failure rates which could cause a dangerous system failure and which are detected by diagnostic tests, see 9.4.4;

c) estimates of random hardware failure rates which could cause a dangerous system failure and which are not detected by diagnostic tests, see 9.4.4;

d) environmental limits to maintain failure rate validity;

e) the mechanical and climatic environment (e.g. vibration, shock, temperature, humidity) for which the FS-PLC is intended;

f) the manufacturer declared maximum useful lifetime of the FS-PLC which shall be 20 years or less unless the FS-PLC manufacturer can justify a longer lifetime by providing evidence, based on calculations, showing that reliability data is valid for the longer lifetime.

NOTE Some individual components within a FS-PLC have known lifetimes of less than 20 years. Typical examples include: batteries, electrolytic capacitors, LEDs, etc. As necessary, the periodic replacement of these components are handled as part of the normal maintenance procedures specified by the FS-PLC manufacturer. The maximum useful lifetime limit of 20 years is intended to cover the bulk of the FS-PLC components without known lifetimes.

g) periodic proof test method and interval (and the basis for the requirement) and/or maintenance requirements;

h) diagnostic coverage internal to the FS-PLC;

i) diagnostic test interval internal to the FS-PLC;

j) Mean Time To Restoration (MTTR) and Mean Repair Time (MRT), if applicable;

k) Safe Failure Fraction (SFF);

l) hardware fault tolerance;

m) application limits recommended to avoid systematic failures;

n) de-ratings applied to the components used (see 9.4.9);

o) SILs that can be claimed for the safety-related systems that the FS-PLC will be suitable for use with;

p) hardware revision of the FS-PLC;

q) documentary evidence that a FS-PLC has been validated (see 9.7).

9.4.9 De-rating of components

The manufacturer is expected to demonstrate good engineering practice and implement de-rating principles, including the de-rating of components.

Components shall be operated at less than the component manufacturer's specified maximums under worst case operating conditions: voltage, current, temperature, timing, etc. In those cases where this is not feasible, verification of the suitability of the selected (or only available) component for the intended application(s) shall be required. The component shall be presumed unsuitable until qualified otherwise.

9.4.10 ASIC design and development

A detailed V-model of the ASIC development lifecycle for the design of ASICs is shown in Figure 10. If another ASIC development lifecycle is used, it shall be specified as part of the management of functional safety activities (see 5.4).

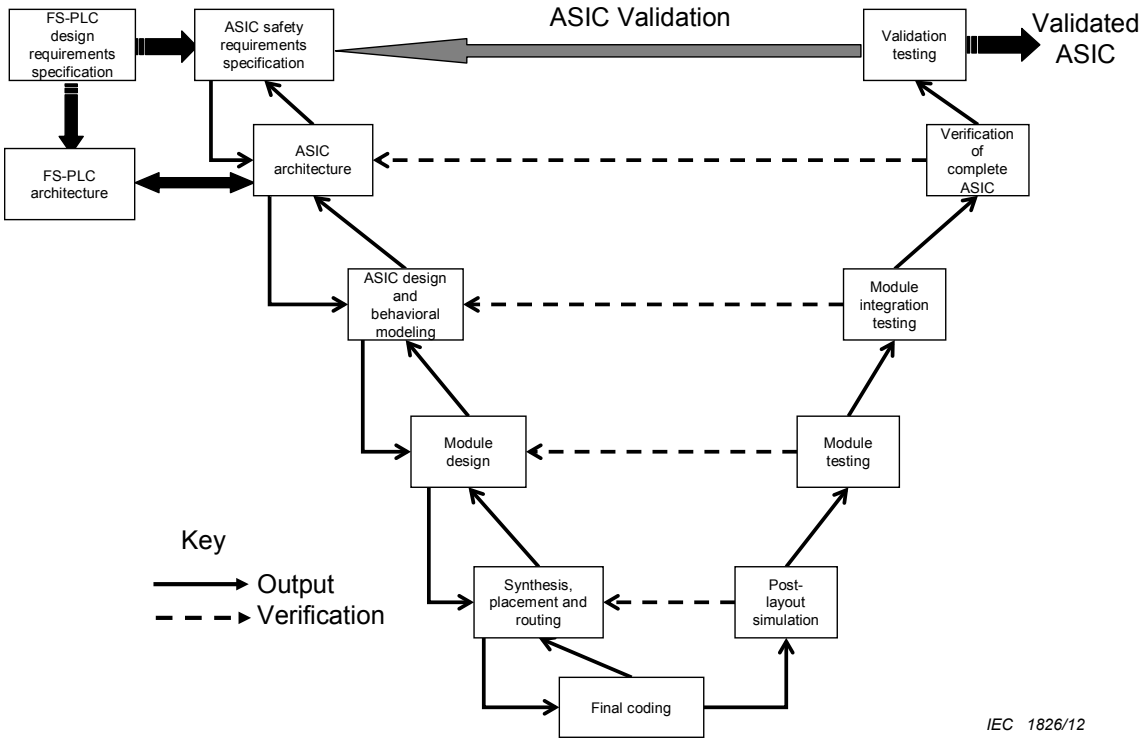


Figure 10 – ASIC development lifecycle (V-Model)

9.4.11 Techniques and measures to prevent the introduction of faults in ASICs

An appropriate group of techniques and measures shall be used that are essential to prevent the introduction of faults during the design and development of ASICs. Depending upon the technical realisation, a differentiation between full and semi-custom digital ASICs and user programmable ICs (FPGA/PLD/CPLD) is necessary. Suitable techniques and measures that support the achievement of relevant properties are defined in IEC 61508-2.

9.5 HW and embedded SW and FS-PLC integration

The integration phase of the safety lifecycle of a FS-PLC consists primarily of functional testing, and either black-box or statistical testing. These tests shall show that all modules, and parts thereof, interact correctly to perform their intended function.

The FS-PLC integration testing shall document the following information:

- the version of the test specification used;
- the criteria for acceptance of the integration tests;
- the version of the FS-PLC being tested;
- the tools and equipment used along with calibration data;
- the results of each test;
- any discrepancy between expected and actual results; and
- the analysis made and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur.

Programmable HW design and development results are integrated with the embedded SW Figure 3, box 19, when their FS-PLC safety function and SIL requirements are satisfied.

After the programmable HW and embedded SW have been integrated, engineering tools and non-programmable HW design and development results are integrated, Figure 3, box 20. During this integration, the FS-PLC safety function and SIL requirements shall be satisfied.

While the sequence is shown as integrating programmable HW before non-programmable HW, this is not a requirement. The test specification shall define the sequence.

9.6 HW operation and maintenance procedures

9.6.1 Objective

The objective of the requirements of 9.6.2 is for the FS-PLC manufacturer to develop procedures to ensure that the required functional safety of the FS-PLC is maintained during operation and maintenance.

9.6.2 Requirements

FS-PLC operation and maintenance procedures shall be prepared which shall specify the following:

a) the routine actions which need to be carried out to maintain the "as-designed" functional safety of the FS-PLC, including routine replacement of components with a pre-defined life, for example cooling fans, batteries, etc.
   - embedded software update and replacement,
   - full or partial application software replacement,
   - HW updates and replacement;

b) the actions and constraints that are necessary (for example, during installation, start-up, normal operation, routine testing, foreseeable disturbances, faults or failures, and shutdown) to prevent an unsafe state and/or reduce the consequences of a hazardous event;

c) the procedures and documentation when faults or failures occur in the FS-PLC, including
   - procedures for fault diagnoses and repair,
   - operational mode on failure,
   - LED/Diagnostic indications,
   - Status/Diagnostic registers,
   - procedures for reporting failures,
   - procedures for analysing failures,
   - procedures for revalidation;

d) the procedures and documentation for maintaining the FS-PLC shall be specified in maintenance reporting requirements.

e) the tools necessary for failure analysis, maintenance and revalidation and procedures for maintaining the tools and equipment.

NOTE 1 The FS-PLC operation and maintenance procedures include the software modification procedures (see Clause 15).

The FS-PLC manufacturer shall upgrade, as necessary, the operation and maintenance procedures based on inputs such as (1) the results of functional safety audits performed by FS-PLC users, (2) tests on the FS-PLC, and (3) field reports.

The routine maintenance actions required to maintain the functional safety (as designed) of the FS-PLC shall be determined by a systematic method, for example by:

- examination of fault trees,
- failure mode and effect analysis.

NOTE 2 A consideration of human factors is a key part in determining the actions required and the appropriate interface(s) with the FS-PLC.

NOTE 3 Proof tests are carried out with a frequency necessary to achieve the target failure measure.

NOTE 4 The frequency of the proof tests, the diagnostic test interval and the time for subsequent repair are dependent upon several factors (see Annex B of IEC 61508-6:2010), including;

the target failure measure associated with the safety integrity level,

the architecture,

the diagnostic coverage of the diagnostic tests, and

the expected demand rate.

NOTE 5 The frequency of the proof tests and the diagnostic test interval are likely to have a crucial bearing on the achievement of hardware safety integrity. One of the principal reasons for carrying out hardware reliability analysis (see 9.4.3.2.2) is to ensure that the frequencies of the two types of tests are appropriate for the target hardware safety integrity.

The FS-PLC operation and maintenance procedures shall be assessed for the impact they may have on the EUC.

For the avoidance of faults and failures during the FS-PLC operation and maintenance procedures, an appropriate group of techniques and measures according to Table B.4 of IEC 61508-2:2010 shall be used.

9.7 HW safety validation

9.7.1 General

The outcome of the validation phase shall include: specific references to the validation plan (9.3), specific requirements of the FS-PLC, test equipment used during the validation, test equipment calibration data, and results for each test.

This phase of the lifecycle is actually performed during several other phases of the lifecycle. For example, during design and development, outputs must be tested to ensure their correctness and consistency with inputs, and it must be demonstrated that the specific faults and failures addressed in subclause 9.4.4.3 are detected.

The objective of the requirements of this phase is to validate that the FS-PLC meets, in all respects, the requirements for functional safety in terms of the required safety functions and the safety integrity (see 9.1).

9.7.2 Requirements

The validation of the FS-PLC shall be carried out in accordance with a prepared safety validation plan (see 9.3).

NOTE 1 Validation of a FS-PLC programmable electronic safety-related system comprises validation of both hardware and software. The requirements for validation of software are contained in Clause 10.

All test measurement equipment used for validation shall be calibrated against a standard traceable to a national standard, if available, or to a well-recognised procedure. All test equipment shall be verified for correct operation.

Each safety function specified in the requirements for FS-PLC (see Clause 6), and all the FS-PLC operation and maintenance procedures shall be validated by test and/or analysis.

Appropriate documentation of the FS-PLC safety validation testing shall be produced and shall state for each safety function

a) the version of the FS-PLC safety validation plan being used;
b) the safety function under test (or analysis), along with the specific reference to the requirement specified during FS-PLC safety validation planning;
c) tools and equipment used, along with calibration data;
d) the results of each test;
e) discrepancies between expected and actual results.

NOTE 2 Separate documentation is not needed for each safety function, but the information in a) to e) apply to every safety function. Where information differs for different safety functions, the differences are stated.

When discrepancies occur (i.e. the actual results deviate from the expected results by more than the stated tolerances), the results of the FS-PLC safety validation testing shall be documented, including

1) the analysis made; and
2) the decision taken on whether to continue the test or issue a change request and return to an earlier part of the validation test.

The FS-PLC manufacturer shall make available results of the FS-PLC safety validation testing to the developer of the EUC or E/E/PE safety-related system only as necessary to enable them to meet the requirements for overall safety validation in IEC 61508-1.

For the avoidance of faults during the FS-PLC safety validation, an appropriate group of techniques and measures (see according to IEC 61508-2) shall be used.

9.8 HW verification

9.8.1 Objective

The objective of 9.8.1 is to confirm that the required activities of each phase are carried out and the results are recorded.

NOTE For convenience all HW verification activities have been drawn together under 9.8, but they are actually performed across several phases.

9.8.2 Requirements

Verification of the deliverables of each FS-PLC hardware related lifecycle phase shall be planned, carried out and documented. These verifications shall be based on the specified inputs to the lifecycle phase. The techniques/tools used in the verification include, for example:

- reviews of the phase’s documentation,
- design reviews,
- functional tests and
- environmental tests.

NOTE Verification is not to be confused with calibration or validation.

10 FS-PLC SW design and development

10.1 General

The requirements of Clause 10 are derived from the software specific requirements contained in the FS-PLC functional safety requirements specification.

Clause 10 applies to the FS-PLC embedded SW and engineering tools and application development software tools, but excludes user application software.

Figure 11 shows the basic reference software model used in this part. The reference model is one example of the implementation of functional safety software, other architectures are possible.

The engineering tools typically include FS application code generator and human machine interface to edit the FS application source code and to monitor the FS-PLC status. An analysis of the safety relevant impact of the engineering tools shall be executed.

The FS-PLC embedded SW receives the FS application code through the FS application code transfer layer and stores them in the FS application storage layer.

The FS application code execution layer loads the FS application code from the FS application storage layer and executes it.

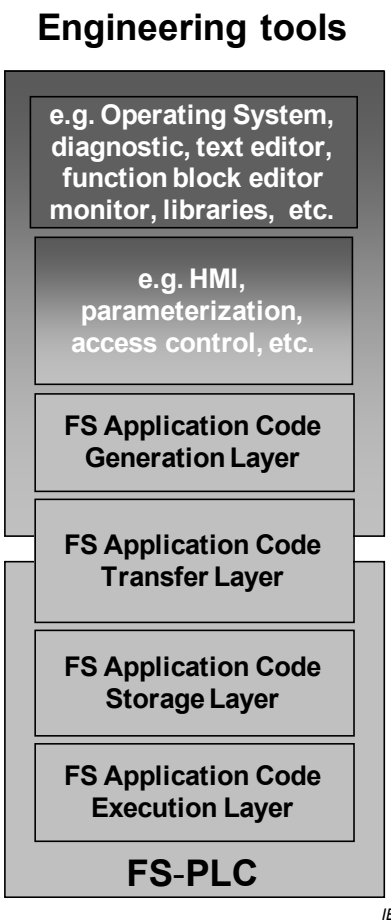


Figure 11 – Model of FS-PLC and engineering tools layers

The FS-PLC SW requirements derived from the software specific requirements contained in the FS-PLC functional safety requirements specification will in most cases be achieved by a combination of embedded SW and engineering tools. It is the combination of both that is required to provide the features that satisfy the following subclauses. The exact division between embedded SW and engineering tools depends on the chosen system architecture.

10.2 Requirements

All of the requirements of IEC 61508-3 apply to FS-PLC SW and online support tools. These are software tools that can directly influence the safety-related system during its run time.

10.3 Classification of engineering tools

The FS-PLC Engineering tools shall be divided into the following classes:

- T1: generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system;
- T2: supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software;
- T3: generates outputs which can directly or indirectly contribute to the executable code of the safety related system.

NOTE 1 T1 examples include: A text editor or a requirements or design support tool with no automatic code generation capabilities; configuration control tools.

NOTE 2 T2 examples include: A test harness generator; a test coverage measurement tool; a static analysis tool.

NOTE 3 T3 examples include: An optimizing compiler where the relationship between the source code program and the generated object code is not obvious; a compiler that incorporates an executable run-time package into the executable code.

NOTE 4 This classification is based on IEC 61508-4:2010, 3.2.11.

Examples of dividing the FS-PLC Engineering Tools into classes are provided in Table 7. The exact division between embedded SW and engineering tools depends on the chosen system architecture.

Table 7 – Examples of tool classification

Class of tools[a]	Class	Reasoning
Engineering Tools – PC OS, diagnostic, text editor, function block editor, monitor, libraries, etc	T1	The output of the tool(s) is verified and validated by the user prior to use in a FS-PLC
Engineering Tools – HMI, parameterization, access control, etc.	T1	Generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system
Engineering Tools – FS application code generation layer, HMI, parameterization	T3	Generates outputs which can directly or indirectly contribute to the executable code of the FS-PLC
Engineering Tools – FS application code transfer layer	T3	May directly or indirectly contribute to the executable code of the safety related system
FS-PLC – application code storage layer	n/a	Embedded system firmware
FS-PLC – application code execution layer	n/a	Embedded system firmware
[a] Tools may have different classifications depending on their output or code generation capability.		

Once this classification has been determined, the applicable requirements of IEC 61508-3 shall be followed.

10.4 SW safety validation planning

NOTE 1 This phase of the lifecycle of a FS-PLC is normally carried out in parallel with the SW design and development requirements, see 10.2.

NOTE 2 See 7.3.2.2 of IEC 61508-3:2010.

Software validation planning is accomplished by specifying the steps that are to be used to demonstrate compliance to the FS-PLC SW functional safety requirements specification (see Clause 6).

The functional safety validation plan shall include the procedures to be followed, a description of the test environment and pass/fail criteria.

11 FS-PLC safety validation

The objective of Clause 11 is to ensure that the FS-PLC system meets, in all respects, the requirements for functional safety in terms of the required safety functions and safety integrity defined in Clause 6.

The manufacturer shall develop and execute a validation plan from the information defined in Clauses 6 and 12.

A validation report shall be developed and retained by the FS-PLC manufacturer. This report shall include Type Test reports. These type test reports shall cover the minimum FS-PLC system level tests specified in Clauses 12 through 13.2.

The FS-PLC manufacturer shall have the FS-PLC subjected to a safety assessment performed by an independent organization/department for SIL 3 development as defined in Clause 14, (see Table 5 of IEC 61508-1:2010).

12 FS-PLC type tests

12.1 General

Type tests of the FS-PLC system shall be performed to ensure that the FS-PLC system operates as specified while in the environments for which it is intended.

The type tests shall cover the minimum FS-PLC system level tests specified in 12.2 through 12.5 and shall follow the FS-PLC Validation Plan discussed in 9.3.

A type test report shall be written and retained by the FS-PLC manufacturer.

12.2 Type test requirements

As part of each FS-PLC system test effort, a Proper Functioning Verification Procedure (PFVP) and a PFVP test program shall be provided. To the maximum extent possible, the PFVP shall be fully automated and integrated as part of the PFVP test program, external instrumentation and manual test steps shall be minimized as part of the PFVP. Unless otherwise noted, these requirements must be verified during type testing: climatic, mechanical, EMC, fault tolerance, etc.

The PFVP test program and PFVP shall be used to verify:

a) proper setup of the FS-PLC equipment under test (EUT);

b) proper operation of the FS-PLC EUT before, during, and after type testing, as specified in Table 8;

c) during testing, unless stated otherwise (refer to Table 8, performance criteria FS) there shall be no:

   i) destruction of hardware,

   ii) unintended modification of the operating system and test programs and/or alteration of their execution,

   iii) unintended modification of system and application data stored or exchanged,

   iv) erratic or unintended behavior of the FS-PLC EUT. For example:

      1) deviation of the analog I/O point accuracy out of specified limits,

      2) deviation of communication response times and minimum error rates, out of specified limits,

      3) deviation of system scan and response times beyond worst case calculated limits,

      4) deviation of control program timers, out of specified limits,

      5) failure to complete a scan,

      6) loss of correct time of day,

d) all various system operational modes significant for a typical FS-PLC implementation such as start-up and shut-down, cold/warm/hot restart, "normal run", "normal stop", "program/monitor via external HMI", etc.

e) initialization and reset conditions of all system components during controlled start-up and shut-down.

Keep in mind instrumentation limitations which prevent the real-time verification of some or all of these items during type testing. For example, when trying to verify the published accuracy limits when analog outputs are looped back to exercise analog inputs. In these cases, system verification test limits are set as tight as possible. Other examples include, operating modes, initialization and reset conditions, etc.

The PFVP shall, where applicable, exercise the FS-PLC EUT in such a manner that:

a) all relevant functions and parts of the FS-PLC EUT shall be functioning in such a way that the information paths to/from each type of module/function shall be exercised and monitored for correct behavior;

b) a necessary and sufficient subset of the I/O and communication channels and their features, specified by the manufacturer, shall be exercised and monitored for correct behavior. (See 2.2 of IEC 61131-2:2007);

c) all relevant external and internal system status information reporting means such as LED displays, alarm signals, system alarms shall be exercised and monitored for correct behavior;

   NOTE Instrumentation limitations sometimes prevent the real-time verification of some system functions, for example, front panel indicators, during increased level testing.

d) the PFVP test program/PFVP shall exercise the FS-PLC EUT in such a manner to reflect, as far as possible, worst case response time conditions: rapidly changing inputs and outputs, continuous external communications, continuous peer-to-peer communications, etc. Measurement of the response time, where applicable, shall take into account the following system activities, that may take longer to execute:

   i) conditional Print statements,

   ii) conditional floating point calculations or array manipulations,

   iii) burst of events, multiple simultaneously changing I/O points,

   iv) burst of communication messages from external sources,

v) remote monitoring of I/O points during a burst of events resulting in a corresponding burst of internally generated messages,

vi) loss of a communication link from opens, shorts, or EMI resulting in internal time-outs or fault responses,

vii) behavior during the application or in the presence of a single random hardware fault resulting in internal time-outs or fault responses;

e) during type testing, the FS-PLC EUT shall be exercised with power supply sources at the levels specified in IEC 61131-2 (voltage, frequency, etc).

During type testing, the PFVP shall be able to verify proper performance against the following criteria while subjected to the various conditions/restraints required herein.

Table 8 – Performance criteria

Performance criteria	Operation during the test	Operation after the test
A	The FS-PLC system shall continue to operate as intended. No degradation or loss of function or performance.	The FS-PLC system shall continue to operate as intended.
B	The FS-PLC performance is allowed to degrade in the following ways: 1) analog values may not vary more than ± the manufacturer specified % of full scale, 2) spurious FS-PLC system alarms where no change of state has occurred: e.g. from redundant to non-redundant. 3) an intentional change of state The following are not allowed: • unintentional loss of control or change of operating mode: e.g., loss of data, loss of communication, digital I/O state changes, redundant to non-redundant. • irreversible loss of stored data. • change in worst case FS-PLC system response times (see NOTE 1).	The FS-PLC system shall continue to operate as intended. Temporary degradation of performance must be self-recoverable.
C	Loss of function of the FS-PLC is allowed but without destruction of hardware or software (program or data).	The FS-PLC system shall continue to operate as intended automatically, after manual restart or power OFF/power ON cycling.
FS	Functions of the FS-PLC EUT intended for safety application: 1) Same as Performance Criteria A, or 2) May be disturbed temporarily or permanently if the EUT reacts to a disturbance in a way that is detectable and the EUT maintains or achieves (in a stated time) a defined state or states of the FS-PLC. Functions not intended for safety applications may be disturbed temporarily or permanently	Destruction of safety related components is allowed if the defined state of the FS-PLC EUT is maintained or achieved within a stated time. Destruction of non-safety related components is allowed.
NOTE 1 FS-PLC system response times include the maximum duration from a step change on any FS-PLC system input point to a step change of any FS-PLC system output point, and a step change on any FS-PLC system input point to a step change on any output point of another FS-PLC system via a peer-to-peer link. NOTE 2 Source: modified 6.2 of IEC 61326-3-1:2008 and 8.3.2 of IEC 61131-2:2007.		

12.3 Climatic test requirements

For climatic test requirements, see IEC 61131-2.

Before and after each environmental withstand test, the FS-PLC EUT shall be verified for proper operation via the PFVP. In addition, during each immunity type test, the FS-PLC EUT shall be verified for proper operation via the PFVP.

Special tests for conditions more severe than 61131-2 shall be agreed to by the manufacturer and the user.

12.4 Mechanical test requirements

For mechanical test requirements, see IEC 61131-2.

Before and after each mechanical withstand test, the FS-PLC EUT shall be verified for proper operation via the PFVP. In addition, during each immunity type test, the FS-PLC EUT shall be verified for proper operation via the PFVP.

Special tests for conditions more severe than 61131-2 shall be agreed to by the manufacturer and the user.

12.5 EMC test requirements

12.5.1 General

IEC/TS 61000-1-2 shall be consulted for a methodology for the achievement of functional safety with regards to electromagnetic phenomena. However, since actual electromagnetic test levels are not contained therein, the test requirements of 12.5.2 or 12.5.3 shall be used.

These requirements do not apply to the non-safety-related functions of the equipment or systems.

Before, during, and after each EMC immunity test, the FS-PLC system under test shall be verified for proper operation via the PFVP as specified by the performance criteria and Table 8. The emissions test requirements for an FS-PLC are identical to those specified in IEC 61131-2. During each emission test, the FS-PLC system under test shall be exercised to simulate a typical system environment. This can be accomplished by using the automated portions of the PFVP to exercise the system.

12.5.2 General EMC environment

This subclause 12.5.2 specifies the EMC immunity requirements for a FS-PLC intended for use in a general EMC environment, i.e. an environment without restrictions or controls related to EMC phenomena.

Increased immunity test levels in Table 9 and Table 10 are related to functional safety aspects only. They are not applicable for the assessment of reliability and availability aspects. The increased immunity test levels apply only to the safety-related functions having a specific performance criterion for functional safety (performance criterion FS). The increased immunity test levels are the maximum test values. Further tests with higher values are not required for compliance with this standard.

Table 9 and Table 10 contain all of the EMC immunity requirements of IEC 61131-2.

Table 9 – Immunity test levels for enclosure port tests in general EMC environment

Environmental phenomenon	Basic standard	Test	Test level	Performance criteria
Electrostatic discharge	IEC 61000-4-2	Contact	±6 kV [a]	FS
		Air	±8 kV [a]	
Radio-frequency Electro-magnetic field Amplitude modulated	IEC 61000-4-3	2,0 GHz - 2,7 GHz	3 V/m[b]	FS
		1,4 GHz - 2,0 GHz	10 V/m	
		80 GHz - 1,0 GHz	20 V/m[b]	
Power frequency magnetic fields	IEC 61000-4-8	50 Hz/60 Hz	30 A/m[c] No increased test level applies.	FS

a Levels shall be applied in accordance with the environmental conditions described in IEC 61000-4-2 on parts which may be accessible by persons other than staff working in accordance with defined procedures for the control of ESD but not to equipment where access is limited to appropriately trained personnel only.

b These values – increased over IEC 61131-2 values – shall be applied in frequency ranges used for mobile transmitters in general, except when reliable measures are realised to avoid the use of such equipment nearby. ISM frequencies shall be taken into account on an individual basis.

c Applicable only to equipment containing devices susceptible to magnetic fields.

Table 10 – Immunity test levels in general EMC environment

	Environmental phenomenon	Fast transient burst	High energy surge (NOTE)	Radiofrequency interference	
	Basic standard	IEC 61000-4-4	IEC 61000-4-5	IEC 61000-4-6	
	Performance criteria	FS	FS	FS	
Interface/port (designation)	**Specific interface/port**	**Test level**	**Test level[f]**	**Test level**	**Values derived from**
Equipment power (F) and I/O power (J) and auxiliary power output (K)	a.c. power	3 kV[a] (5/50 ns, 5 kHz)	4 kV CM 2 kV DM	10 V[b] 15 kHz to 80 MHz	IEC 61326-3-1:2008 Table 1b
	d.c. power[e]	3 kV[a] (5/50 ns, 5 kHz)	2 kV CM[,c] 1 kV DM	10 V[b] 15 kHz to 80 MHz	IEC 61326-3-1:2008 Table 1c
I/Os (C and D)	General I/O	2 kV[a,d] (5/50 ns, 5 kHz)	2 kV CM	10 V[b] 15 kHz to 80 MHz	IEC 61326-3-1:2008 Table 1d
	I/O connected direct to power supply networks	3 kV[a] (5/50 ns, 5 kHz)	4 kV CM 2 kV DM	10 V[b] 15 kHz to 80 MHz	IEC 61326-3-1:2008 Table 1e
Functional Earthing (H)	-	2 kV[a] (5/50 ns, 5 kHz)	No Test	3 V	IEC 61326-3-1:2008 Table 1f

The required immunity level can be achieved through the use of external protection devices.

a For equipment intended to be used in SIL 3 applications, the duration of the test at the highest level shall be increased by a factor of 5 compared to the duration as given in the basic standard.
b The values – increased over IEC 61131-2 values – shall be applied in frequency ranges used for mobile transmitters in general, except when reliable measures are realised to avoid the use of such equipment nearby. ISM frequencies have to be taken into account on an individual basis.
c Only in the case of lines within a building which are longer than 30 m, or which leave the building (including lines of outdoor installations).
d Only in case of lines >3 m.
e DC connections between parts of equipment/system which are not connected to a d.c. distribution network are treated as I/O signal/control ports.
f DM = differential mode, CM = common mode

12.5.3 Specified EMC environment

Subclause 12.5.3 specifies the EMC immunity requirements for a FS-PLC intended for use in the EMC environment specified by the FS-PLC manufacturer.

The EMC immunity requirements specified in Table 11 and Table 12 include the requirements of IEC 61131-2.

The environment of industrial application with a specified electromagnetic environment typically includes the following characteristics:

- industrial area with limited access;
- limited use of mobile transmitter;
- dedicated cables for power supply and control, signal or communication lines;
- separation between power supply and control, signal or communication cables;
- factory building mostly consisting of metal construction;

- overvoltage/lightning protection by appropriate measures (for example, metal construction of the building or use of protection devices);
- pipe heating systems driven by a.c. main power may be present;
- no high-voltage substation close to sensitive areas;
- presence of CISPR 11 Group 2 ISM equipment using ISM frequencies only with low power;
- competent staff;
- periodic maintenance of equipment and systems;
- mounting and installation guidelines for equipment and systems.

A more detailed description of the above-mentioned typical characteristics is given in Annex B of IEC 61326-3-2:2008.

Table 11 – Immunity test levels for enclosure port tests in specified EMC environment

Environmental phenomenon	Basic standard	Test	Test level	Performance criteria
Electrostatic discharge	IEC 61000-4-2	Contact	±6 kV [a]	A
		Air	±8 kV [a]	
Radio-frequency Electro-magnetic field Amplitude modulated	IEC 61000-4-3	2,0 GHz - 2,7 GHz	3 V/m	A
		1,4 GHz - 2,0 GHz	10 V/m	
		80 MHz -1,0 GHz	10 V/m[b]	
Power frequency magnetic fields	IEC 61000-4-8	50 Hz /60 Hz	100 A/m[c]	A

a Levels shall be chosen in accordance with the environmental conditions described in Annex A of IEC 61000-4-2:2008 and applied on parts which may be accessible by persons other than staff working in accordance with defined procedures for the control of ESD but not to equipment where access is limited to appropriately trained personnel only.

b Except for the ITU broadcast frequency bands 87 MHz to 108 MHz, 174 MHz to 230 MHz, and 470 MHz to 790 MHz, where the level shall be 3 V/m.

c Applicable only to equipment containing devices susceptible to magnetic fields.

Table 12 – Immunity test levels in specified EMC environment

	Environmental phenomenon	Fast transient burst	High energy surge (NOTE)	Radiofrequency interference	
	Basic standard	IEC 61000-4-4	IEC 61000-4-5	IEC 61000-4-6	
	Performance criteria	A	A	A	
Interface/Port (designation)	**Specific interface/port**	**Test level**	**Test level[f]**	**Test level**	**Values derived from**
Equipment power (F) and I/O power (J) and auxiliary power output (K)	a.c. power	2 kV (5/50 ns, 5 kHz)	2 kV CM 1 kV DM	10 V[a] 10 kHz to 80 MHz	IEC 61326-3-2:2008 Table 1b
	d.c. power[e]	2 kV (5/50 ns, 5 kHz)	1 kV CM 0,5 kV DM	10 V[a] 10 kHz to 80 MHz	IEC 61326-3-2:2008 Table 1c
I/O signal/control (C and D)	General I/O	1 kV[b] (5/50 ns, 5 kHz)	1 kV CM[c] (NOTE)	10 V[b, d] 10 kHz to 80 MHz	IEC 61326-3-2:2008 Table 1d
	I/O connected direct to power supply networks	2 kV (5/50 ns, 5 kHz)	2 kV CM 1 kV DM	10 V[d] 10 kHz to 80 MHz	IEC 61326-3-2:2008 Table 1e
Functional Earthing (H)	-	2 kV[b] (5/50 ns, 5 kHz)	1 kV CM[c] (NOTE)	10 V[d] 10 kHz to 80 MHz	IEC 61326-3-2:2008 Table 1f

NOTE The performance criteria FS is allowed.

a In the frequency range 10 kHz up to 150 kHz the impedance of the CDN has to comply with the asymmetric impedance requirements of IEC 61000-4-6 at 150 kHz. Calibration shall be performed in accordance with IEC 61000-4-6. Sufficient decoupling can be demonstrated if the impedance criterion is met both with the AE port short-circuited

b Only in case of lines >3 m.

c Only in the case of lines within a building which are longer than 30 m, or which leave the building (including lines of outdoor installations)

d In the frequency range 10 kHz up to 150 kHz the impedance of the CDN has to comply with the asymmetric impedance requirements of IEC 61000-4-6 at 150 kHz. Calibration is to be performed in accordance with IEC 61000-4-6. Sufficient decoupling can be demonstrated if the impedance criterion is met both with the AE port short-circuited and then open-circuited.

e DC connections between parts of equipment/system which are not connected to a d.c. distribution network are treated as I/O signal/control ports.

f DM = differential mode, CM = common mode

13 FS-PLC verification

13.1 Verification plan

The FS-PLC verification plan shall be executed and shall contain at least the following items:

- review of requirement specification;
- review of design processes;
- review of HW design (example: circuit diagram, bill of material (BOM));
- review of embedded SW design;
- review of engineering tools suitability, only for FS relevant portions. See Figure 5;
- review of test specification (module test, integration test);
- review of test-specification of system test and type test;
- failure modes effects analysis (FMEA);

- review of test results (example: module test, integration test, system test and type test);
- HW failure test, e.g. simulation, physical;
- criticality analysis;
- embedded SW failure test, e.g. simulation;
- review method of calculation of reliability data (example: common cause analysis, Markov modelling, Markov calculation).

Reviews shall be independent and documented.

13.2 Fault insertion test requirements

A fault insertion test is the deliberate insertion of a fault to determine its effect on the operation of the FS-PLC.

Fault insertion tests shall be carried out as part of verification testing with the following objectives:

- to verify that the failure effects predicted in the hardware FMEA are correct, and hence that their failure rates are included in the correct fault classification (see 9.4.7);
- to verify that run time diagnostic tests react as intended in the design;
- to verify that the fault reaction of the FS-PLC is as intended in the design;
- to verify that permitted on-line maintenance processes, for example exchange of a module, operate as intended in the design.

Fault insertion tests may be performed at a component level or at a higher level on an element or on a sub-system.

Examples of fault insertion tests at component level are:

– open circuiting a component;
– short circuiting a component;
– causing a digital IC output to stick in the wrong state.

Examples of fault insertion tests at element or sub-system level are:

a) removing or inserting a module during run-time;
b) simulating voltage rail over- or under-voltage;
c) corruption of data transferred between elements or sub-systems.

Table 13 shows the required effectiveness of the fault insertion tests, depending on the target SIL and the required diagnostic coverage.

For low effectiveness, tests shall be applied at least at element or sub-system level, including data connections between units.

For medium and high effectiveness, tests shall also be applied at component level, with sufficient rigor to verify the claimed diagnostic coverage. Tests shall be applied

- where the failure effect predicted by FMEA is not clear by inspection;
- where the failure rate of the failure effect is significant;
- where run time diagnostic tests are intended to detect the fault.

NOTE The required rigor of the fault insertion tests depends on the diagnostic coverage claimed, the effectiveness of the FMEA, the architecture of the FS-PLC, etc.

The PFVP shall be used to verify the correct operation of the FS-PLC

- before performing a fault insertion test;
- during a fault insertion test, if the intended reaction is to continue normal operation;
- after restitution following a fault insertion test.

Before, during, and after each fault insertion test, the FS-PLC EUT shall be verified for proper operation using the PFVP.

Table 13 – Fault tolerance test, required effectiveness

Required effectiveness of fault insertion testing			
Required diagnostic coverage	SIL1	SIL2	SIL3
<90 %	Low	Low	Medium
≥90 %	High	High	High

The method of applying fault insertion tests, the specific tests to be applied, and the required outcome of each test shall be stated in the verification test plan. The quantity and rigor of fault insertion tests shall be agreed by the FS-PLC manufacturer and the assessor taking into account the complexity of the FS-PLC, its intended application and its safety integrity level.

After product release, it may be necessary to repeat some fault insertion tests to verify a product modification, or enhancement. The scope of the required re-test shall be determined as part of the change impact analysis.

13.3 As qualified versus as shipped

The manufacturer shall take measures to ensure that all products shipped to a customer perform equal or better than the units used during type testing.

NOTE The following list contains example techniques that can be used:

a) using conservative margins during type testing, for example:

   1) operating temperature: 10 °C beyond upper and lower published specifications,

   2) operating humidity: 30 % above high operating limit or 95 % RH, whichever is greater,

   3) operating vibration: 30 % above the published “g” limit,

   4) EMC (immunity): 50 % beyond the published limit;

b) using additional tests during type testing: highly accelerated life testing (HALT), etc;

c) testing with additional units during type testing;

d) 100 % testing of all shipped units, or determine via analysis the critical characteristics of the system and 100 % test of these;

e) using additional tests during manufacturing: highly accelerated increased level testing (HAST), etc;

f) additional quality assurance checks, assessments, analysis, etc;

g) forbid any changes to the design, components or materials from those in the type tested product.

h) perform formal change impact analysis

14 Functional safety assessment

14.1 Objective

The objective of the requirements of 14.1 is to specify the activities necessary to investigate and arrive at a judgement on the adequacy of the functional safety achieved by the FS-PLC

and the compliance to the relevant subclauses of this standard achieved by the FS-PLC, and to determine if compliance to the relevant subclauses of this part has been achieved.

A functional safety assessment of the FS-PLC shall be carried out, to provide assurance that the necessary level of safety has been achieved. Its results shall be presented in a safety assessment report. The report shall explain the activities carried out by the safety assessor to determine how the FS-PLC system/subsystem/equipment, (hardware and software) has been designed to meet its specified requirements, and possibly specify some additional conditions for the operation of the system/subsystem/equipment.

The assessor/assessment team shall be at least independent from the development team of the FS-PLC.

14.2 Assessment requirements

14.2.1 Assessment evidence and documentation

The assessment shall provide evidence that all necessary verification and validation steps are carried out to provide evidence that the:

a) measures to avoid failures (functional safety management [FSM] activities) are suitable for the required SIL,

b) the measures to control failures of hard- and software are suitable for the required SIL.

The functional safety assessment shall be based on the evaluation of following documentation:

- the FS-PLC system (or subsystem/equipment) requirements specification;
- definition of system/subsystem/equipment;
- V&V (verification and validation) plan;
- the safety plan;
- functional safety management report in accordance with IEC 61508-1 and this standard (evidence of safety management);
- report of technical measures in accordance with IEC 61508-2 and IEC 61508-3 and this standard; test plan(s) and report(s);
- the compliance to environmental and EMC requirements;
- compliance to the requirements of IEC 61131-2.

14.2.2 Assessment method

1) One or more persons shall be appointed to carry out one or more functional safety assessments in order to arrive at a judgement on the adequacy of:
   a) the functional safety achieved by the FS-PLC, within their particular environment, in respect to the relevant subclauses of this standard;
   b) the compliance to the relevant subclauses of this standard, achieved in the case of elements/subsystems.
2) Those carrying out a functional safety assessment shall have access to all persons involved in any FS-PLC safety lifecycle activities and all relevant information and equipment (both hardware and software).
3) A functional safety assessment shall be applied to all phases throughout the overall lifecycle, including documentation, verification and management of functional safety.
4) Those carrying out a functional safety assessment shall consider the activities carried out and the outputs obtained during each phase of the overall safety lifecycle and judge whether adequate functional safety has been achieved based on the objectives and requirements in this standard.

5) The competency of the assessor/assessment team must be relevant for FS-PLC hard- and software development and shall be documented.

6) All relevant claims of compliance made by suppliers and other parties responsible for achieving functional safety shall be included in the functional safety assessment.

7) A functional safety assessment may be carried out after each phase of the overall FS-PLC safety lifecycle, or after a number of safety lifecycle phases.

8) A functional safety assessment shall include assessment of the evidence that functional safety audit(s) have been carried out (either full or partial) relevant to its scope.

9) If performed incrementally, each functional safety assessment shall consider at least the following:

   a) the work done since the previous functional safety assessment;

   b) the plans or strategy for implementing further functional safety assessments;

   c) the recommendations of the previous functional safety assessments and the extent to which changes have been made to meet them.

10) Each functional safety assessment shall be planned by the manufacturer. The plan shall specify all information necessary to facilitate an effective assessment, including:

   a) the scope of the functional safety assessment;

   b) the organisations involved;

   c) the resources required;

   d) those to undertake the functional safety assessment and their competency;

   e) the level of independence of those undertaking the functional safety assessment;

   f) the outputs from the functional safety assessment;

   g) how the functional safety assessment relates to, and shall be integrated with, other functional safety assessments;

   h) when during the FS-PLC safety lifecycle the assessment(s) will be performed.

11) Prior to a functional safety assessment taking place, its plan shall be approved by those carrying it out and by those responsible for the management of functional safety.

12) At the conclusion of a functional safety assessment, those carrying out the assessment shall document, in accordance with the assessment's plans and terms of reference:

   a) the activities conducted;

   b) the findings made;

   c) the conclusions arrived at;

   d) a judgement on the adequacy of functional safety in accordance with the requirements of this standard;

   e) recommendations that arise from the assessment, including recommendations for acceptance, qualified acceptance or rejection.

13) The relevant outputs of the functional safety assessment of a compliant item shall be made available to those having responsibilities for any overall FS-PLC lifecycle activities including the designers and assessors of the FS-PLC.

14) The output of the functional safety assessment of a compliant item shall include the following information to facilitate the re-use of the assessment results in the context of a larger system:

   a) the precise identification of the compliant item including the version of its hardware and software;

   b) the conditions assumed during the assessment;

   c) reference to the documentation evidence on which the assessment conclusion was based;

   d) the procedures, methods and tools used for assessing the systematic capability along with the justification of its effectiveness;

e) the procedures, methods and tools used for assessing the hardware safety integrity together with the justification of the approach adopted and the quality of the data;

f) the assessment results obtained in relation to the requirements of this standard and to the specification of the safety characteristics of the compliant item in its safety manual;

15) Those carrying out a functional safety assessment shall be competent for the activities to be undertaken, according to the requirements of 5.4.2.2.2 and 5.4.2.2.3.

14.3 FS-PLC assessment information

The information of Table 14 shall be maintained by the FS-PLC manufacturer.

Table 14 – Functional safety assessment Information

FS-PLC safety lifecycle phase	Information
Concept	Description (FS-PLC concept)
FS-PLC scope definition	Description (FS-PLC scope definition)
FS-PLC functional safety requirements	Specification (FS-PLC functional safety requirements, comprising: FS-PLC safety functions and FS-PLC safety integrity)
Functional safety requirements allocation	Description (functional safety requirements allocation)
FS-PLC operation and maintenance planning	Plan (FS-PLC operation and maintenance)
FS-PLC safety verification and validation planning	Plan (FS-PLC safety verification and validation)
Realisation	Design and Development documentation (see IEC 61508-2 and IEC 61508-3)
FS-PLC safety verification and validation	Report (FS-PLC safety verification and validation)
FS-PLC operation and maintenance	FS-PLC operation and maintenance procedures
FS-PLC modification	Request (FS-PLC modification); Report (FS-PLC modification) and retrofit Log (FS-PLC modification) impact analysis;
Concerning all phases	Plan (safety); Plan (verification); Report (verification); Plan (functional safety assessment); Report (functional safety assessment)

14.4 Independence

The minimum level of independence of those carrying out a functional safety assessment shall be as specified in Table 15. Table 15 shall be interpreted as follows:

- X: the level of independence specified is the minimum for the specified safety integrity level/systematic capability. If a lower level of independence is adopted, then the rationale for using it shall be detailed;
- X1 and X2;
- Y: the level of independence specified is considered insufficient for the specified safety integrity level/ systematic capability.

In the context of Table 15, only cells marked X, X1, X2 or Y shall be used as a basis for determining the level of independence. For cells marked X1 or X2, either X1 or X2 is applicable (not both), depending on a number of factors specific to the FS-PLC design. The rationale for choosing X1 or X2 should be detailed. Factors that will make X2 more appropriate than X1 are:

– lack of previous experience with a similar design;
– greater degree of complexity;
– greater degree of novelty of design;
– greater degree of novelty of technology.

NOTE 1 Depending upon the company organization and expertise within the company, the requirement for independent persons and departments, in some cases, is met by using an external organization. Conversely, companies that have internal organizations skilled in risk assessment and the application of safety-related systems, that are independent of and separate (by ways of management and other resources) from those responsible for the main development, in some cases, use their own resources to meet the requirements for an independent organization.

NOTE 2 See 3.8.11, 3.8.12 and 3.8.13 of IEC 61508-4:2010 for definitions of independent person, independent department, and independent organization respectively.

NOTE 3 Those carrying out a functional safety assessment are careful in offering advice on anything within the scope of the assessment, since this could compromise their independence. It is often appropriate to give advice on aspects that could incur a judgement of inadequate safety, such as a shortfall in evidence, but it is usually inappropriate to offer advice or give recommendations for specific remedies for these or other problems.

In the context of Table 15, the minimum levels of independence shall be based on the highest systematic capability claimed for the FS-PLC, specified in terms of the safety integrity level.

Table 15 – Minimum levels of independence of those carrying out functional safety assessment

Minimum level of independence	Safety integrity level / Systematic capability			
	1	2	3	4
Independent person	X	X1	Y	Y
Independent department		X2	X1	Y
Independent organization			X2	X

15 FS-PLC operation, maintenance and modification procedures

15.1 Objective

The objective of 15.1 is to ensure that the FS-PLC manufacturer provides operation, maintenance and modification procedures for the FS-PLC system that meet, in all respects, the requirements for safety in terms of the required safety functions and safety integrity defined in Clause 6.

The information for these operation, maintenance and modification procedures is specified in Clause 16.

15.2 FS-PLC modification

Manufacturers that claim compliance with this standard shall maintain a system to manage changes, e.g. as a result of the detection of defects, to improve design or manufacturing process or to improve functionalities. This system shall include the documentation of: details of the modification, analyses of its impact (including the need for re-verification and re-validation), approvals for the modification, revalidation/re-verification results, and any associated changes to a product's operation or documentation. For additional details, see 7.16 of IEC 61508-1:2010 and 7.8 of IEC 61508-3:2010.

All FS-PLC modifications shall be analyzed to determine the effect that a change or an enhancement to a FS-PLC system module will have to other modules in that system as well as to other parts of the safety-related system.

This analysis shall be performed prior to a modification or enhancement being performed.

After the analysis has been completed a decision shall be made concerning the need for re-verification of the FS-PLC system. This depends on the number of modules affected, the criticality of the affected modules and the nature of the change. The possible decisions are:

- only the changed module shall be re-verified;
- all affected modules shall be re-verified; or
- the complete FS-PLC system shall be re-verified.

The FS-PLC manufacturer shall retain a history of this analysis and the decision for all changes that affect safety relevant portions of the FS-PLC.

16 Information to be provided by the FS-PLC manufacturer for the user

16.1 General

The manufacturer shall provide users with information required for the application, installation, commissioning, operation and maintenance of the FS-PLC. In addition, the manufacturer may provide user training. Information to be made available can be in other than printed form.

16.2 Information on conformance to this standard

The manufacturer shall make available, on request, compliance verification information.

16.3 Information on type and content of documentation

Four types of documentation are defined:

- catalogues and datasheets,
- user's manuals,
- safety manual and
- technical documentation.

NOTE For the preparation of the instructions, see IEC 62079 and IEC 61506.

16.4 Information on catalogues and/or datasheets

These documents shall contain the description and the specifications of the FS-PLC and its associated peripherals. Additionally, they shall contain any other relevant information to aid in understanding the application and use of these products including functional characteristics, equipment configuration rules, normal service conditions, and list compliance with standards and certifications.

16.5 Safety manual

16.5.1 General

The purpose of the safety manual is to document all the information relating to an FS-PLC that is required to enable the integration of the FS-PLC into a safety-related system, that safety-related system being in compliance with the requirements of IEC 61508 series.

NOTE This text is adapted from D.2.2 of IEC 61508-2:2010 and D.2.2 of IEC 61508-3:2010.

16.5.2 Safety manual contents

16.5.2.1 General

Every FS-PLC shall have a safety manual. In general, the safety manual shall contain:

a) a functional specification of the functions capable of being performed;
b) an identification of the hardware and/or software configuration of the FS-PLC to enable configuration management of the E/E/PE safety-related system in accordance with 6.2.1 of IEC 61508-1:2010;

c) constraints on the use of the FS-PLC and/or assumptions on which analysis of the behaviour or failure rates of the FS-PLC are based.

16.5.2.2 Safety manual contents

The safety manual shall specify the functions of the compliant item. These may be used to support a safety function of a safety-related system or functions in a subsystem or element. The specification should clearly describe both the functions and the input and output interfaces.

For every function, the safety manual shall contain:

a) the failure modes of the compliant item (in terms of the behavior of its outputs), due to random hardware failures, that result in a failure of the function and that are not detected by diagnostics internal to the FS-PLC;

b) for every failure mode in a), an estimated failure rate;

c) the failure modes of the compliant item (in terms of the behavior of its outputs) due to random hardware failures that result in a failure of the function and that are detected by diagnostics internal to the FS-PLC;

d) the failure modes of the diagnostics internal to the FS-PLC (in terms of the behavior of its outputs) due to random hardware failures that result in a failure of the diagnostics to detect failures of the function;

e) for every failure mode in c) and d), the estimated failure rate;

f) for every failure mode in c) that is detected by diagnostics internal to the FS-PLC, the diagnostic test interval;

g) for every failure mode in c), the outputs of the compliant item initiated by the internal diagnostics;

NOTE 1 The outputs of the internal diagnostics include initiation of additional measures (technical/procedural) to the E/E/PE safety-related system, subsystem or element to achieve or maintain a safe state of the EUC.

h) any periodic proof test and/or maintenance requirements;

i) for those failure modes, in respect of a specified function, that are capable of being detected by external diagnostics, sufficient information shall be provided to facilitate the development of an external diagnostics capability. The information shall include details of failure modes and for those failure modes the failure rates;

j) the hardware fault tolerance;

k) the classification as type A or type B of that part of the FS-PLC that provides the function;

NOTE 2 Failure modes are classified as being safe or dangerous when the application of the FS-PLC is known in relation to the hazards of the EUC. For example, if a sensor is applied in such a way that a high output is used to signal a hazard of the EUC (for example high pressure), then a failure mode that prevents the correct indication of the hazard (for example output stuck low) is classified as dangerous whereas a failure mode that causes the sensor output to go high is classified as safe. This depends on how the sensor signal is interpreted by the FS-PLC and so cannot be specified without constraining the way that the sensor is applied.

Also, the level of diagnostic coverage claimed for a FS-PLC generally vary from one application to another depending on the extent of any diagnostics in the FS-PLC or external signal processing that possibly supplements any internal diagnostics of the FS-PLC.

It follows that any estimate of the hardware fault tolerance or the safe failure fraction is made only if constraints are placed on the application of the FS-PLC. These constraints are outside the control of the supplier of the FS-PLC. Therefore, no claims shall be made in the safety manual, in respect of the hardware fault tolerance or the safe failure fraction or any other functional safety characteristic that is dependent on knowledge of safe and dangerous failure modes, unless the underlying assumptions, as to what constitute safe and dangerous failure modes, are clearly specified.

l) guidance on how to include the FS-PLC contribution to the safety function response time or process safety time.

For every function of the FS-PLC that is liable to systematic failure, the manual shall contain:

1) the systematic capability of the FS-PLC or that part of the element that provides the function;

2) any instructions or constraints relating to the application of the FS-PLC, relevant to the function, that should be observed in order to prevent systematic failures of the FS-PLC.

NOTE 3 The systematic safety integrity indicated by the systematic capability can be achieved only when the instructions and constraints are observed. Where violations occur, the claim for systematic capability is partially or wholly invalid.

16.5.2.3 Engineering tool safety manual contents

The engineering tools shall be identified and all necessary instructions for their use shall be available to the integrator and user.

NOTE For engineering tools this is demonstrated by clearly identifying the element and demonstrating that its content is unchanged.

Annex A
(informative)

Reliability calculations

A.1 General

Annex A references a number of examples of techniques for calculating the probabilities of failure for a safety instrumented system designed and installed in accordance with IEC 61511-1. This information is informative in nature and should not be interpreted as the only evaluation techniques that might be used.

The methodologies referenced are from Annex B of IEC 61508-6:2010, from IEC 61078, from IEC 61025, from IEC 61165, and from the ISA TR 84.00.02 series.

A.2 Reliability block diagram technique

IEC 61078 and Annex B of IEC 61508-6:2010 illustrate the reliability block diagram technique for calculating the probabilities of failure for safety instrumented functions designed in accordance with this standard.

A.3 Fault tree analysis technique

IEC 61025 and ISA TR 84.00.02-3 illustrate the fault tree analysis technique for calculating the probabilities of failure for safety instrumented functions designed in accordance with this standard.

A.4 Markov modelling technique

IEC 61165 and ISA TR 84.00.02-4 illustrate the Markov modelling technique for calculating the probabilities of failures for safety instrumented functions designed in accordance with this standard.

Annex B
(informative)

Typical FS-PLC Architectures

B.1 FS-PLC subsystems architectural examples

FS-PLC subsystems may incorporate multiple architectures. Further information on architectural examples is provided in B.3.2.2 and B.3.3.2 of IEC 61508-6:2010.

An M out of N architecture consists of N channels, any one of which can contribute to processing of the FS-PLC safety function. At least M channels are required to perform the FS-PLC safety function. The system executes the FS-PLC safety function if M channels are functioning properly. (N-M) defines the fault tolerance of the system, where (N-M+1) channel faults would result in the failure of the FS-PLC safety function.

Examples:

1oo1: The fault tolerance is 0 and the number of channels is 1. This architecture consists of a single channel, where any dangerous failure leads to a failure of the safety function when a demand arises.

1oo2: The fault tolerance is 1 and the number of channels is 2. This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be a dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

2oo2: The fault tolerance is 0 and the number of channels is 2. This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

2oo3: The fault tolerance is 1 and the number of channels 3. This architecture consists of three channels connected in parallel with a majority voting arrangement for the output signals, such that the output state is not changed if only one channel gives a different result which disagrees with the other two channels. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

The following architecture implementations are typical of what can be found in FS-PLCs.

B.2 Single FS-PLC with single I/O and external watchdog (1oo1D)

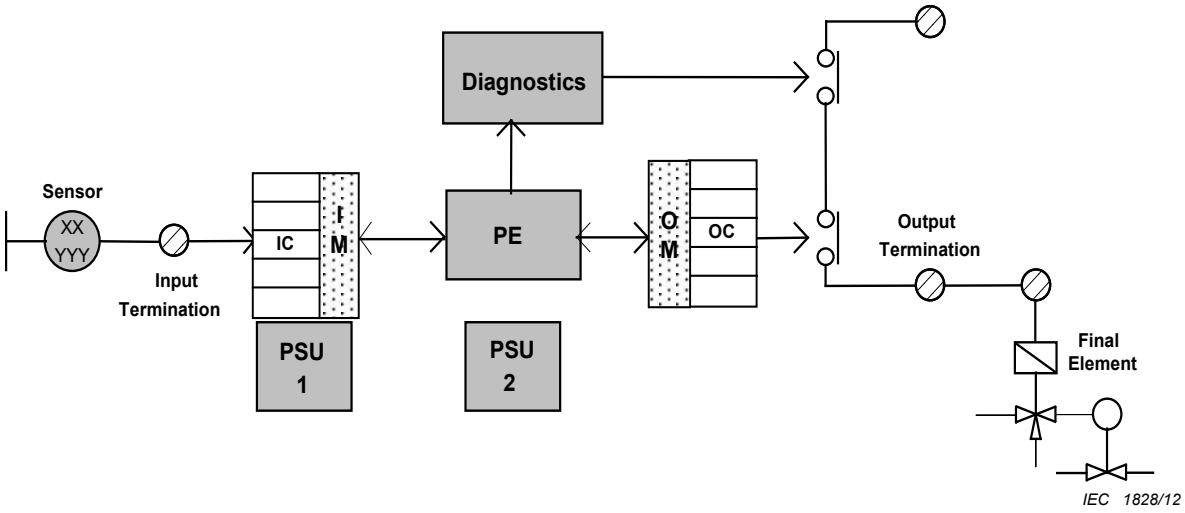


Figure B.1 – Single FS-PLC with single I/O and external watchdog (1oo1D)

This configuration has no redundancy. It consists of a single channel: single processing element (PE), input channel (IC) on an input module (IM), output channel (OC) on an output module (OM). This configuration may include redundant power supply units (PSU). The external watchdog (diagnostic) function provides a secondary means of de-energizing the outputs and putting the process under control in a safe state. This external watchdog function de-energizes the secondary contact output if a dangerous fault is detected in the logic solver or the associated output module. The outputs are shown as contacts but can be realized by solid state switches or other means.

All safe faults result in a false trip of the process under control. All dangerous detected faults also result in a false trip of the process under control since the system has to be shut down to replace any of the modules.

B.3 Dual PE with single I/O and external watchdogs (1oo1D)

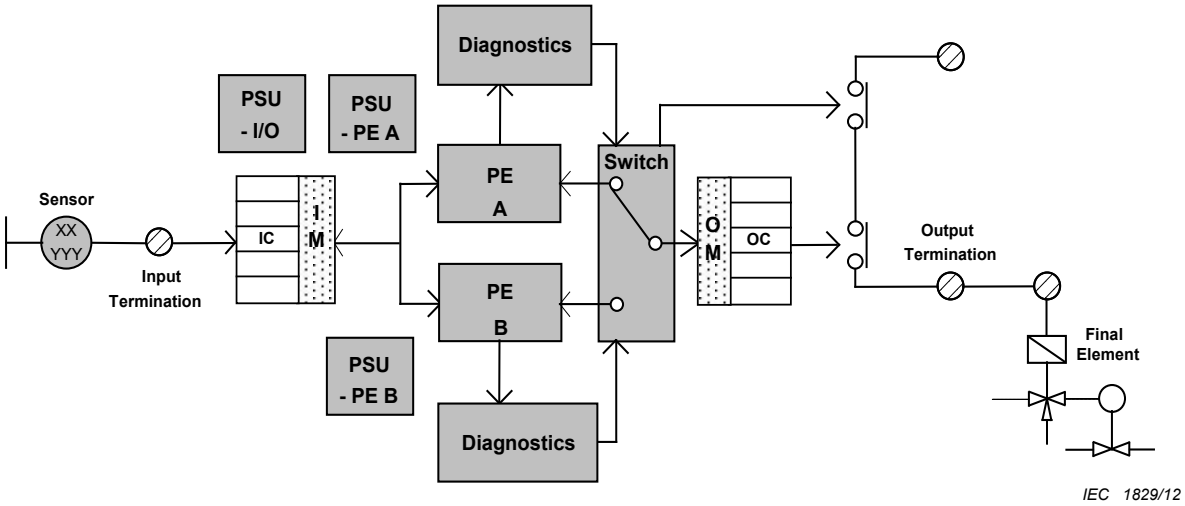


Figure B.2 – Dual PE with single I/O and external watchdogs (1oo1D)

This dual configuration has redundant processing elements and external watchdogs. The switch shown is controlled by the watchdog functions which are monitoring the diagnostic results of the processing elements. The secondary means of de-energizing the outputs will be activated if both the diagnostic inputs to the switch are de-activated. The switch is periodically

changed to the other position so that its functionality and the functionality and the diagnostics of each processing part can be checked in the other state. The two processing elements compare results and if a discrepancy is detected, both of the watchdogs are commanded to de-activate the outputs. Hence any discrepancy between the processing parts will result in the outputs being de-energized to put the process under control in a safe state. Detected faults in any of the single I/O modules will also result in the outputs being de-energized. Safe undetected faults of the logic solver as well as the comparison errors mentioned above result in a false trip of the process under control, other detected safe and dangerous fault of either processing element can be repaired on line.

If a dangerous fault of the processor driving the outputs is undetected, the safety system will be in a fail-to-function state.

B.4 Dual PE with dual I/O, no inter-processor communication, and 1oo2 shutdown logic

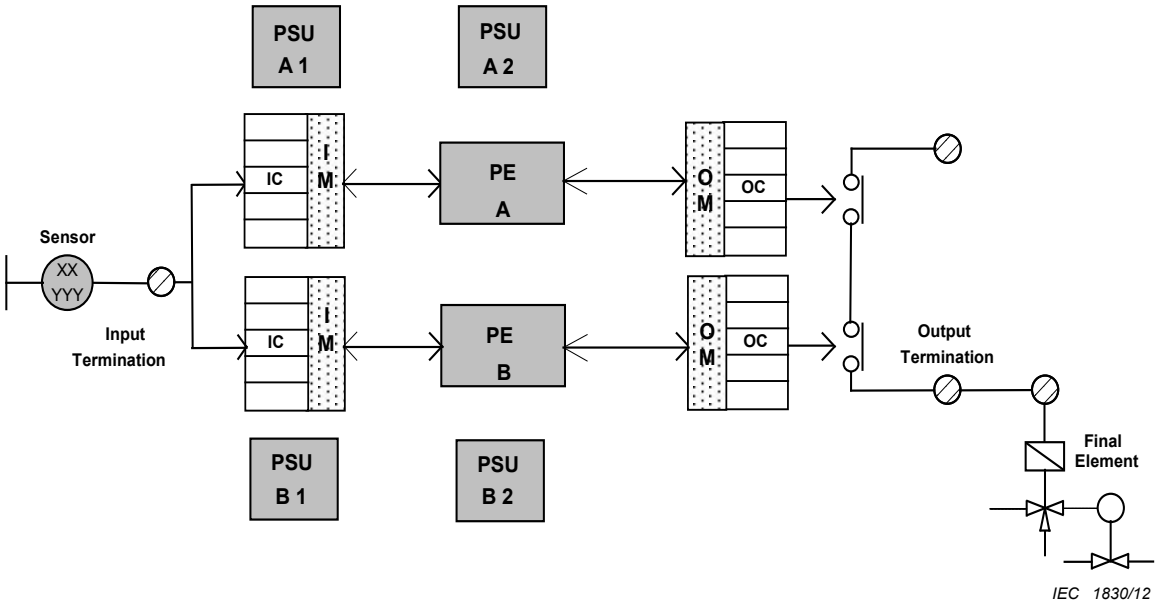


Figure B.3 – Dual PE with dual I/O, no inter-processor communication, and 1oo2 shutdown logic

This dual configuration shown has two independent channels. There is no communication between the processing elements. Diagnostic coverage is determined by the diagnostic coverage achievable in a single channel system. The outputs from one channel to each final element are wired in series with the outputs from the other channel, and hence each channel can open the output circuit and put the process under control in a safe state. Each processing element will command the outputs to a safe state if any input makes a transition which corresponds to a dangerous event or if a dangerous fault is detected in any of the modules in the channel. The configuration shown does not have external watchdogs, since the outputs from each channel are wired in series.

All safe faults and dangerous detected faults in the system result in a false trip of the process under control.

B.5 Dual PE with dual I/O, inter-processor communication, and 1oo2D shutdown logic

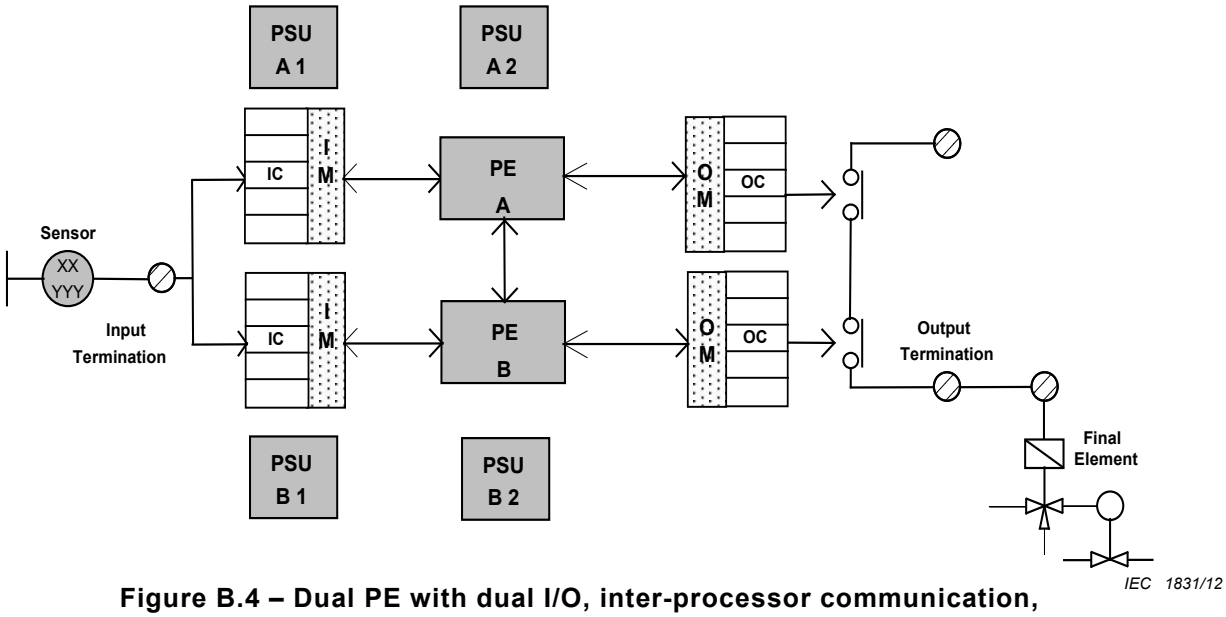


Figure B.4 – Dual PE with dual I/O, inter-processor communication, and 1oo2D shutdown logic

This dual configuration also has two independent channels. This system has communication between the processing elements. This communication increases the overall diagnostic coverage of the processing elements because of the comparison testing that can be performed. The communication also allows the processors to compare input values and continue operation with a healthy input in the event of a detected fault on the other input. All other safe faults and all dangerous detected faults in the system result in a false trip of the process under control.

B.6 Dual PE with dual I/O, no inter-processor communication, external watchdogs, and 2oo2 shutdown logic

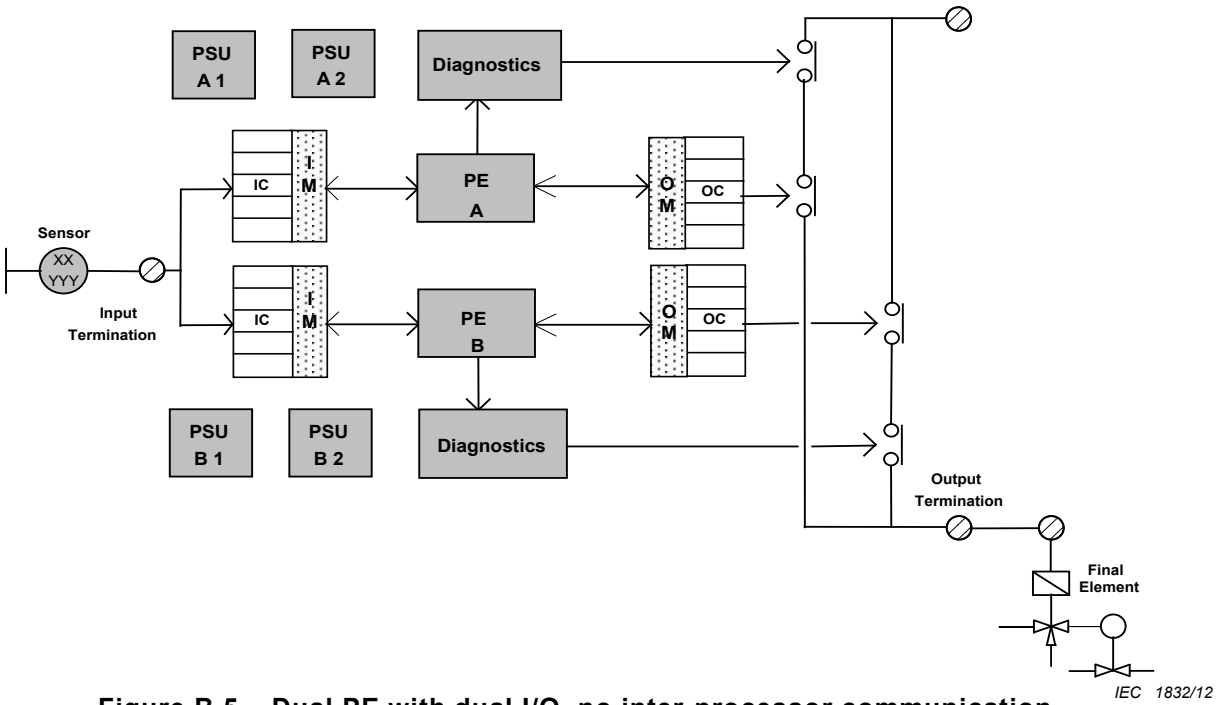


Figure B.5 – Dual PE with dual I/O, no inter-processor communication, external watchdogs, and 2oo2 shutdown logic

This configuration has two independent 1oo1D channels. The system has no communication between the processing elements. The outputs to the final elements from each channel are wired in parallel to reduce the number of false or spurious trips. Hence both channels must command the outputs to open before an output is opened. This wiring produces a 2oo2 voting of the outputs from each channel. The system has external watchdogs in each channel to improve the safety. These watchdogs provide a secondary means of de-energizing the output of a channel if a dangerous fault of a logic solver or an output module is detected.

All dangerous undetected faults in any module in either channel of the system will put the system in a fail-to-function state.

B.7 Dual PE with dual I/O, inter-processor communication, external watchdogs, and 2oo2D shutdown logic

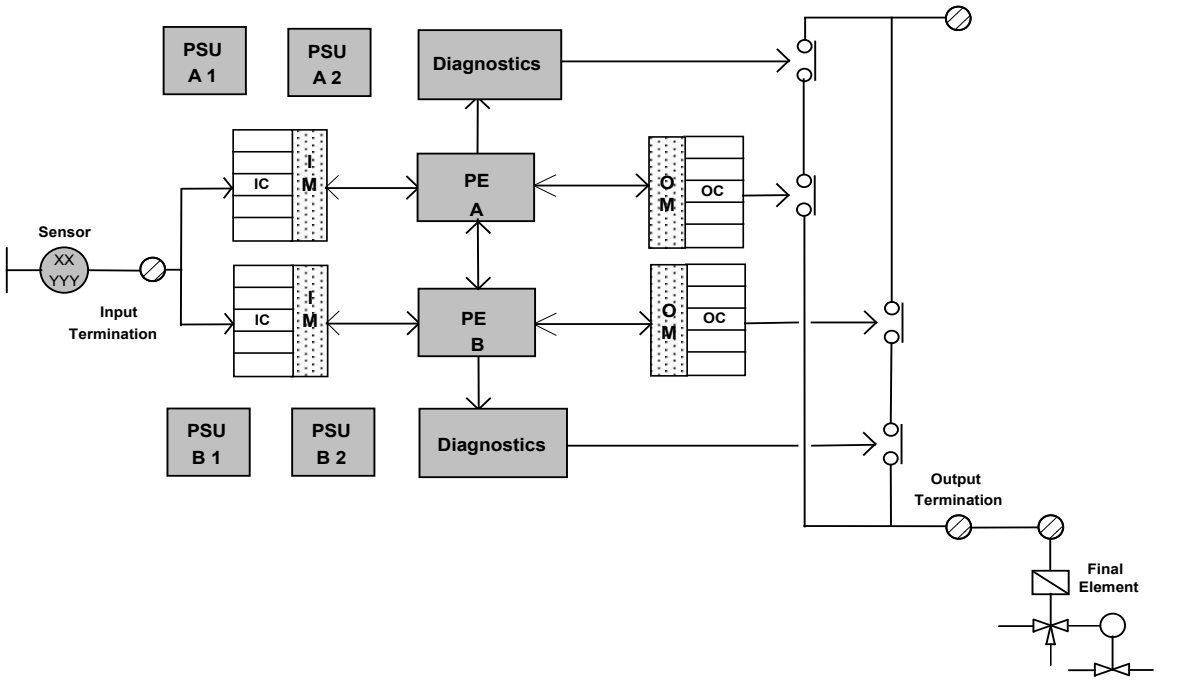


Figure B.6 – Dual PE with dual I/O, inter-processor communication, external watchdogs, and 2oo2D shutdown logic

This redundant configuration has two independent channels. The system has communication between the processing elements. The outputs to the final elements from each channel are wired in parallel to reduce the number of false or spurious trips. Hence both channels must command the outputs to open before an output is opened. The system has external watchdogs in each channel or leg to improve the safety. These watchdogs provide a secondary means of de-energizing the output of a leg if a dangerous fault of a processor is detected. The inter-processor communication enhances the diagnostic capability since comparisons can be made between the output states of the two channels.

All detected faults in this system which can be localized to a channel can be repaired on-line.

B.8 Triple PE with triple I/O, inter-processor communication, and 2oo3D shutdown logic

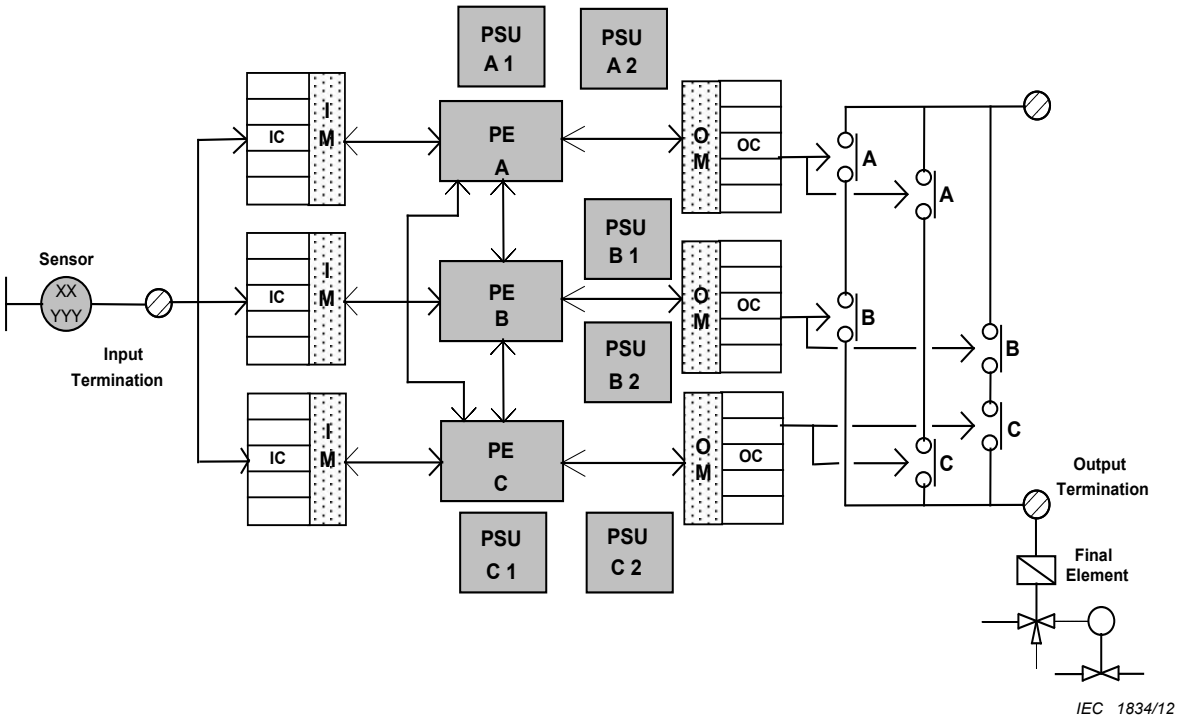


Figure B.7 – Triple PE with triple I/O, inter-processor communication, and 2oo3D shutdown logic

This redundant configuration contains three channels with inter-processor communication. Each output to the final element utilizes a fault tolerant hex output voter circuit which performs a 2oo3 vote on the three inputs to the voter. Utilizing the inter-processor communication, the processors can perform a 2oo3 vote on the sensor value read by the system. The 2oo3 voting also allows a fault in any of the three legs to be out voted. Any detected safe or dangerous fault in the triple system can be repaired on-line without shutting down the process under control.

Annex C
(informative)

Energise to trip applications of FS-PLC

C.1 General

The majority of on-demand safety functions act as de-energise to trip. In other words, the output(s) are de-energised when the safety function is demanded.

In contrast, certain safety functions act as energise to trip. In other words, the output(s) are energised when the safety function is demanded.

Energise to trip applications are often concerned with mitigation of the consequences of a hazardous event, rather than its prevention. Typical applications are in Fire and Gas Protection, for example, the sounding of an evacuation alarm, or the operation of a fire suppressant release valve.

The demands on the FS-PLC used in energise to trip applications are quite different, and more severe. If an FS-PLC is potentially to be used in energise to trip applications, the manufacturer should consider this and provide specific failure data and instructions for use in such applications.

C.2 Safe state and demand state

For de-energise to trip applications, the demand state of the safety function is usually the same as the defined safe state, the outputs are de-energised. For energise to trip applications, the demand state is output(s) energised, but the defined safe state is still typically outputs de-energised. Hence the action taken on a detected fault is different to the action taken when the safety function is demanded.

This is necessary in certain applications, for example the uncommanded release of suppressant due to an internal fault could itself be a severe hazard.

C.3 Additional information required for use in energise to trip applications

The following information should additionally be provided to the user:

- random hardware failure rates for energise to trip operation. The reliability model of the FS-PLC (see 9.4.3) is likely to be different for energise to trip and a separate FMEA may need to be performed to determine the failure rates. Note that the fail to trip failure rates are likely to be much higher for energise to trip;
- any difference to the systematic safety integrity of the FS-PLC when operating in energise to trip mode;
- any special operating conditions or recommended fault mitigation measures that should be observed when operating energise to trip;
- the distinction between the FS-PLC action on demand and action on detection of a fault should be made clear.

C.4 Particular considerations

The FS-PLC manufacturer and user should pay particular attention to the following:

- the FS-PLC is particularly dependent on power supply integrity in energise to trip applications. Failure of the power supply will result in an inability of the FS-PLC to respond to a demand. Additionally the FS-PLC may not be able to indicate that it is in a failed state;
- the use of independent, redundant power supplies is recommended. Common cause failures in the power supplies or in the power supply system should be carefully considered;
- compliance with other sector-specific codes and standards should be considered, for example EN54 and NFPA72 for fire and gas protection;
- faults in output circuit field lines and field devices are likely to prevent an energise to trip output from operating on demand. Field circuit monitoring (supervision) of energise to trip outputs is recommended to detect such failures.

Annex D
(informative)

Available failure rate databases

D.1 Databases

The following bibliography is a non-exhaustive list, in no particular order, of sources of failure rate data for electronic and non-electronic components. It should be noted that these sources do not always agree with each other, and therefore care should be taken when applying the data.

- IEC/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*, Union Technique de l'Electricité et de la Communication (www.ute-fr.com). Identical to RDF 2000/Reliability Data Handbook, UTE C 80-810
- Siemens Standard SN 29500, *Failure rates of components, (parts 1 to 14)*; Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.
- Telcordia SR-332, Issue 01: May 2001, *Reliability Prediction Procedure for Electronic Equipment*, (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06).
- EPRD (RAC-STD-6100) – *Electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).
- NNPRD-95 (RAC-STD-6200) – *Non-electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.
- HRD5, *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom
- Chinese Military/Commercial Standard GJB/z 299B, *Electronic Reliability Prediction*, (http://www.itemuk.com/china299b.html)
- ISBN:0442318480, *AT&T reliability manual – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors*, AT&T Reliability Manual, Van Nostrand Reinhold, 1990,.
- FIDES:January, 2004, *Reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA*. FIDES is available on request at fides@innovation.net.
- IEEE Gold book – *The IEEE Gold book IEEE recommended practice for the design of reliable, industrial and commercial power systems provides data concerning equipment reliability used in industrial and commercial power distribution systems*. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Phone: +1 800 678 IEEE (in the US and Canada) +1 732 981 0060 (outside of the US and Canada), FAX: +1 732 981 9667 e-mail: customer.service@ieee.org.
- IRPH ITALTEL, *Reliability Prediction Handbook* – The Italtel IRPH handbook is available on request from: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy. This is the Italian telecommunication companies version of CNET RDF. The standards are based on the same data sets with only some of the procedures and factors changed.
- PRISM (RAC / EPRD) – The PRISM software is available from the address below, or is incorporated within several commercially available reliability software packages: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

D.2 Helpful standards concerning component failure

The following standards contain information with regard to component failure.

- IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*
- IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*
- IEC 60319, *Presentation and specification of reliability data for electronic components*
- IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*
- IEC 60721-1, *Classification of environmental conditions – Part 1: Environmental parameters and their severities*
- IEC 61709, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*
- IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

NOTE See Annex D of this standard for further information on failure modes of electrical/electronic components.

Annex E
(informative)

Methodology for the estimation of common cause failure rates in a multiple channel FS-PLC

E.1 General

This informative Annex provides a simple qualitative approach for the estimation of common cause failure rates that can be applied to the FS-PLC design.

Also see CCF estimation in Annex D of IEC 61508-6:2010.

E.2 Methodology

The design of the multiple channel part or parts of the FS-PLC should be assessed to establish the effectiveness of the measures used to safeguard against common cause failures. The items in Table E.1, that are applicable, should be identified and an overall score established, which is used to determine the common cause failure factor from Table E.2 as a percentage value.

Table E.1 – Criteria for estimation of common cause failure

Item	Score
Separation/segregation	
Are all channel elements physically separate, for example on physically separate PCBs?	5
Are all channel elements enclosed in separate shielded enclosures?	5
Are the inputs to the channels completely separate, for example there is no common sense resistor?	5
Are separate and independent I/O data buses used for each channel?	5
Is cross connection or passing of data between channels prevented, other than diagnostic information?	5
Diversity/redundancy	
Are the diagnostic tests of one channel independent of the operation of another channel?	5
Do the channels employ deliberate temporal differences in functional operation (temporal diversity) to reduce the risk of coincident failures?	10
Is different separately-developed embedded software employed in different channels?	10
Is the diagnostic test interval of each channel less than 1 min?	10
Does at least one channel employ substantially different technology to the other channel(s), for example one electromagnetic relay in one channel and electronic in the other(s) ?	10
Design	
Do I/O data buses have strong error detection?	5
Do the FS-PLC designers have previous experience of eliminating common cause failures?	5
Assessment/analysis	
Has the hardware failure mode and effects analysis been used during the design process to identify and eliminate sources of common cause failure?	10
Has the multi-channel design been thoroughly reviewed by competent staff, independent of the design team?	10
Environmental control	
Are there measures to detect and react to over temperature?	5

Item	Score
Is EMC susceptibility tested to increased rather than standard industrial levels?	10
Is there any significant additional environmental protection?	5

Using Table E.1 those items that are considered to affect the multichannel design should be added to provide an overall score for the FS-PLC design. Where equivalent means of avoiding common cause failures have been used in the FS-PLC design then the relevant score can be claimed provided that the equivalence is justified.

This overall score can be used to determine a common cause failure factor (β) using Table E.2.

Table E.2 – Estimation of common cause failure factor

Overall score	Common cause failure factor β
<45	5 % (0,05)
45 – 70	2 % (0,02)
>70	1 % (0,01)

The common cause failure rate for dangerous undetected failures is determined by multiplying the dangerous undetected random hardware failure rate for one channel by the common cause failure factor (β).

Bibliography

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

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

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61025:2006, *Fault tree analysis (FTA)*

IEC 61069-7:1999, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 7: Assessment of system safety*

IEC 61078:2006, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61131-3:2003, *Programmable controllers – Part 3: Programming languages*

IEC 61165:2006, *Application of Markov techniques*

IEC 61496-1:2008, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

IEC 61496-3:2008, *Safety of machinery – Electro-sensitive protective equipment – Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)*

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

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

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

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety – related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61511-1:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

IEC 61511-2:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1*

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

IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

IEC 62079:2001, *Preparation of instructions – Structuring, content and presentation*

IEC/TR 62380:2004, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

IEC Guide 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications*

CISPR 11:2009, *Industrial, scientific and medical equipment – Radio-frequency disturbance characteristics – Limits and methods of measurement*

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

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

ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14:Reliability, maintainability and availability*

ISO/IEC 12207:2008, *Systems and software engineering – Software life cycle processes*

ISO 8402:1994, *Quality management and quality assurance – Vocabulary*

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

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

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

ISO 13849-2:2003, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

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

IEEE 352-1987, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*

IEEE 828-2005, *IEEE Standard for Software Configuration Management Plans*

IEEE 1042-1987, *IEEE Guide to Software Configuration Management*

ISA TR 84.00.02:2002, *Part-1, Safety Instrumented Function (SIF) – Safety Integrity Level*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

AUTOMATES PROGRAMMABLES –

Partie 6: Sécurité fonctionnelle

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61131-6 a été établie par le sous-comité 65B: Equipements de mesure et de contrôle-commande, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65B/831/FDIS	65B/850/RVD

Le rapport de vote indiqué dans le tableau ci-dessus fournit toutes les informations sur le vote ayant abouti à l'approbation de la présente norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61131, présentées sous le titre général *Automates programmables,* peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

Généralités

La série CEI 61131 comprend les parties suivantes, regroupées sous le titre général *Automates programmables*:

Partie 1: Informations générales
Partie 2: Exigences et essais des équipements
Partie 3: Langages de programmation
Partie 4: Guide pour l'utilisateur
Partie 5: Communications
Partie 6: Sécurité fonctionnelle
Partie 7: Programmation en logique floue
Partie 8: Lignes directrices pour l'application et la mise en œuvre des langages de programmation

Cette partie de la série CEI 61131 constitue la Partie 6 d'une série de normes sur les automates programmables et leurs périphériques associés, et il convient de la lire conjointement avec les autres parties de la série.

Ce document étant la norme de produit FS-PLC, il convient de respecter les dispositions de cette partie dans le domaine des automates programmables et leurs périphériques associés.

Aucune conformité avec la Partie 6 de la CEI 61131 ne peut être déclarée à moins que les exigences de l'Article 4 de cette partie soient respectées.

Les termes d'utilisation générale sont définis dans la Partie 1 de la CEI 61131. Les termes spécifiques sont définis dans chaque partie.

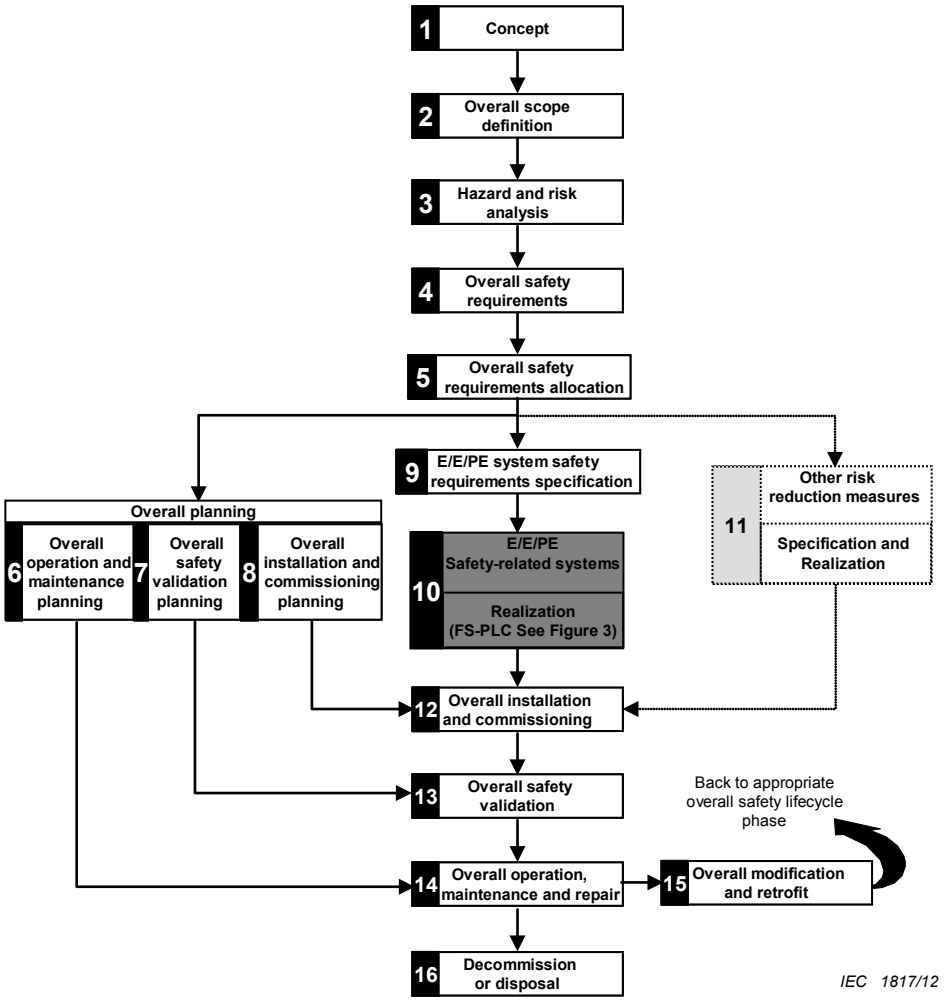
Conformément au 1.1 de la CEI 61508-1:2010, cette partie intègre les exigences spécifiques au produit des CEI 61508-1, 61508-2 et 61508-3 comme appartenant aux automates programmables et à leurs périphériques associés.

L'objectif de ce document est de suivre dans le principe la structure de la série CEI 61508. Cependant, certains aspects n'ont pas de corrélation directe et il est donc nécessaire de les traiter différemment. Cela est dû en partie au fait que l'on aborde dans un seul document le matériel, les logiciels, les microprogrammes, etc.

Structure de cette partie

La Figure 2 de la CEI 61508-1:2010 est incluse ici, sous la dénomination Figure 1. Elle a été ajustée de manière à montrer comment un automate programmable de sécurité fonctionnelle (FS-PLC) s'adapte à l'ensemble du cycle de vie d'un système électrique/électronique/électronique programmable relatif à la sécurité. Bien que la case 10 de la Figure 1 inclue des capteurs, un sous-système logique et des éléments finaux (par exemple, des actionneurs), car c'est le point de vue de la CEI 61508-1, ici, l'accent est mis sur le FS-PLC comme cela est référencé à la Figure 3.

C'est pourquoi la phase Réalisation, Figure 1, case 10, incarne uniquement le sous-système logique, dans la perspective de cette partie.



NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.

NOTE 2 The phases represented by box 11 is outside the scope of this standard.

NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 10 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

NOTE 4 See IEC 61508-1, Table 1 for a description of the objectives and scope of the phases represented by each box.

NOTE 5 The technical requirements necessary for the overall operation, maintenance, repair Modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E? PE safety-related system and its elements and components.

Légende

Anglais	Français
Concept	Concept
Overall scope definition	Définition du domaine d'application général
Hazard and risk analysis	Analyse des risques et des dangers
Overall safety requirements	Exigences de sécurité générales
Overall safety requirements allocation	Allocation des exigences de sécurité générales
Overall planning	Planification générale
Overall operation and maintenance planning	Planification générale du fonctionnement et de la maintenance
Overall safety validation planning	Planification générale de la validation de la sécurité
Overall installation and commissioning planning	Planification générale de l'installation et de la mise en service
E/E/PE system safety requirements specification	Spécification des exigences de sécurité pour les systèmes électriques/électroniques/électroniques programmables

Anglais	Français
E/E/PE Safety-related systems	Systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
Realization (FS-PLC See Figure 3)	Réalisation (FS-PLC, voir Figure 3)
Other risk reduction measures	Autres mesures de réduction des risques
Specification and Realization	Spécification et réalisation
Overall installation and commissioning	Installation et mise en service générales
Overall safety validation	Validation générale de la sécurité
Overall operation, maintenance and repair	Fonctionnement, maintenance et réparation généraux
Decommission or disposal	Mise hors service ou destruction
Overall modification and retrofit	Modification et amélioration générales
Back to appropriate overall safety lifecycle phase	Retour à la phase appropriée du cycle de vie de sécurité générale
NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.	NOTE 1 Les activités relatives à la vérification, à la gestion de la sécurité fonctionnelle et à l'évaluation de la sécurité fonctionnelle ne sont pas affichées pour plus de clarté, mais elles sont relatives à toutes les phases du cycle de vie de sécurité global du logiciel et du système électrique/électronique/électronique programmable.
NOTE 2 The phases represented by box 11 is outside the scope of this standard.	NOTE 2 Les phases représentées dans la case 11 ne relèvent pas du domaine d'application de la présente norme.
NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 10 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.	NOTE 3 La CEI 61508-2 et la CEI 61508-3 concernent la case 10 (réalisation) mais également, le cas échéant, les aspects électroniques programmables (matériel et logiciel) des cases 13, 14 et 15.
NOTE 4 See IEC 61508-1, Table 1 for a description of the objectives and scope of the phases represented by each box.	NOTE 4 Pour obtenir une description des objectifs et du domaine d'application des phases représentées dans chaque case, voir la CEI 61508-1, Tableau 1.
NOTE 5 The technical requirements necessary for the overall operation, maintenance, repair Modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.	NOTE 5 Les exigences techniques relatives aux activités générales de fonctionnement, de maintenance, de réparation, de modification, d'amélioration, de mise hors service ou de destruction seront spécifiées dans la documentation du fournisseur du système électrique/électronique/électronique programmable relatif à la sécurité et de ses éléments et composants.

Figure 1 – FS-PLC dans l'ensemble des phases du cycle de vie de sécurité d'un système électrique/électronique/électronique programmable relatif à la sécurité

Les domaines inclus dans cette partie sont la gestion du cycle de vie de sécurité du FS-PLC, l'allocation des exigences de sécurité fonctionnelle et la planification du développement; avec un intérêt tout particulier pour la phase Réalisation (case 10) du cycle de vie de sécurité global, présenté dans la Figure 1. Cette partie suppose que le FS-PLC est utilisé en tant que sous-système logique pour l'ensemble du système électrique/électronique/électronique programmable.

La Figure 1, Réalisation (case 10), inclut:

- l'attribution des aspects sécuritaires du FS-PLC au matériel, au logiciel ou au microprogramme, ou toute autre combinaison du FS-PLC,
- les architectures matérielles du FS-PLC,
- les activités de vérification et de validation au niveau du FS-PLC,

- les exigences de modification du FS-PLC,
- les informations sur le fonctionnement et la maintenance pour l'utilisateur du FS-PLC,
- les informations fournies par le fabricant du FS-PLC pour l'utilisateur.

AUTOMATES PROGRAMMABLES –

Partie 6: Sécurité fonctionnelle

1 Domaine d'application

Cette partie de la série CEI 61131 spécifie les exigences pour les automates programmables (PLC) et leurs périphériques associés, comme défini dans la Partie 1, visant à être utilisés comme sous-système logique d'un système électrique/électronique/électronique programmable relatif à la sécurité. Un automate programmable et ses périphériques associés, conformes aux exigences de cette partie, sont considérés comme appropriés dans un système électrique/électronique/électronique programmable relatif à la sécurité et sont identifiés comme un automate programmable de sécurité fonctionnelle (FS-PLC). Un FS-PLC est généralement un sous-système matériel ou logiciel. Un FS-PLC peut également inclure des éléments logiciels, par exemple des blocs fonctionnels prédéfinis.

En général, un système électrique/électronique/électronique programmable relatif à la sécurité est constitué de capteurs, d'actionneurs, d'un logiciel et d'un sous-système logique. Cette partie est une implémentation spécifique pour les produits des exigences de la série CEI 61508 et la conformité à cette partie remplit toutes les exigences applicables de la série CEI 61508 relative aux FS-PLC. Bien que la série CEI 61508 soit une norme système, cette partie fournit des exigences spécifiques aux produits pour l'application des principes de la série CEI 61508 relative aux FS-PLC.

Cette partie de la série CEI 61131 traite uniquement de la sécurité fonctionnelle et des exigences d'intégrité de sécurité d'un FS-PLC lorsqu'il est utilisé comme partie d'un système électrique/électronique/électronique programmable relatif à la sécurité. La définition des exigences de sécurité fonctionnelle de l'ensemble du système électrique/électronique/électronique programmable relatif à la sécurité et la définition des exigences de sécurité fonctionnelle de l'utilisation finale dans une application du système électrique/électronique/électronique programmable relatif à la sécurité n'entre pas dans le cadre de cette partie, mais elles sont des données à prendre en compte pour cette partie. Pour les informations spécifiques aux applications, le lecteur est renvoyé à des références de normes telles que la série CEI 61511, la CEI 62061 et la série ISO 13849.

Cette partie ne couvre pas les exigences de sécurité générale pour un FS-PLC telles que les exigences relatives aux chocs électriques et aux dangers liés aux incendies spécifiés dans la CEI 61131-2.

Cette partie s'applique à un FS-PLC ayant un niveau d'intégrité de sécurité (SIL) inférieur ou égal à SIL 3.

L'objectif de cette partie est:

- d'établir et de décrire les éléments du cycle de vie de sécurité d'un FS-PLC, conformément au cycle de vie général de sécurité identifié dans les CEI 61508-1, -2 et -3;
- d'établir et de décrire les exigences pour le matériel et les logiciels des FS-PLC relatifs à la sécurité fonctionnelle et aux exigences d'intégrité de sécurité d'un système électrique/électronique/électronique programmable relatif à la sécurité;
- d'établir des méthodes d'évaluation pour un FS-PLC dans cette partie pour les paramètres/critères suivants:
  - une déclaration de niveau d'intégrité de sécurité (SIL) pour laquelle le FS-PLC est compétent,
  - une valeur de probabilité de défaillance à la demande (PFD),

  - une valeur de fréquence moyenne de défaillance dangereuse par heure (PFH),
  - une valeur pour la fraction de défaillance en sécurité (SFF),
  - une valeur pour la tolérance aux pannes matérielles (HFT),
  - une valeur de couverture de diagnostic (DC),
  - la vérification que les processus de cycle de vie de sécurité spécifiés par le fabricant de FS-PLC sont en place,
  - l'état de sécurité défini,
  - les mesures et techniques pour la prévention et le contrôle des pannes systématiques, et
  - pour chaque mode de défaillance traité dans cette partie, le comportement fonctionnel de l'état de panne;
- d'établir les définitions et d'identifier les principales caractéristiques pour la sélection et l'application des FS-PLC et leurs périphériques associés.

Cette partie est principalement destinée aux fabricants de FS-PLC. Elle inclut également le rôle essentiel des utilisateurs de FS-PLC via les exigences de la documentation utilisateur. Certaines instructions utilisateur concernant les FS-PLC peuvent se trouver dans la CEI 61131-4.

Les exigences du Guide ISO/CEI 51 et du Guide CEI 104 relatives à cette partie sont intégrées ci-dessous.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60947-5-1:2003, *Appareillage à basse tension – Partie 5-1: Appareils et éléments de commutation pour circuits de commande – Appareils électromécaniques pour circuits de commande*

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

CEI 61000-4-2:2008, *Compatibilité électromagnétique (CEM) – Partie 4-2: Techniques d'essai et de mesure – Essai d'immunité aux décharges électrostatiques*

CEI 61000-4-3:2006, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques*

CEI 61000-4-4:2012, *Compatibilité électromagnétique (CEM) – Partie 4-4: Techniques d'essai et de mesure – Essai d'immunité aux transitoires électriques rapides en salves*

CEI 61000-4-5:2005, *Compatibilité électromagnétique (CEM) – Partie 4-5: Techniques d'essai et de mesure – Essai d'immunité aux ondes de choc*

CEI 61000-4-6:2008, *Compatibilité électromagnétique (CEM) – Partie 4-6: Techniques d'essai et de mesure – Immunité aux perturbations conduites, induites par les champs radioélectriques*

CEI 61000-4-8:2009, *Compatibilité électromagnétique (CEM) – Partie 4-8: Techniques d'essai et de mesure – Essai d'immunité au champ magnétique à la fréquence du réseau*

CEI 61131-1:2003, *Automates programmables – Partie 1: Informations générales*

CEI 61131-2:2007, *Automates programmables – Partie 2: Exigences et essais des équipements*

CEI 61131-4:2004, *Programmable controllers – Part 4: User guidelines* (disponible en anglais seulement)

CEI 61326-3-1:2008, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

CEI 61326-3-2:2008, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

CEI 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

CEI 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61784-3:2010, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

CEI 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

Guide CEI 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications* (disponible en anglais seulement)

Guide ISO/CEI 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

EN 50205:2002, *Relais de tout ou rien à contacts guidés (liés)*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
logiciel d'application
programme d'application
partie du logiciel d'un système électronique programmable qui spécifie les fonctions réalisées par une tâche relative à l'EUC plutôt que le fonctionnement du dispositif programmable proprement dit et des services qu'il fournit
[SOURCE: CEI 61508-4:2010, 3.2.7]

3.2
circuit intégré propre à une application
ASIC
circuit intégré conçu et fabriqué pour une fonction spécifique et pour lequel la fonctionnalité est définie par le développeur du produit

[SOURCE: CEI 61508-4:2010, 3.2.15, modifiée]

3.3
architecture
configuration spécifique des éléments matériels et logiciels dans un système

[SOURCE: CEI 61508-4:2010, 3.3.4]

3.4
disponibilité
probabilité qu'un élément puisse accomplir sa fonction prévue, exprimée à l'aide d'une valeur décimale comprise entre zéro et un

EXEMPLE A = 0,9 signifie qu'un produit est disponible 90 % du temps.

Note 1 à l'article: Pour $\lambda T << 1$, $A = 1 - \lambda T$, Voir 3.23.

3.5
fréquence moyenne de défaillance dangereuse par heure
PFH
fréquence moyenne de défaillance dangereuse d'un système électrique/électronique/électronique programmable relatif à la sécurité pour effectuer la fonction de sécurité spécifiée au cours d'une période donnée

Note 1 à l'article: Le terme "probabilité de défaillance dangereuse par heure" n'est pas utilisé dans la présente norme alors que l'acronyme PFH a été conservé, mais il est utilisé pour "fréquence moyenne de défaillance dangereuse [h]".

Note 2 à l'article: D'un point de vue théorique, la PFH est la moyenne de l'intensité de défaillance inconditionnelle, également appelée fréquence de défaillance, généralement indiquée comme suit *w(t)*. Il convient de ne pas la confondre avec le taux de défaillance (voir l'Annexe B de la CEI 61508-6:2010).

Note 3 à l'article: Lorsque le système électrique/électronique/électronique programmable relatif à la sécurité est la dernière couche de sécurité, il convient de calculer la PFH à partir de son manque de fiabilité $F(T)=1-R(t)$ (voir le taux de défaillance ci-dessus). Lorsqu'il ne s'agit pas du dernier système relatif à la sécurité, il convient de calculer la PFH à partir de son indisponibilité *U(t)* (voir la PFD, 3.38). Les approximations PFH sont données par $F(T)/T$ et 1/MTTF dans le premier cas et par 1/MTBF dans le deuxième cas.

Note 4 à l'article: Lorsque le système électrique/électronique/électronique programmable relatif à la sécurité implique uniquement des défaillances rapidement réparables, le taux de défaillance asymptotique λ_{as} est rapidement atteint. Il fournit une estimation de la PFH.

[SOURCE: CEI 61508-4:2010, 3.6.19]

3.6
canal noir
parties d'un canal de communication qui ne sont pas conçues ou validées conformément à la série CEI 61508

Note 1 à l'article: Voir: 7.4.11.2 de la CEI 61508-2:2010.

3.7
canal
élément ou groupe d'éléments exécutant la fonction de sécurité d'un élément de manière indépendante

EXEMPLE Une configuration à deux canaux (ou à canal doublé) comprend deux canaux réalisant indépendamment la même fonction..

Note 1 à l'article: Ce terme peut être utilisé pour décrire un système complet, ou une partie d'un système (par exemple, capteurs ou éléments finaux).

[SOURCE: CEI 61508-4:2010, 3.3.6]

3.8
défaillance de cause commune
CCF
défaillance résultant d'un ou plusieurs événements qui, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance du système
[SOURCE: CEI 61508-4:2010, 3.6.10]

3.9 cybersécurité
protection des données sur les systèmes informatiques et d'information contre la perte ou la corruption due à des activités intentionnelles ou involontaires effectuées par des individus non autorisés ou malveillants

Note 1 à l'article: Ce terme concerne la défense contre de telles activités via le réseau ou d'autres interfaces de communication.

3.10
défaillance dangereuse
FS-PLC
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en oeuvre de la fonction de sécurité qui:

a) empêche le fonctionnement nécessaire de la fonction de sécurité (mode de sollicitation) ou provoque la défaillance d'une fonction de sécurité (mode continu) de sorte que l'EUC est mis dans un état dangereux ou potentiellement dangereux, ou

b) diminue la probabilité que la fonction de sécurité fonctionne correctement lorsque c'est nécessaire

[SOURCE: CEI 61508-4:2010, 3.6.7]

3.11
panne dangereuse
panne susceptible d'entraîner une défaillance dangereuse

Note 1 à l'article: Si une panne dangereuse est détectée, des mesures sont prises pour éviter une défaillance dangereuse.

3.12
état de sécurité défini
état du FS-PLC, défini par son fabricant, au moment où survient une défaillance dangereuse

Note 1 à l'article: En général, l'état de sécurité défini correspond à l'état par défaut de chaque sortie du FS-PLC. Pour les sorties numériques, cet état est considéré comme hors tension, sauf indication contraire. Pour les sorties analogiques, cet état est égal à zéro volt ou zéro ampère, sauf indication contraire. Pour les ports de communications, cet état est défini comme aucune communication, sauf indication contraire.

3.13
défaillance détectée
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise détectée par les essais de diagnostic, les essais de sûreté, l'intervention d'un opérateur ou via un fonctionnement normal

EXEMPLE Inspection physique et essais manuels.

3.14
couverture de diagnostic
DC

fraction des défaillances dangereuses détectées par des essais de diagnostic automatiques en ligne, calculée à l'aide des taux de défaillances dangereuses associés aux défaillances dangereuses détectées divisés par le taux total de défaillances dangereuses

Note 1 à l'article: La couverture de diagnostic des défaillances dangereuses est calculée à l'aide de l'équation suivante, où DC correspond à la couverture de diagnostic, λ_{DD} est le taux de défaillances dangereuses détectées et λ_{Dtotal} est le taux total de défaillances dangereuses:

$$DC = \Sigma\lambda_{DD} / \Sigma\lambda_{Dtotal}$$

Note 2 à l'article: Cette définition est applicable à condition que les composants individuels aient des taux de défaillances constants.

[SOURCE: CEI 61508-4:2010, 3.8.6]

3.15
électrique/électronique/électronique programmable
système électrique/électronique/électronique programmable

3.16
élément
partie d'un sous-système comprenant un seul composant ou n'importe quel groupe de composants et réalisant une ou plusieurs fonctions de sécurité de l'élément

[SOURCE: CEI 62061:2005, 3.2.6, modifiée]

Note 1 à l'article: Un élément peut comporter le matériel et/ou le logiciel.

[SOURCE: CEI 61508-4:2010, 3.4.5, modifiée]

3.17
fonction de sécurité de l'élément
partie d'une fonction de sécurité mise en œuvre par un élément

[SOURCE: CEI 61508-4:2010, 3.5.3, modifiée]

3.18
logiciel embarqué
microprogramme intégré
FW
logiciel contrôlant le fonctionnement du FS-PLC ou l'un de ses sous-systèmes

Note 1 à l'article: Le logiciel embarqué est fourni par le fabricant du FS-PLC et est installé dans le FS-PLC. L'utilisateur n'a pas d'accès direct au logiciel intégré. Le fabricant du FS-PLC développe ou écrit le logiciel embarqué pour contrôler son FS-PLC. Cela peut, par exemple, contrôler le sous-système de communication ou l'interprétation du programme développé par l'utilisateur avec les outils d'ingénierie.

Note 2 à l'article: Autre terme pour logiciel embarqué.

Note 3 à l'article: Les microprogrammes peuvent être ou non relatifs à la sécurité.

3.19
outils d'ingénierie
logiciel permettant de développer le programme d'application

EXEMPLE: Le logiciel des outils d'ingénierie est fourni par le fabricant du FS-PLC pour être installé sur le poste de travail d'un ordinateur. Dans ce package logiciel, l'utilisateur développe ou écrit son programme d'application pour contrôler son processus. Ce programme d'application est ensuite téléchargé dans le FS-PLC, où il détermine le contrôle du FS-PLC, de l'équipement associé et, par conséquent, du processus de l'utilisateur.

Note 1 à l'article: Les logiciels et programmes d'application peuvent être ou non relatifs à la sécurité.

3.20
équipement commandé
EUC
équipement, machine, appareil ou installation utilisés pour les activités de fabrication, de traitement, de transport, médicales ou d'autres activités

Note 1 à l'article:Le système de commande de l'EUC est séparé et distinct de.l'EUT.

[SOURCE: CEI 61508-4:2010, 3.2.1]

3.21
équipement à l'essai
EUT
configuration(s) représentative(s), définie(s) par le fabricant, utilisée(s) pour les essais de type

3.22
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

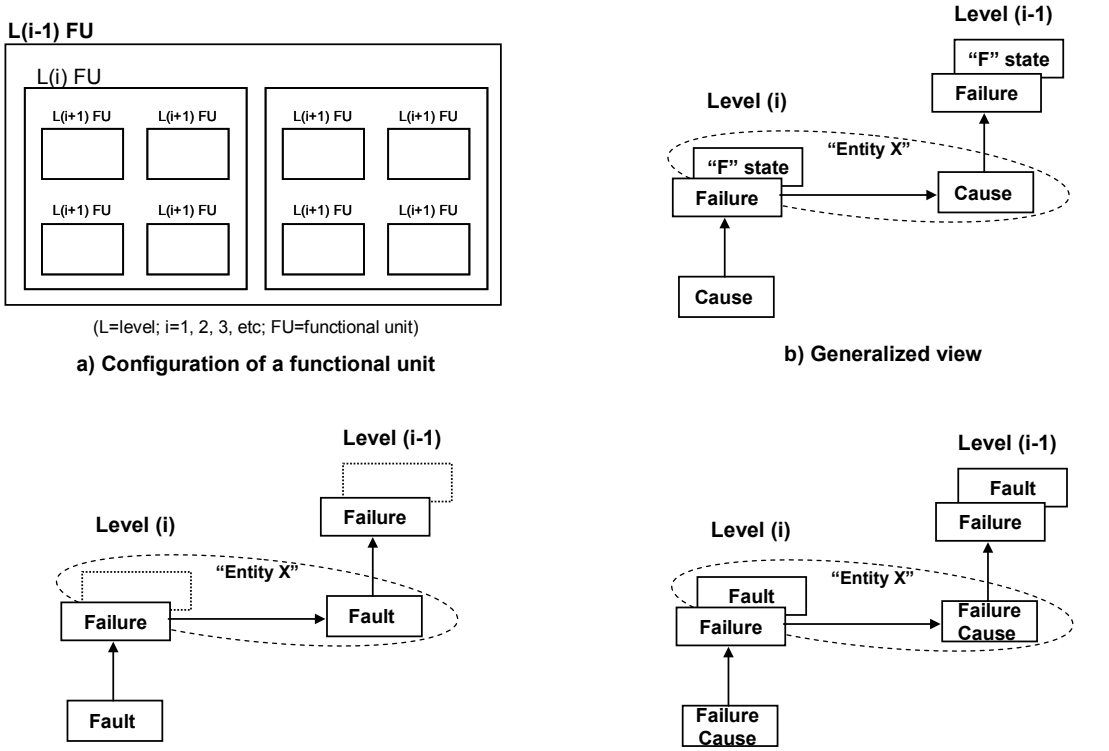
Note 1 à l'article: Cette définition est basée sur la CEI 60050-191:1990, 191-04-01, avec des modifications apportées pour inclure les défaillances systématiques dues, par exemple, à des lacunes dans la spécification ou le logiciel.

VOIR: Figure 2 pour plus d'informations sur la relation entre les pannes et les défaillances.

Note 2 à l'article: L'accomplissement des fonctions requises exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportement à éviter. L'occurrence d'un comportement à éviter est une défaillance.

Note 3 à l'article: Les défaillances sont soit aléatoires (dans le matériel), soit systématiques (dans le logiciel ou le matériel), voir 3.42 et 3.56.

[SOURCE: CEI 61508-4:2010:2010, 3.6.4]



a) Configuration of a functional unit

b) Generalized view

c) From the point of view of IEC 61508 and ISO/IEC 2382-14

d) From the point of view of IEC 60050(191)

Légende

Anglais	Français
L(i-1) FU	N(i-1) UF
L(i) FU	N(i) UF
L(i+1) FU	N(i+1) UF
(L=level; i=1, 2, 3, etc; FU=functional unit)	(N=niveau; i=1, 2, 3, etc; UF=unité fonctionnelle)
a) configuration of a functional unit	a) Configuration d'une unité fonctionnelle
Level(i-1)	Niveau (i-1)
Level (i)	Niveau (i)
"Entity X"	"Entité X"
Level (i-1)	Niveau (i-1)
Failure	Défaillance
Fault	Panne
c) From the point of view of IEC 61508 and ISO/IEC 2382-14	c) Du point de vue de la CEI 61508 et de l'ISO/CEI 2382-14
Level (i-1)	Niveau (i-1)
Level (i)	Niveau (i)
"F" state	Etat "P"
Failure	Défaillance
"Entity X"	"Entité X"
Cause	Cause
b) Generalized view	b) Vue générale
Level (i-1)	Niveau (i-1)
Level (i)	Niveau (i)
Fault	Panne

Anglais	Français
Failure	Défaillance
Failure Cause	Défaillance Cause
d) From the point of view of IEC 60050(191)	d) Du point de vue de la CEI 60050(191)

NOTE 1 Comme indiqué dans a), une unité fonctionnelle peut être vue en tant que composition hiérarchique de plusieurs niveaux, chacun pouvant à son tour être appelé unité fonctionnelle. Dans le niveau (i), une "cause" est susceptible de se manifester comme une erreur (différence par rapport à la valeur ou à l'état approprié) dans l'unité fonctionnelle de ce niveau (i), et, si elle n'est pas corrigée ou contournée, il est possible qu'elle entraîne une défaillance de cette unité fonctionnelle, suite à quoi elle passe en état "P" dans lequel elle n'est plus en mesure d'accomplir la fonction requise (voir b)). Cet état "P" de l'unité fonctionnelle du niveau (i) est à son tour susceptible de se manifester comme une erreur dans l'unité fonctionnelle du niveau (i-1) et, si elle n'est pas corrigée ou contournée, elle peut entraîner une défaillance de l'unité fonctionnelle de ce niveau (i-1).

NOTE 2 Dans cette chaîne de cause à effet, la même chose ("Entité X") peut être vue comme un état (état "P") de l'unité fonctionnelle du niveau (i) auquel elle est passée suite à sa défaillance, et également comme la cause de la défaillance de l'unité fonctionnelle du niveau (i-1). Cette "Entité X" combine le concept de "panne" dans la série CEI 61508 et l'ISO/CEI 2382-14, qui met l'accent sur son aspect de cause comme illustré dans c), et celui de "panne" dans la CEI 60050-191, qui met l'accent sur son aspect d'état comme illustré dans d). L'état "P" est appelé panne dans la CEI 60050-191, mais il n'est pas défini dans la série CEI 61508 et dans l'ISO/CEI 2382-14.

NOTE 3 Dans certains cas, les défaillances ou les erreurs sont susceptibles d'être causées par un événement extérieur tel que la foudre ou le bruit électrostatique, plutôt que par une panne interne. De même, une panne (dans les deux vocabulaires) peut se produire sans défaillance préalable. C'est le cas, par exemple, pour les pannes de conception.

Figure 2 – Modèle de défaillance

3.23
taux de défaillance

paramètre de fiabilité ($\lambda(t)$) d'une entité (composants ou systèmes simples) tel que $\lambda(t).dt$ est la probabilité de défaillance de cette entité comprise dans les limites [$t,\ t+dt$], à condition qu'aucune défaillance ne se soit produite pendant [$0,\ t$]

Note 1 à l'article D'un point de vue mathématique, $\lambda(t)$ est la probabilité conditionnelle de défaillance par unité de temps pendant [$t,\ t+dt$]. Elle est en relation étroite avec la fonction de fiabilité (c'est-à-dire la probabilité d'aucune défaillance de 0 à t) par la formule générale

$R(t) = \exp(-\int_0^t \lambda(\tau) d\tau$. Inversement, elle est définie à partir de la fonction de fiabilité par $\lambda(t) = -\frac{dR(t)}{dt}\frac{1}{R(t)}$.

Note 2 à l'article Les taux de défaillance et leurs incertitudes peuvent être estimés à partir du retour d'exploitation en utilisant les statistiques conventionnelles. Pendant la « durée de vie utile » (c'est-à-dire après le déverminage et avant l'usure), le taux de défaillance d'un article simple est plus ou moins constant, $\lambda(t) \equiv \lambda$.

Note 3 à l'article La moyenne de $\lambda(t)$ pendant une période donnée [0, T], $\lambda_{avg}(T) = (\int_0^T \lambda(\tau) d\tau)/T$, ne représente pas un taux de défaillance car elle ne peut pas être utilisée pour le calcul de R(t) comme indiqué à la Note 1 à l'article. Elle peut toutefois être interprétée comme la fréquence moyenne de défaillance sur cette période (c'est-à-dire la PFH, voir Annexe B de la CEI 61508-6:2010).

Note 4 à l'article Le taux de défaillance d'une série d'articles est la somme des taux de défaillance de chaque article.

Note 5 à l'article Le taux de défaillance de systèmes redondants est généralement non constant. Néanmoins, lorsque toutes les défaillances sont révélées rapidement, sont indépendantes et rapidement réparées, $\lambda(t)$ tend rapidement vers une valeur asymptotique λ_{as} correspondant au taux de défaillance équivalent des systèmes. Il convient de ne pas le confondre avec le taux de défaillance moyen décrit à la Note 3 à l'article qui ne tend pas nécessairement vers une valeur asymptotique.

[SOURCE: CEI 61508-4:2010, 3.6.16]

3.24
panne
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise.
[SOURCE: ISO/CEI 2382-14:1997, 14.01.10]

Note 1 à l'article: La CEI 60050-191:1990, 191-05-01 définit le terme 'fault' (en français «panne») comme un état d'inaptitude à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive, à d'autres actions programmées ou à un manque de ressources extérieures. Voir la Figure 2 pour obtenir une illustration de ces deux points de vue.

[SOURCE: CEI 61508-4:2010, 3.6.1, modifiée]

3.25
tolérance aux pannes
aptitude d'une unité fonctionnelle à continuer à accomplir une fonction requise en cas d'anomalies ou d'erreurs

[SOURCE: ISO/CEI 2382-14:1997, 14.04.06, modifiée]

Note 1 à l'article: La définition de la CEI 60050-191:1990, 191-15-05 ne prend en compte que les pannes de sous entités. Voir la Note 1 à l'article de 3.24.

[SOURCE: CEI 61508-4:2010, 3.6.3]

Note 2 à l'article: Les pannes et les erreurs à prendre en compte incluent celles impliquant les interfaces du FS-PLC.

3.26
spécification des exigences de sécurité fonctionnelle du FS-PLC
spécification contenant les exigences de la fonction de sécurité et de ses niveaux d'intégrité de sécurité associés pour le FS-PLC

3.27
sécurité fonctionnelle
sous-ensemble de la sécurité globale se rapportant à l'EUC et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité et des dispositifs externes de réduction de risque

[SOURCE: CEI 61508-4:2010, 3.1.12]

Note 1 à l'article: La sécurité fonctionnelle est, par essence, l'aptitude d'un système relatif à la sécurité à mettre en place ou à conserver un état de sécurité.

3.28
matériel
dispositifs physiques électriques, mécaniques ou autres du FS-PLC connectés ensemble pour accomplir diverses fonctions

3.29
sous-système très complexe relatif à la sécurité
partie d'un système électrique/électronique/électronique programmable relatif à la sécurité pour lequel:

- le mode de défaillance d'au moins un composant n'est pas correctement défini, ou
- le comportement du sous-système en état de panne ne peut pas être complètement déterminé, ou
- il n'y a pas suffisamment de données de défaillance dans le domaine pour montrer que les taux de défaillances déclarés sont respectés

EXEMPLE Un FS-PLC. Il est issu du sous-système de type B, comme décrit dans la CEI 61508-2:2010, 7.4.4.1.3.

Note 1 à l'article: Se reporter aux systèmes de Type A (9.4.3.2.2) et de Type B (9.4.3.2.3).

3.30
sous-système logique
un sous-système logique est défini comme la partie d'un système électrique/électronique/électronique programmable relatif à la sécurité qui effectue la fonction logique mais exclut les capteurs et les éléments finaux

EXEMPLE Un FS-PLC est un sous-système logique.

3.31
durée moyenne de dépannage
MRT
durée totale de dépannage prévue

Note 1 à l'article: Le MRT comprend les durées (b), (c) et (d) pour les durées applicables à la MTTR (voir 3.34).

[SOURCE: CEI 61508-4:2010, 3.6.22]

3.32
durée moyenne de bon fonctionnement
MTBF
paramètre (généralement exprimé en heures) basé sur des statistiques qui permet de comparer la fiabilité de différents produits

Note 1 à l'article: Mathématiquement, il s'agit de la réciproque du taux de défaillance d'un produit réparable.

Note 2 à l'article: La durée moyenne de bon fonctionnement est une moyenne arithmétique déterminée à partir d'un grand nombre d'unités sur une longue période.

Note 3 à l'article: Pour un produit complexe tel qu'un courant porteur en ligne, le taux de défaillance moyen approche un taux de défaillance constant avec une fonction de fiabilité exponentielle: $R(t) = e^{-\lambda t}$

Note 4 à l'article: MTBF = MTTF + MTTR.

SEE: Note 2 à l'article de 3.33.

3.33
durée moyenne de fonctionnement avant défaillance
MTTF
paramètre (généralement exprimé en heures) basé sur des statistiques qui permet de comparer la fiabilité de différents produits non réparables

Note 1 à l'article: Pour un produit non réparable avec un taux de défaillance constant, la durée moyenne de fonctionnement avant défaillance est la réciproque du taux de défaillance du produit.

Note 2 à l'article: La durée moyenne de fonctionnement avant défaillance est une moyenne arithmétique déterminée à partir d'un grand nombre d'unités sur une longue période.

Note 3 à l'article: Bien que les deux termes "durée moyenne de bon fonctionnement" et "durée moyenne de fonctionnement avant défaillance" soient parfois utilisés indifféremment, ils se réfèrent respectivement à des produits réparables et non réparables. Il convient d'utiliser la durée moyenne de bon fonctionnement uniquement pour les produits qui sont réparés normalement, puis remis en service.

3.34
durée moyenne de rétablissement
MTTR
durée prévue de rétablissement effectif

Note 1 à l'article: La MTTR comprend:

- le temps de détection de la défaillance (a), et
- le temps écoulé avant de commencer la réparation (b), et
- le temps de réparation effectif (c), et
- le temps écoulé avant la remise en fonctionnement du composant (d)

Le temps de démarrage applicable à (b) est la fin du temps (a); le temps de démarrage applicable à (c) est la fin du temps (b) et le temps de démarrage applicable à (d) est la fin du temps (c).

[SOURCE: CEI 61508-4:2010, 3.6.21, modifiée]

3.35
mode de fonctionnement
manière dont fonctionne une fonction de sécurité qui peut être en mode à faible sollicitation, en mode à sollicitation élevée ou en mode continu

Note 1 à l'article: Le système E/E/PE relatif à la sécurité qui réalise la fonction de sécurité n'a généralement pas d'influence sur l'EUC ou son système de commande jusqu'à l'occurrence d'une sollicitation. Cependant, si le système E/E/PE relatif à la sécurité n'est plus en mesure de réaliser la fonction de sécurité du fait d'une défaillance, il peut alors faire passer l'EUC à un état de sécurité (voir 7.4.6 de la CEI 61508-2:2010).

[SOURCE: CEI 61508-4:2010, 3.5.16]

3.35.1
mode à faible sollicitation
où la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et où la fréquence des sollicitations n'est pas supérieure à une par an

[SOURCE: CEI 61508-4:2010, 3.5.16]

3.35.2
mode à sollicitation élevée
où la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et où la fréquence des sollicitations est supérieure à une par an

[SOURCE: CEI 61508-4:2010, 3.5.16]

3.35.3
mode continu
où la fonction de sécurité maintient l'EUC dans un état de sécurité en fonctionnement normal

[SOURCE: CEI 61508-4:2010, 3.5.16]

3.36
M pour N
MooN
architecture composée de "N" canaux indépendants qui sont connectés de façon telle qu'au moins "M" canaux sont requis pour accomplir la fonction de sécurité

3.37
temps de sécurité du processus
cas le plus défavorable
durée entre l'occurrence d'une défaillance, avec potentialité de donner lieu à un événement dangereux, se produisant dans l'EUC ou son système de commande et le temps nécessaire pour accomplir l'action dans l'EUC pour empêcher l'occurrence de l'événement dangereux
[SOURCE: CEI 61508-4:2010, 3.6.20]

3.38
probabilité de défaillance dangereuse à une sollicitation
PFD
indisponibilité de sécurité (voir CEI 60050-191) d'un système E/E/PE relatif à la sécurité pour réaliser la fonction de sécurité spécifiée sur sollicitation de l'EUC ou de son système de commande

Note 1 à l'article L'indisponibilité [instantanée] (selon la CEI 60050-191) est la probabilité qu'un article ne soit pas en mesure de réaliser une fonction requise dans des conditions données à un moment donné, en supposant l'existence des ressources externes requises. Elle est généralement exprimée par U (*t*).

Note 2 à l'article La disponibilité [instantanée] ne dépend pas des états (en fonctionnement ou en défaillance) dans lesquels l'article se trouve avant t. Elle caractérise un article qui doit uniquement être apte à fonctionner lorsqu'il doit le faire, par exemple, un système E/E/PE relatif à la sécurité fonctionnant en mode faible sollicitation.

Note 3 à l'article Si elle est vérifiée périodiquement, la PFD d'un système E/E/PE relatif à la sécurité est, par rapport à la fonction de sécurité spécifiée, représentée par une courbe en dents de scie avec une large gamme de probabilités comprises entre un niveau minimal, juste après un essai, et un niveau maximal, juste avant un essai.

[SOURCE: CEI 61508-4:2010, 3.6.17]

3.39
matériel programmable
matériel pouvant être piloté ou modifié (fonctionnalités ou performances) par un logiciel embarqué

EXEMPLES Les réseaux prédiffusés programmables, les mémoires flash et les produits basés sur des microprocesseurs.

3.40
essai de sûreté
essai périodique
essai périodique destiné à détecter les défaillances dangereuses cachées d'un système relatif à la sécurité de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition « comme neuf » ou dans une condition aussi proche que possible de celle-ci

Note 1 à l'article: L'efficacité de l'essai périodique dépend à la fois de la couverture des défaillances et de l'efficacité de la réparation. Dans la pratique, il n'est pas facile de détecter 100 % des défaillances dangereuses cachées pour des systèmes autres que les systèmes E/E/PE relatifs à la sécurité de faible complexité. Il convient de conserver cet objectif. Au minimum, toutes les fonctions de sécurité qui sont exécutées sont contrôlées selon la spécification des exigences de sécurité des systèmes E/E/PE. Si des canaux séparés sont utilisés, ces essais sont réalisés séparément pour chacun des canaux. Pour des éléments complexes, il peut se révéler nécessaire d'effectuer une analyse pour démontrer que la probabilité de défaillance dangereuse cachée non détectée par des essais périodiques est négligeable pendant toute la durée de vie du système E/E/PE relatif à la sécurité.

Note 2 à l'article: La réalisation d'un essai périodique nécessite un certain temps. Pendant ce temps, le système E/E/PE relatif à la sécurité peut être inhibé en totalité ou en partie. La durée de l'essai périodique peut ne pas être prise en compte uniquement si la partie du système E/E/PE relatif à la sécurité soumise à l'essai reste disponible, en cas de sollicitation de fonctionnement ou si l'EUC est arrêté pendant l'essai.

Note 3 à l'article: Pendant un essai périodique, le système E/E/PE relatif à la sécurité peut être indisponible, en totalité ou en partie, pour réagir à une sollicitation de fonctionnement. La MTTR (durée moyenne de réparation) peut ne pas être prise en compte pour les calculs de SIL uniquement si l'EUC est arrêté pendant la réparation ou si les dispositifs externes de réduction de risque sont installés et présentent une efficacité équivalente.

[SOURCE: CEI 61508-4:2010, 3.8.5]

3.41
procédure de vérification de bon fonctionnement
PVBF
méthodologie d'essai d'un FS-PLC

3.42
défaillance aléatoire du matériel
défaillance survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel

Note 1 à l'article: Il existe de nombreux mécanismes de dégradation se produisant à des fréquences différentes dans divers composants et, puisque les tolérances de fabrication ont pour conséquence une défaillance des composants causée par ces mécanismes après des durées de fonctionnement inégales, les défaillances survenant dans un équipement comprenant plusieurs composants surviennent à des fréquences prévisibles, mais à des instants imprévisibles (c'est-à-dire aléatoires)..

Note 2 à l'article: L'une des différences majeures entre les défaillances aléatoires du matériel et les défaillances systématiques (voir 3.56) est que les taux de défaillance du système (ou d'autres mesures appropriées), générés par les défaillances aléatoires du matériel, peuvent être prédits avec une précision raisonnablement fiable, alors que les défaillances systématiques, de par leur nature même, ne peuvent être prédites avec précision. C'est-à-dire que les taux de défaillance du système issus des défaillances aléatoires du matériel peuvent être quantifiés de manière assez fiable, mais que ceux issus des défaillances systématiques ne peuvent être quantifiés de manière statistique avec précision du fait que les événements à leur origine ne peuvent être facilement prédits.

[SOURCE: CEI 61508-4:2010, 3.6.5]

3.43
fiabilité
probabilité qu'un produit spécifique fonctionne pendant une durée/période (*t*) spécifique sans défaillance

Note 1 à l'article: Pour un produit complexe tel qu'un automate programmable, le taux de défaillance moyen approche un taux de défaillance constant avec une fonction de fiabilité exponentielle: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 à l'article: Si la durée (*t*) de la dernière équation correspond à la durée moyenne de bon fonctionnement, l'équation présente une fiabilité de 0,368, ce qui signifie que seuls 36,8 % d'un produit spécifique fonctionneront sans défaillance pendant la durée moyenne de bon fonctionnement.

3.44
risque
combinaison de la probabilité d'un dommage et de sa gravité

[SOURCE: Guide ISO/CEI 51:1999, définition 3.2]

Note 1 à l'article: Pour plus de détails sur ce concept, voir l'Annexe A de la CEI 61508-5:2010.

[SOURCE: CEI 61508-4:2010, 3.1.6]

3.45
défaillance en sécurité
FS-PLC
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la fonction de sécurité qui:

a) conduit au fonctionnement parasite de la fonction de sécurité avec la potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité, ou

b) augmente la probabilité du fonctionnement parasite de la fonction de sécurité avec potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité

[SOURCE: CEI 61508-4:2010, 3.6.8]

3.46
panne sécurisée
panne ne pouvant pas entraîner de défaillance dangereuse

3.47
taux de défaillance non dangereuse
SFF
propriété d'un élément relatif à la sécurité définie par le rapport des taux de défaillance moyens des défaillances en sécurité et dangereuses détectées et des défaillances en sécurité et dangereuses

Note 1 à l'article: Ce rapport est représenté par l'équation suivante:

$$SFF = (\Sigma\lambda_{Savg} + \Sigma\lambda_{Ddavg})/(\Sigma\lambda_{Savg} + \Sigma\lambda_{Ddavg} + \Sigma\lambda_{Duavg})$$

lorsque les taux de défaillance sont basés sur des taux de défaillance constants, l'équation peut être simplifiée comme suit:

$$SFF = (\Sigma\lambda_{S} + \Sigma\lambda_{Dd})/(\Sigma\lambda_{S} + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

[SOURCE: CEI 61508-4:2010, 3.6.15, modifiée]

3.48
état de sécurité
état de l'EUC lorsque la sécurité est réalisée

Note 1 à l'article Pendant son évolution depuis un état potentiellement dangereux vers un état de sécurité final, l'EUC est susceptible de passer par un certain nombre d'états de sécurité intermédiaires. Dans certaines situations, l'état de sécurité n'est atteint que durant le temps où l'EUC est continuellement commandé. Cette commande continuée peut s'étendre sur une période courte ou indéfinie.

[SOURCE: CEI 61508-4:2010, 3.1.13, modifiée]

3.49
temps de réponse de la fonction de sécurité
dans le cas le plus défavorable, temps écoulé suite à l'activation d'un capteur de sécurité, avant que ne soit atteint l'état de sécurité correspondant de son (ses) actionneur(s) de sécurité, du fait d'erreurs ou de défaillances avérées sur le canal de la fonction de sécurité.

[SOURCE: CEI 61784-3:2010, 3.1.1.36, modifiée]

3.50
intégrité de sécurité
probabilité pour qu'un système E/E/PE relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité spécifiées dans toutes les conditions énoncées et dans une période de temps spécifiée

Note 1 à l'article: Plus le niveau d'intégrité de sécurité d'un système relatif à la sécurité est élevé, plus la probabilité d'une défaillance du système dans l'exécution des fonctions de sécurité spécifiées ou dans l'adoption d'un état spécifié lorsque requis est faible.

Note 2 à l'article: Il existe quatre niveaux d'intégrité de sécurité (voir la CEI 61508-4:2010, 3.5.8).

Note 3 à l'article: Il convient que l'évaluation de l'intégrité de sécurité prenne en compte toutes les causes de défaillance (à la fois les défaillances aléatoires du matériel et les défaillances systématiques) conduisant à un état de non-sécurité, par exemple les défaillances de matériel, les défaillances induites du logiciel et les défaillances dues aux perturbations électriques. Certaines de ces défaillances, en particulier les défaillances aléatoires du matériel, peuvent être quantifiées à l'aide de mesures telles que la fréquence moyenne de défaillance en mode de défaillance dangereux, ou la probabilité de non fonctionnement en cas de sollicitation d'un système de protection relatif à la sécurité. Cependant, l'intégrité de sécurité dépend également de plusieurs facteurs qui ne peuvent être précisément quantifiés, mais simplement considérés d'un point de vue qualitatif..

Note 4 à l'article: L'intégrité de sécurité comprend l'intégrité de sécurité du matériel (voir la CEI 61508-4:2010, 3.5.7) et l'intégrité de sécurité systématique (voir la CEI 61508-4:2010, 3.5.6).

Note 5 à l'article: Cette définition est centrée sur la fiabilité des systèmes relatifs à la sécurité dans l'exécution des fonctions de sécurité (voir CEI 60050-191:1990, 191-12-01 pour une définition de la fiabilité).

[SOURCE: CEI 61508-4:2010, 3.5.4]

3.51
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

Note 1 à l'article: Les objectifs chiffrés de défaillance (voir CEI 61508-4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de la CEI 61508-1:2010.

Note 2 à l'article: Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité.

Note 3 à l'article: Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "Système relatif à la sécurité à SIL *n*" (où *n* est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge les fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à *n*..

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

Note 6 à l'article: Ce schéma de spécification s'applique uniquement au système relatif à la sécurité.

Note 7 à l'article: Les mesures de défaillance cible des quatre niveaux d'intégrité de sécurité sont spécifiées dans le Tableau 1 et le Tableau 2 de cette partie.

3.52
niveau d'intégrité de sécurité maximal
niveau d'intégrité de sécurité maximal pouvant être atteint par un FS-PLC en fonction des contraintes architecturales et de l'intégrité de sécurité systématique

[SOURCE: adapté de la CEI 62061:2005, 3.2.24]

3.53
système relatif à la sécurité
système désigné qui, à la fois,

– met en œuvre les fonctions de sécurité requises pour atteindre ou maintenir un état de sécurité de l'EUC et
– est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/PE relatifs à la sécurité, et aux dispositifs externes de réduction de risque, l'intégrité de sécurité nécessaire pour les fonctions de sécurité requises

Note 1 à l'article: Ce terme fait référence aux systèmes désignés comme systèmes relatifs à la sécurité qui, avec les dispositifs externes de réduction de risque (voir CEI 61508-4:2010, 3.4.2), sont destinés à réaliser la réduction de risque nécessaire, afin de satisfaire au niveau de risque tolérable requis (voir 61508-4:2010, 3.1.7). Voir également l'Annexe A de la CEI 61508-5:2010.

Note 2 à l'article: Les systèmes relatifs à la sécurité sont conçus pour empêcher l'EUC d'entrer dans un état dangereux en prenant les mesures appropriées dès la réception de la commande. La défaillance d'un système relatif à la sécurité serait incluse dans les événements à l'origine du ou des dangers déterminés. Bien qu'il puisse exister d'autres systèmes possédant des fonctions de sécurité, ce sont les systèmes relatifs à la sécurité qui ont été choisis pour obtenir à leur façon le niveau de risque tolérable requis. Les systèmes relatifs à la sécurité peuvent globalement être répartis en systèmes relatifs à la sécurité de commande et en systèmes relatifs à la sécurité de protection.

Note 3 à l'article: Les systèmes relatifs à la sécurité peuvent faire partie intégrante du système de commande de l'EUC ou peuvent être interfacés avec l'EUC par l'intermédiaire de capteurs et/ou d'actionneurs. Cela signifie qu'il est possible d'atteindre le niveau d'intégrité de sécurité requis en mettant en œuvre les fonctions de sécurité dans le système de commande de l'EUC (et éventuellement également par l'adjonction de systèmes séparés et indépendants) ou que ces fonctions de sécurité peuvent être exécutées par des systèmes séparés et indépendants dédiés à la sécurité.

Note 8 à l'article: Un système relatif à la sécurité peut

a) être conçu pour prévenir un événement dangereux (c'est-à-dire qu'aucun événement dangereux ne survient tant que les systèmes relatifs à la sécurité exécutent leurs fonctions de sécurité),
b) être conçu pour réduire les effets de l'événement préjudiciable, réduisant ainsi le risque en limitant les conséquences de ce risque,
c) être conçu pour réaliser une combinaison de a) e de b).

Note 5 à l'article: Une personne peut faire partie d'un système relatif à la sécurité (voir la 61508-4:2010, 3.4.1). Par exemple, une personne peut recevoir des informations d'un dispositif électronique programmable et exécuter une activité de sécurité à partir de cette information, ou exécuter une activité de sécurité par l'intermédiaire d'un dispositif électronique programmable.

Note 6 à l'article: Un système relatif à la sécurité recouvre l'ensemble des matériels, logiciels, ainsi que tous les équipements annexes (par exemple, alimentation) nécessaires pour exécuter la fonction de sécurité spécifiée (les capteurs, les autres dispositifs d'entrée, les éléments terminaux (actionneurs) ainsi que les autres dispositifs de sortie sont par conséquent compris dans le système relatif à la sécurité).

Note 7 à l'article: Un système relatif à la sécurité peut être basé sur une large gamme de technologies, comprenant les technologies électrique, électronique, électronique programmable, hydraulique et pneumatique.

[SOURCE: CEI 61508-4:2010, 3.4.1]

3.54
logiciel
création intellectuelle comprenant les programmes, les procédures, les données, les règles et toute la documentation associée afférente au fonctionnement du système de traitement des données

Note 1 à l'article: Le logiciel est indépendant du support sur lequel il est enregistré.

Note 2 à l'article: Cette définition, sans la Note à l'article 1, est différente de celle de l'ISO/CEI 2382-1 (voir bibliographie), et la définition complète est différente de celle de l'ISO 9000-3, avec l'ajout du mot données.

[SOURCE: CEI 61508-4:2010, 3.2.5]

3.55
sous-système
partie d'un FS-PLC comprenant un composant unique ou un ensemble de composants, réalisant une ou plusieurs fonctions

Note 1 à l'article: Dans la présente partie, le terme «sous-système» est utilisé différemment que dans la définition de la CEI 61508-4.

3.56
défaillance systématique
défaillance liée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

[SOURCE: CEI 60050-191:1990, 191-04-19]

Note 1 à l'article: Une maintenance corrective, sans modification, n'élimine généralement pas la cause d'une défaillance.

Note 2 à l'article: Une défaillance systématique peut être induite en simulant la cause de la défaillance.

EXEMPLES Les causes de défaillances systématiques peuvent, par exemple, inclure des erreurs humaines dans

– la spécification des exigences de sécurité fonctionnelle;

– la conception, la fabrication, l'installation, le fonctionnement du matériel;

– la conception, l'implémentation, etc. du logiciel.

Note 3 à l'article: Dans la présente norme, les défaillances d'un système relatif à la sécurité sont classées en défaillances aléatoires du matériel (voir 3.6.5) ou en défaillances systématiques.

[SOURCE: CEI 61508-4:2010, 3.6.6]

3.57
durée de fonctionnement utile
cas le plus défavorable
temps minimum écoulé entre l'installation du FS-PLC et le moment où les taux de défaillance des composants du FS-PLC ne peuvent plus être prédits avec une quelconque précision

EXEMPLE Par exemple, le moment où les calculs de facteurs bêta initiaux définis dans la CEI 61508-6:2010, Annexe D ne sont plus valables.

3.58
validation
confirmation, par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique prévu sont satisfaites

Note 1 à l'article: Adapté de l'ISO 8402, à l'exception des notes.

Note 2 à l'article: La présente norme spécifie trois phases de validation:

– validation de sécurité générale (voir Figure 2 de la CEI 61508-1:2010),

– validation des systèmes E/E/PE (voir Figure 3 de la CEI 61508-1:2010),

– validation du logiciel (voir Figure 4 de la CEI 61508-1:2010).

Note 3 à l'article: La validation est l'activité qui consiste à démontrer que le système relatif à la sécurité considéré, avant ou après installation, correspond en tout point aux exigences de sécurité fonctionnelles contenues dans la spécification de ce système relatif à la sécurité. Ainsi, par exemple, la validation du logiciel consiste en la confirmation, par examen et apport de preuves tangibles, que le logiciel répond à la spécification des exigences de sécurité du logiciel.

[SOURCE: CEI 61508-4:2010, 3.8.2]

3.59
vérification
confirmation, par examen et apport de preuves tangibles, que les exigences ont été satisfaites

Note 1 à l'article: Adapté de l'ISO 8402, à l'exception des notes.

Note 2 à l'article: Dans le contexte de la présente norme, la vérification est l'activité qui consiste, pour chaque phase du cycle de vie de sécurité correspondant (général, FS-PLC), à démontrer par analyse, raisonnement mathématique et/ou essais que, pour les entrées spécifiques, les éléments livrables remplissent en tout point les objectifs et les exigences fixés pour la phase spécifique.

EXEMPLE Les activités de vérification incluent

– les revues relatives aux sorties d'une phase (documents concernant toutes les phases du cycle de vie de sécurité) destinées à assurer la conformité aux objectifs et aux exigences de la phase, en tenant compte des entrées spécifiques à cette phase,
– les revues de conception,
– les essais réalisés sur les produits conçus afin d'assurer que leur fonctionnement est conforme à leur spécification,
– les essais d'intégration réalisés lors de l'assemblage, élément par élément, de différentes parties d'un système et la réalisation d'essais d'environnement afin de s'assurer que toutes les parties fonctionnent les unes avec les autres conformément aux spécifications.

[SOURCE: CEI 61508-4:2010, 3.8.1]

Note 3 à l'article: Dans la présente norme, la phase de vérification inclut toutes les activités associées au développement du FS-PLC et à la preuve que le FS-PLC développé remplit sa spécification.

4 Conformité à la présente norme

La présente partie intègre les exigences spécifiques au produit des CEI 61508-1, CEI 61508-2 et CEI 61508-3. Bien que la série CEI 61508 soit une norme système, cette partie fournit des exigences spécifiques au produit avec des informations plus précises pour l'application des principes de la série CEI 61508 relative à un FS-PLC.

La conformité à la présente norme est uniquement applicable lorsqu'un automate programmable et ses périphériques associés, comme défini dans la CEI 61131-1, sont conçus pour être utilisés en tant que sous-système logique d'un système électrique/électronique/électronique programmable relatif à la sécurité et sont identifiés comme automate programmable de sécurité fonctionnelle (FS-PLC). Ces FS-PLC peuvent également inclure des éléments logiciels, par exemple des blocs de fonctions prédéfinis.

Pour se conformer à la présente norme, il doit être démontré que les exigences relatives à la sécurité fonctionnelle de chaque article et paragraphe de cette partie sont satisfaites.

Un FS-PLC doit d'abord répondre aux exigences applicables de la Partie 2 avant d'être ugé conforme à cette partie. Il n'existe aucune exigence équivalente pour la conformité à la Partie 3.

La conformité à ces articles et paragraphes est de la responsabilité du fabricant du FS-PLC.

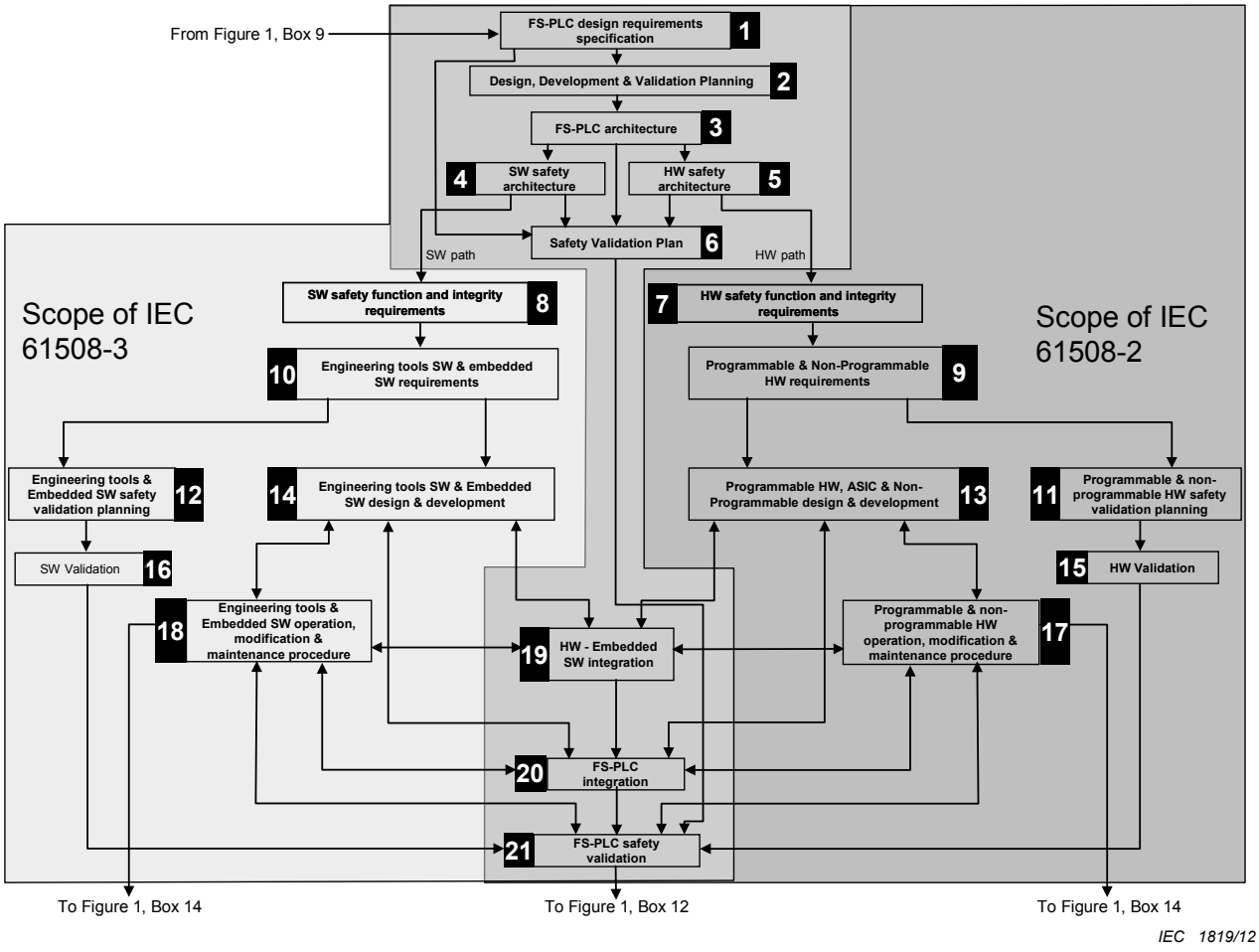
5 Cycle de vie de sécurité du FS-PLC

5.1 Généralités

Afin de gérer de manière systématique toutes les activités nécessaires à la réalisation de la ou des fonctions logiques requises pour le FS-PLC et de répondre au niveau d'intégrité de

sécurité maximal pour le FS-PLC, le 5.1 adopte en tant qu'infrastructure technique un cycle de vie de sécurité pour le FS-PLC, voir la Figure 3.

La Figure 3 est basée sur les Figures 2, 3 et 4 de la CEI 61508-1:2010, les Figures 2 et 4 de la CEI 61508-2:2010 et les Figures 2, 3, 4 et 5 de la CEI 61508-3:2010.



IEC 1819/12

Légende

Anglais	Français
From Figure1, Box 9	A partir de la Figure 1, case 9
FS-PLC design requirements specification	Spécification des exigences de conception du FS-PLC
Design, Development & Validation Planning	Planification de la conception, du développement et de la validation
FS-PLC architecture	Architecture du FS-PLC
SW safety architecture	Architecture de sécurité logicielle
HW safety architecture	Architecture de sécurité matérielle
SW path	Branche logicielle
Safety Validation Plan	Plan de validation de la sécurité
HW path	Branche matérielle
Scope of IEC 61508-3	Domaine d'application de la CEI 61508-3
SW safety function and integrity requirements	Exigences d'intégrité et fonction de sécurité logicielle
HW safety function and integrity requirements	Exigences d'intégrité et fonction de sécurité matérielle
Scope of IEC 61508-2	Domaine d'application de la CEI 61508-2

Anglais	Français
Engineering tools SW & embedded SW requirements	Outils d'ingénierie logiciel et exigences du logiciel embarqué
SW Validation	Validation du logiciel
Programmable & Non-Programmable HW requirements	Exigences matérielles programmables et non programmables
Engineering tools SW & Embedded SW design & development	Outils d'ingénierie logiciel et conception et développement du logiciel embarqué
Engineering tools & Embedded SW safety validation planning	Outils d'ingénierie et planification de la validation de la sécurité du logiciel embarqué
Engineering tools & Embedded SW operation, modification & maintenance procedure	Outils d'ingénierie et procédures de fonctionnement, de modification et de maintenance du logiciel intégré
HW-Embedded SW integration	Installation du logiciel embarqué dans le matériel
FS-PLC integration	Intégration du FS-PLC
Programmable & Non-Programmable HW requirements	Exigences pour les matériels programmables et non programmables
Programmable HW, ASIC & Non-Programmable design & development	Conception et développement du matériel programmable et non programmable et des circuits intégrés spécifiques
Programmable & non-programmable HW safety validation planning	Planification de la validation de la sécurité du matériel programmable et non programmable
HW Validation	Validation du matériel
Programmable & non-programmable HW operation, modification & maintenance procedure	Procédures de fonctionnement, de modification et de maintenance du matériel programmable et non programmable
FS-PLC safety validation	Validation de la sécurité du FS-PLC
To Figure 1, Box 14	Vers la Figure 1, case 14
To Figure 1, Box 12	Vers la Figure 1, case 12
To Figure 1, Box 14	Vers la Figure 1, case 14

NOTE 1 Les références "A partir de la Figure 1 ou Vers la Figure 1 case 9, 12 ou 14" correspondent à la Figure 1 de cette partie.

NOTE 2 Cette figure décrit les tâches caractéristiques associées au développement d'un FS-PLC. Elle ne représente pas une procédure pas à pas fixe du développement d'un FS-PLC.

Figure 3 – Cycle de vie de sécurité du FS-PLC (en phase de réalisation)

Pour toutes les phases du cycle de vie de sécurité du FS-PLC, présentées dans la Figure 3, les Articles 5 à 16 définissent les exigences pour le FS-PLC, conformément à la CEI 61508-2 et à la CEI 61508-3. La Figure 3 diffère quelque peu des figures source de la CEI 61508-1, de la CEI 61508-2 et de la CEI 61508-3, pas en substance, mais pour apporter certaines clarifications et distinctions.

Les exigences des Articles 5 à 16 incluent toutes les spécifications des exigences de sécurité du FS-PLC: le matériel (y compris circuits intégrés spécifiques, FPGA, etc.) et le logiciel. La Figure 3 représente le flux des décisions architecturales du FS-PLC prises et les exigences sont ensuite divisées entre les spécifications des exigences de sécurité matérielles du FS-PLC et les spécifications des exigences de sécurité logicielle du FS-PLC.

En ce qui concerne la partie logicielle du FS-PLC, deux types de tâches logicielles sont présentées (outils d'ingénierie et logiciel intégré). Même si ces deux tâches sont considérées comme logicielles, il existe des différences distinctes en matière d'impact et de relation au développement matériel, aux outils, aux méthodes, etc.

En ce qui concerne la partie matérielle du FS-PLC, trois types de tâches matérielles sont présentées (matériel programmable, circuits intégrés spécifiques et matériel non programmable). Même si ces trois tâches sont considérées comme matérielles, il existe des différences distinctes en matière d'impact et de relation avec le développement logiciel, aux outils, aux méthodes, etc.

Les cases 17, 18, 19 et 20 de la Figure 3 illustrent une intégration progressive des pièces logicielles et matérielles du FS-PLC.

Le premier niveau d'intégration intervient entre le matériel programmable et le logiciel embarqué sur le matériel. Cela est clairement démontré dans les figures source de la CEI 61508.

Le deuxième niveau d'intégration intervient lorsque toutes les parties du FS-PLC sont disponibles; le matériel programmable et son logiciel embarqué, le matériel non programmable et les outils d'ingénierie. Bien qu'implicite dans les figures source de la CEI 61508; cela est expliqué dans la Figure 3.

La validation de la sécurité du FS-PLC peut uniquement être effectuée après ce deuxième niveau d'intégration.

5.2 Exigences du niveau d'intégrité de sécurité fonctionnelle du FS-PLC

5.2.1 Généralités

Avant de débuter la phase de réalisation, la sécurité fonctionnelle et les exigences d'intégrité de sécurité, définissant les fonctions logiques du FS-PLC et leurs niveaux d'intégrité de sécurité, doivent être définies. Ensuite, il faut allouer la sécurité fonctionnelle et les exigences du niveau d'intégrité de sécurité au matériel, au logiciel ou aux deux. Cela conduit à des exigences détaillées pour le matériel et le logiciel, tel que spécifié dans les Articles 9 et 10, respectivement.

Les phases du cycle de vie matériel et logiciel appliquées dans cette partie sont les suivantes:

- Spécification des exigences de conception du FS-PLC [case 1 de la Figure 3; Article 6]
- Planification de la conception, du développement et de la validation [case 2 de la Figure 3; Article 7]
- Architecture du FS-PLC [case 3 de la Figure 3; Article 8]
- Architecture de sécurité logicielle [case 4 de la Figure 3]
- Architecture de sécurité matérielle [case 5 de la Figure 3]
- Plan de validation de la sécurité [case 6 de la Figure 3; Article 11]
- Exigences d'intégrité et fonction de sécurité matérielle [case 7 de la Figure 3]
- Exigences d'intégrité et fonction de sécurité logicielle [case 8 de la Figure 3]
- Exigences matérielles programmables et non programmables [case 9 de la Figure 3]
- Outils d’ingénieries logiciel et exigences du logiciel embarqué [case 10 de la Figure 3; Paragraphe 10.3]
- Planification de la validation de la sécurité du matériel programmable et non programmable [case 11 de la Figure 3]
- Outils d’ingénieries et de planification de la validation de la sécurité du logiciel embarqué [case 12 de la Figure 3; Paragraphe 10.4]
- Conception et développement du matériel programmable et non programmable [case 13 de la Figure 3]

- Outils d'ingénieries logiciel et conception et développement du logiciel embarqué [case 14 de la Figure 3; Article 10]
- Validation du matériel [case 15 de la Figure 3; Paragraphe 9.7]
- Validation du logiciel [case 16 de la Figure 3]
- Procédures de fonctionnement et de modification du matériel programmable et non programmable [case 17 de la Figure 3; Article 15]
- Outils d'ingénieries et procédures de fonctionnement et de modification du logiciel embarqué [case 18 de la Figure 3]
- Intégration du logiciel embarqué dans le matériel [case 19 de la Figure 3; Paragraphe 9.5]
- Intégration du FS-PLC [case 20 de la Figure 3]
- Validation de la sécurité du FS-PLC [case 21 de la Figure 3; Article 11]

5.2.2 Sécurité des données

5.2.2.1 Généralités

L'analyse des dangers et des menaces sécuritaires est normalement nécessaire afin que les applications relatives à la sécurité protègent des attaques intentionnelles et les modifications involontaires. La sécurité peut être appliquée via la mise en place de mesures et de politiques de sécurité appropriées, telles que des mesures physiques (par exemple, mécaniques ou électroniques) ou organisationnelles.

Lorsque les communications relatives à la sécurité font partie du FS-PLC, il existe une possibilité de modification involontaire des paramètres des dispositifs du réseau. Les dispositifs de communication relatifs à la sécurité doivent disposer de protections contre les modifications involontaires.

Lorsqu'elles sont applicables, les exigences relatives à la sécurité globale, définies dans la CEI 62443, doivent être respectées.

5.2.2.2 Hypothèses de sécurité pour la garantie de la sécurité fonctionnelle et du niveau d'intégrité de sécurité maximal

Il est recommandé que la politique de sécurité de base pour le ou les environnements de sécurité du FS-PLC, en fonction de la complexité de l'équipement, traite les services de sécurité suivants:

- contrôles d'accès logique vers, et entre, le FS-PLC, y compris les interfaces homme-machine. Ces contrôles logiques sont restreints à une communauté spécifique d'utilisateurs, autorisée à gérer l'accès à un ou plusieurs des dispositifs. En général, l'accès logique est restreint à un petit groupe d'utilisateurs qui installent, entretiennent et administrent ces services et autorisent, en fonction du rôle, l'accès, la modification et/ou l'utilisation des informations spécifiées.
- contrôles de gestion afin que, dans un environnement de sécurité spécifique, il y ait une approche commune de la gestion et de l'administration de la politique de sécurité, avec une seule autorité ayant toutes les responsabilités.
- contrôles physiques afin de limiter l'accès non autorisé au FS-PLC (y compris les matériels de sauvegarde, le câblage, les connexions).

Le cas échéant, le fabricant du FS-PLC doit fournir des indications concernant la manière dont ils doivent être mis en œuvre.

Sur la base de l'analyse des dangers et des menaces sécuritaires, des mesures appropriées doivent être appliquées. Par exemple:

a) contrôle des écritures de communication,

b) accès mécanique ou logique par interrupteur à clé,

c) directives permettant de limiter l'accès physique, par exemple au moyen d'enceintes verrouillées,

d) directives concernant l'accès limité via les réseaux,

e) protection intégrale du mot de passe,

f) indicateurs d'effraction,

g) détection et suivi de la gestion des modifications.

5.3 Système de gestion de la qualité

Un système de gestion de la qualité doit être utilisé pour le développement et la fabrication des FS-PLC. Il doit:

- être une condition préalable à la conception, au développement et à la fabrication du matériel (y compris circuits intégrés spécifiques, FPGA, etc.) / logiciel du FS-PLC,
- décrire les exigences pour les processus de développement et de fabrication du matériel (y compris circuits intégrés spécifiques, FPGA, etc.) / logiciel,
- garantir que les FS-PLC sont conformes aux exigences définies dans la présente norme et dans toutes les normes de référence,
- assurer une bonne documentation des résultats du développement et de l'essai du matériel (y compris circuits intégrés spécifiques, FPGA, etc.) / logiciel,
- garantir des étapes de développement et de fabrication du matériel (y compris circuits intégrés spécifiques, FPGA, etc.) / logiciel,
- inclure des systèmes de gestion des modifications/contrôle de révision et de gestion de la configuration.

NOTE Un exemple d'exigences pour un système de gestion de la qualité est décrit dans l'ISO 9001.

5.4 Gestion du cycle de vie de sécurité du FS-PLC

5.4.1 Objectifs

Le premier objectif des exigences de 5.4 est de spécifier les responsabilités dans la gestion de la sécurité fonctionnelle de chaque personne responsable d'un FS-PLC, ou d'une ou plusieurs phases d'un système FS-PLC et des cycles de vie des logiciels de sécurité.

Le deuxième objectif des exigences de 5.4 est de spécifier les activités que les responsables de la gestion de la sécurité fonctionnelle doivent effectuer.

NOTE Les mesures organisationnelles traitées en 5.4 concernent l'implémentation effective des exigences techniques et portent uniquement sur la mise en place et la maintenance de la sécurité fonctionnelle du FS-PLC. Les exigences techniques nécessaires à la maintenance de la sécurité fonctionnelle sont spécifiées dans les informations fournies par le fabricant. Voir Article 16.

5.4.2 Exigences et procédures

5.4.2.1 Exigences

5.4.2.1.1 Généralités

Une organisation ayant des responsabilités en matière de réalisation d'un FS-PLC, ou concernant une ou plusieurs phases du cycle de vie de sécurité global, du système FS-PLC ou du logiciel, doit désigner une ou plusieurs personnes en charge de gérer toutes les responsabilités pour:

- le FS-PLC et les différentes phases de son cycle de vie;
- coordonner les activités relatives à la sécurité effectuées au cours de ces phases;

- les interfaces entre ces phases et les autres phases réalisées par d'autres organisations;
- accomplir les exigences de 5.4.2.1.2 à 5.4.2.1.11 et 5.4.2.2.2;
- coordonner les évaluations de la sécurité fonctionnelle (voir 5.4.2.1.11 b) et Article 14) – en particulier lorsqu'elles diffèrent d'une phase à l'autre – y compris communiquer, planifier et intégrer la documentation, les jugements et les recommandations;
- s'assurer que la sécurité fonctionnelle est réalisée et démontrée conformément aux objectifs et aux exigences de la présente norme.

NOTE Il est permis de déléguer les responsabilités en matière d'activités relatives à la sécurité, ou des phases du cycle de vie de sécurité, à d'autres personnes, en particulier celles nécessitant une certaine expertise. Cependant, il faut déléguer cette responsabilité à une ou peu de personnes ayant une autorité de gestion suffisante.

5.4.2.1.2 Politique et stratégie de mise en place de la sécurité fonctionnelle

La politique et la stratégie de mise en place de la sécurité fonctionnelle doivent être spécifiées, ainsi que les moyens d'évaluer leur mise en place et les moyens pour les transmettre au sein de l'organisation.

5.4.2.1.3 Identification des responsabilités

Tous les services, personnes et organisations responsables de la réalisation d'activités au cours des phases du cycle de vie de sécurité global, du système FS-PLC ou du logiciel (y compris les personnes responsables de la vérification et de l'évaluation de la sécurité fonctionnelle et, le cas échéant, les autorités responsables des licences ou les organismes de réglementation de la sécurité) doivent être identifiés, et leurs responsabilités doivent leur être entièrement et clairement communiquées.

5.4.2.1.4 Communication des informations

Des procédures doivent être développées pour définir le type d'informations à communiquer entre les parties concernées et la mise en place de cette communication.

NOTE Voir l'Article 5 de la CEI 61508-1:2010 pour obtenir les exigences concernant la documentation.

5.4.2.1.5 Suivi

Des procédures doivent être développées pour assurer un suivi rapide et une résolution satisfaisante des recommandations relatives au FS-PLC, y compris celles provenant:

a) de l'évaluation de la sécurité fonctionnelle (voir Article 14);
b) des activités de vérification (voir Article 13);
c) des activités de validation (voir Article 11);
d) de la gestion de la configuration (voir Article 15).

5.4.2.1.6 Analyse des défaillances sur le terrain et des informations utilisateur

Des procédures doivent être développées pour l'analyse des défaillances sur le terrain et des informations utilisateur disponibles, y compris:

- la reconnaissance des pannes systématiques pouvant menacer la sécurité fonctionnelle;
- l'évaluation des taux de défaillance au cours du fonctionnement et de la maintenance afin de vérifier s'ils sont conformes aux exigences spécifiées lors de la définition du domaine d’application global des phases du cycle de vie.

5.4.2.1.7 Audits internes de qualité

Des exigences pour les audits internes périodiques de qualité des processus de conception et de fabrication du FS-PLC doivent être spécifiées, y compris:

a) la fréquence des audits internes de qualité;

b) le niveau d'indépendance des personnes qui mènent les audits;

c) la documentation nécessaire, les actions correctives et les activités de suivi.

5.4.2.1.8 Modification

Des procédures doivent être développées pour:

a) initier les modifications du FS-PLC;

b) obtenir l'approbation et l'autorisation pour les modifications.

5.4.2.1.9 Conservation des informations

Des procédures doivent être développées pour la conservation d'informations précises sur les pannes et les défaillances du FS-PLC.

5.4.2.1.10 Gestion de la configuration

Des procédures doivent être développées pour la gestion de la configuration du FS-PLC, y compris, en particulier:

a) le point, selon les phases spécifiques, auquel le contrôle de configuration formel doit être implémenté,

b) les procédures à utiliser pour identifier uniquement toutes les parties constituantes d'un élément (matériel et logiciel),

c) les procédures de prévention contre l'entrée d'éléments non autorisés dans le service.

5.4.2.1.11 Gestion de configuration logicielle

Des procédures doivent être développées pour la gestion de configuration logicielle des FS-PLC au cours des phases appropriées du cycle de vie de sécurité des FS-PLC; les éléments suivants doivent particulièrement être spécifiés:

a) les contrôles administratifs et techniques tout au long du cycle de vie de la sécurité fonctionnelle du logiciel, afin de gérer les modifications logicielles et, par conséquent, s'assurer que les exigences spécifiées pour la sécurité fonctionnelle du logiciel continuent d'être satisfaites,

b) une garantie que toutes les opérations nécessaires ont été effectuées pour démontrer que l'intégrité de sécurité fonctionnelle requise du logiciel a été respectée,

c) un moyen de conserver précisément, avec une identification unique, tous les éléments de configuration nécessaires pour répondre aux exigences d'intégrité de sécurité du FS-PLC,

d) les éléments de configuration, y compris au moins les suivants:

- exigences et analyse de la sécurité fonctionnelle,
- spécification logicielle et documents de conception,
- modules du code source du logiciel,
- plans d'essais et résultats,
- logiciels et packages logiciels préexistants à intégrer dans le FS-PLC,
- tous les outils et environnements de développement utilisés pour créer, soumettre aux essais ou accomplir des actions sur le logiciel du FS-PLC.

e) les procédures de contrôle des modifications:

- pour empêcher les modifications non autorisées,

- pour documenter les demandes de modification,
- pour analyser l'impact d'une modification proposée,
- pour approuver ou rejeter la demande de modification;
- pour documenter les détails et l'autorisation de toutes les modifications approuvées,
- pour établir une configuration de base aux points appropriés dans le développement du logiciel,
- pour documenter l'essai d'intégration (partiel) qui justifie les bases et
- pour garantir la composition et l'élaboration de toutes les bases logicielles (y compris la récupération de bases précédentes).

L'autorité et la décision de gestion sont nécessaires pour indiquer et appliquer l'utilisation de contrôles administratifs et techniques.

f) une procédure qui garantit que les méthodes appropriées sont implémentées pour charger le logiciel d'application et des données dans le FS-PLC,

Les systèmes de localisation cible spécifiques et les systèmes généraux sont à prendre en considération si possible.

g) la documentation des informations suivantes pour autoriser un audit de configuration ultérieur:
   - statut de la configuration,
   - statut de la version,
   - justification et approbation de toutes les modifications,
   - détails de la modification.

h) la documentation formelle de la version du logiciel relatif à la sécurité fonctionnelle. Des copies originales du logiciel ainsi que toute la documentation associée et la version des données en service doivent être conservées afin de documenter la maintenance et la modification tout au long de la vie opérationnelle du logiciel.

NOTE Pour plus d'informations sur la gestion de la configuration, voir l'ISO/CEI 12207, l'IEEE 828-2005, l'IEEE 1042-1987.

5.4.2.2 Gestion de la sécurité fonctionnelle par les individus

5.4.2.2.1 Individus et spécification des activités

Les personnes responsables d'une ou de plusieurs phases du système FS-PLC ou des cycles de vie de sécurité logicielle doivent, selon les phases dont ils sont responsables et conformément aux procédures définies en 5.4.2.1, et ses paragraphes, spécifier toutes les activités techniques et la gestion nécessaire pour garantir la réalisation, l'évaluation et la maintenance de la sécurité fonctionnelle du FS-PLC, y compris:

a) les techniques et mesures sélectionnées utilisées pour répondre aux exigences d'un article ou d'un paragraphe spécifié;

b) les activités d'évaluation de la sécurité fonctionnelle, et la manière dont la mise en place de cette sécurité sera expliquée à ceux qui effectueront son évaluation (voir Article 14);

Les procédures appropriées pour l'évaluation de la sécurité fonctionnelle doivent être utilisées afin de définir

- la sélection d'une organisation appropriée, ou d'une ou de plusieurs personnes, au niveau d'indépendance nécessaire;
- l'élaboration, et l'acceptation des modifications, aux termes de référence pour l'évaluation de la sécurité fonctionnelle;
- le remplacement des personnes effectuant l'évaluation de la sécurité fonctionnelle à tout moment au cours du cycle de vie d'un système;

- la résolution des conflits impliquant les personnes effectuant les évaluations de la sécurité fonctionnelle.

5.4.2.2.2 Procédures et individus

Des procédures doivent être disponibles pour garantir que toutes les personnes ayant des responsabilités définies conformément à 5.4.2.1 et 5.4.2.1.3 (c'est-à-dire toutes les personnes impliquées dans les activités du cycle de vie du logiciel ou du système FS-PLC, y compris les activités de vérification, de gestion de la sécurité fonctionnelle et de l'évaluation de la sécurité fonctionnelle) aient les compétences appropriées (c'est-à-dire la formation, les connaissances techniques, l'expérience et les qualifications) pour les tâches spécifiques qu'elles doivent effectuer. Ces procédures doivent inclure les exigences pour l'actualisation, la mise à jour et l'évaluation continue des compétences.

5.4.2.2.3 Compétence et individus

La pertinence des compétences doit être considérée conforme à l'application spécifique, en prenant en considération tous les facteurs appropriés, y compris:

a) les responsabilités de la personne;

b) le niveau de surveillance exigé;

c) les niveaux d'intégrité de sécurité du FS-PLC – plus le niveau d'intégrité de sécurité est élevé, plus la spécification des compétences doit être rigoureuse;

d) la nouveauté de la conception, des procédures de conception ou de l'application – plus elles sont nouvelles ou non soumises à essai, plus la spécification des compétences doit être rigoureuse;

e) les expériences précédentes et leur pertinence face aux tâches spécifiques à effectuer et la technologie utilisée – plus les compétences requises sont importantes, plus la correspondance doit être proche entre les compétences développées au cours d'expériences précédentes et celles requises pour les activités spécifiques à accomplir;

f) le type de compétences appropriées aux circonstances (par exemple, les qualifications, l'expérience, les formations pertinentes et la pratique successive, et les aptitudes à diriger du personnel et à prendre des décisions);

g) les connaissances techniques appropriées au domaine d'application et à la technologie;

h) les connaissances techniques appropriées à la technologie en matière de sécurité;

i) les connaissances du cadre légal et réglementaire en matière de sécurité;

j) la pertinence des qualifications face aux activités spécifiques à effectuer.

Les compétences de toutes les personnes ayant des responsabilités définies conformément à 5.4.2.1 et 5.4.2.1.3 doivent être documentées.

5.4.2.3 Fournisseurs

Les fournisseurs distribuant des produits ou des services à une organisation ayant toute la responsabilité du FS-PLC ou des cycles de vie de sécurité du logiciel (voir 5.4.2.1), doivent fournir leurs produits ou services tels que spécifiés par cette organisation et avoir un système de gestion de la qualité approprié.

Les fournisseurs doivent disposer d'un système de gestion de la qualité et en outre d'un système approprié de gestion de la sécurité.

5.4.2.4 Planification de la sécurité fonctionnelle du logiciel

La planification de la sécurité fonctionnelle doit définir la stratégie pour l'obtention, le développement, l'intégration, la vérification, la validation et la modification du logiciel dans la mesure exigée par le niveau d'intégrité de sécurité des fonctions de sécurité implémentées par le FS-PLC.

NOTE 1 La philosophie de cette approche est d'utiliser la planification de la sécurité fonctionnelle comme opportunité pour personnaliser la présente norme de manière à prendre en compte l'intégrité de sécurité requise pour chaque fonction de sécurité implémentée par le FS-PLC.

Lorsque le logiciel est conçu pour implémenter des fonctions de sécurité du FS-PLC de différents niveaux d'intégrité de sécurité, tous les logiciels doivent être traités comme appartenant au plus haut niveau d'intégrité de sécurité, sauf si une indépendance appropriée entre les fonctions de sécurité du FS-PLC des différents niveaux d'intégrité de sécurité peut être montrée dans l'implémentation. La justification de l'indépendance doit être documentée.

NOTE 2 Voir la CEI 61508-3:2010, 6.2.2 pour consulter des rubriques complémentaires.

5.4.3 Exécution et surveillance

Les activités spécifiées suite à 5.4.2 et ses paragraphes doivent être implémentées et surveillées.

5.4.4 Gestion de la sécurité fonctionnelle

Les activités relatives à la gestion de la sécurité fonctionnelle doivent être appliquées aux phases appropriées du cycle de vie de sécurité du FS-PLC et du logiciel conformément au niveau d'intégrité de sécurité souhaité et à la CEI 61508.

6 Spécification des exigences de conception du FS-PLC

6.1 Généralités

Le premier objectif de cette phase est de distribuer la sécurité fonctionnelle et les exigences d'intégrité de sécurité du FS-PLC, contenues dans la spécification des exigences de conception. Il s'agit des exigences d'intégrité et de sécurité fonctionnelle du FS-PLC du système électrique/électronique/électronique programmable relatif à la sécurité pour la ou les applications visées.

Le deuxième objectif de cette phase est d'allouer un niveau d'intégrité de sécurité au FS-PLC, selon la fonction désignée du système électrique/électronique/électronique programmable relatif à la sécurité que le FS-PLC est censé fournir (conception et spécification).

6.2 Contenu de la spécification des exigences de conception

La spécification des exigences de conception du FS-PLC doit contenir:

a) la fourniture d'une ou plusieurs exigences de sécurité relatives au matériel, au logiciel ou à une combinaison des deux avec des détails suffisants pour la conception et le développement du FS-PLC,

   NOTE 1 Parmi les exemples de fonctions de sécurité du FS-PLC, on peut citer le placement d'une sortie en état de sécurité, comme défini par le fabricant, ou le maintien d'un état de sécurité défini par fabricant.

b) le niveau d'intégrité de sécurité maximal souhaité pour le FS-PLC;

c) la spécification de l'état ou des états de sécurité du FS-PLC;

d) la spécification des limites de fonctionnement du FS-PLC en modes de fonctionnement faible sollicitation et sollicitation élevée/continue;

   NOTE 2 Lorsque le FS-PLC est utilisé dans différentes configurations, différentes limites de niveau d'intégrité de sécurité peuvent s'appliquer aux différentes configurations.

e) une description de toutes les mesures et techniques nécessaires à la mise en place de la sécurité fonctionnelle requise. La description doit inclure:

   1) le temps nécessaire à un FS-PLC pour traiter un ou des signaux externes afin d'activer une ou des fonctions spécifiées; par exemple, fonction de sécurité du FS-PLC sous conditions normales et défaillantes, entrée-sortie, calcul à fournir à

une sortie, écriture externe d'une sortie, communications sur le réseau, performances;

NOTE 3 Le temps de réponse le plus défavorable pour la fonction de sécurité du FS-PLC contribue au temps de réponse le plus défavorable de la fonction de sécurité de l'ensemble du système électrique/électronique/électronique programmable relatif à la sécurité. Voir CEI 61784-3.

2) toutes les informations relatives à la sécurité fonctionnelle pouvant avoir une influence sur la conception du système électrique/électronique/électronique programmable relatif à la sécurité;

3) toutes les interfaces avec le FS-PLC;

4) les essais de diagnostic de panne externes;

NOTE 4 Par exemple, la détection des charges ouvertes ou en court-circuit dans le cas d'une décharge pour les sorties numériques.

5) tous les modes de fonctionnement pertinents du FS-PLC;

6) tous les modes de comportement requis des FS-PLC – en particulier, le comportement relatif à la détection des pannes;

7) la signification de toutes les interactions matérielles/logicielles – le cas échéant, toutes les contraintes requises entre le matériel et le logiciel doivent être identifiées et documentées;

NOTE 5 Lorsque ces interactions ne sont pas connues avant la fin de la conception, seules des contraintes générales sont fixées.

8) les conditions de contrainte et de limitation pour les FS-PLC et les sous-systèmes associés, par exemple les contraintes de temps;

9) toute exigence spécifique relative aux procédures de démarrage et de redémarrage des FS-PLC;

10) les taux de défaillance aléatoire du matériel cible pour chaque effet de défaillance à prendre en compte lors de l'analyse de l'effet et du mode de défaillance;

11) toutes les exigences, contraintes, fonctions et installations pour effectuer des essais de sûreté sur la partie FS-PLC du système électrique/électronique/électronique programmable relatif à la sécurité à mettre en place;

NOTE 6 En général, l'intervalle d'essai de sûreté pour un FS-PLC est la durée de fonctionnement utile.

12) les limites d'immunité électromagnétique et les critères de performances, conformément aux exigences de 12.5;

NOTE 7 Selon l'accord entre le fabricant et l'utilisateur du FS-PLC, des limites plus élevées sont utilisées pour certaines applications, par exemple des applications de rideaux de lumière conformément à la CEI 61496-1.

13) les exigences pour le contrôle des erreurs sur des communications numériques relatives à la sécurité externe;

14) les mesures à mettre en place pour restreindre l'utilisation par des personnes non autorisées (interrupteurs à clé, armoires verrouillées, accès réseau, mots de passe, etc.);

15) événements et alarmes critiques indépendants de l'application, par exemple dégradation du système, dépassement du balayage, redémarrage après panne d'alimentation;

16) cybersécurité – le fabricant spécifie si le FS-PLC peut être connecté à un réseau non sécurisé ainsi que toutes les mesures spécifiques nécessaires à la cybersécurité;

NOTE 8 Pour obtenir des indications concernant l'analyse des risques de sécurité, voir la série CEI 62443.

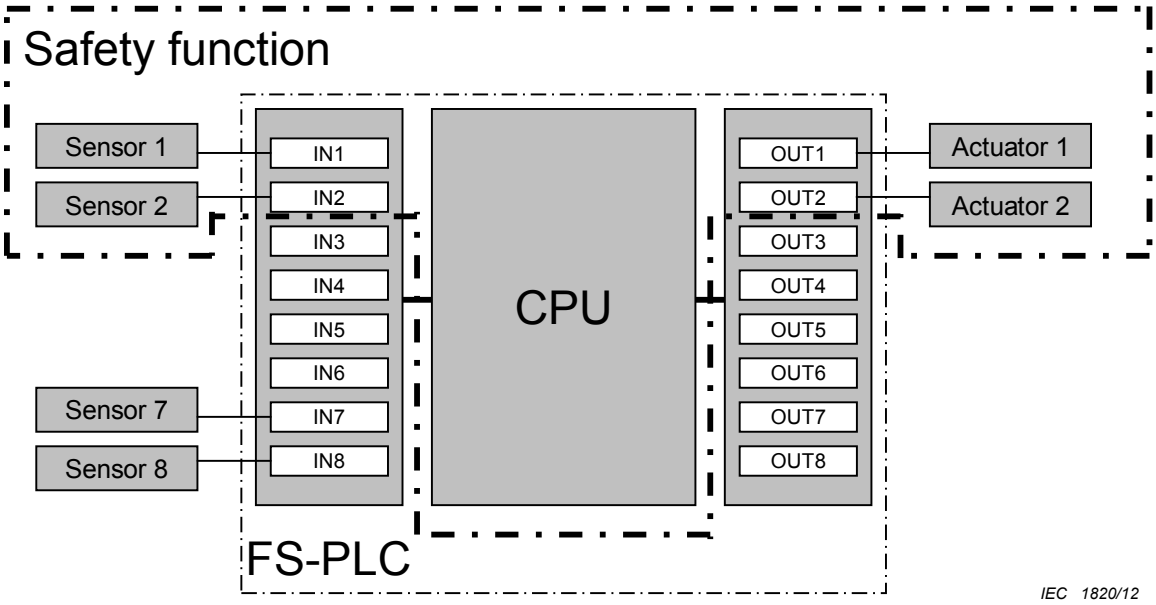
17) une description de l'HMI, des bibliothèques, des outils d'ingénierie, etc. relatifs à la sécurité;

18) les mesures d'assurance qualité/contrôle qualité en place;

19) les techniques et les mesures du Tableau B.1 de la CEI 61508-2:2010 qui sont utilisées.

6.3 Taux de défaillance ciblé

Selon le niveau d'intégrité de sécurité ciblé pour le FS-PLC et son mode de demande, une PFD (voir le Tableau 1) ou une PFH (voir le Tableau 2) du FS-PLC est déterminée.



Légende

Anglais	Français
Safety function	Fonction de sécurité
Sensor 1	Capteur 1
Sensor 2	Capteur 2
IN1	IN1
IN2	IN2
IN3	IN3
IN4	IN4
IN5	IN5
IN6	IN6
IN7	IN7
IN8	IN8
OUT1	OUT1
OUT2	OUT2
OUT3	OUT3
OUT4	OUT4
OUT5	OUT5
OUT6	OUT6
OUT7	OUT7
OUT8	OUT8
CPU	UC
Actuator 1	Actionneur 1

Anglais	Français
Actuator 2	Actionneur 2
Sensor 7	Capteur 7
Sensor 8	Capteur 8
FS-PLC	FS-PLC

Figure 4 – Parties appropriées d'une fonction de sécurité

Les parties appropriées d'une fonction de sécurité sont illustrées à la Figure 4.

Tableau 1 – Niveaux d'intégrité de sécurité pour un mode de fonctionnement à faible sollicitation

Niveau d'intégrité de sécurité d'un système relatif à la sécurité	PFD de la fonction de sécurité	PFD de la contribution du FS-PLC
4[a]	$\geq 10^{-5}$ à $< 10^{-4}$	$< k\ 10^{-4}$
3	$\geq 10^{-4}$ à $< 10^{-3}$	$< k\ 10^{-3}$
2	$\geq 10^{-3}$ à $< 10^{-2}$	$< k\ 10^{-2}$
1	$\geq 10^{-2}$ à $< 10^{-1}$	$< k\ 10^{-1}$
NOTE En général, $0 < k < 0{,}15$		
[a] Cette partie s'applique à un FS-PLC ayant un niveau d'intégrité de sécurité maximal inférieur ou égal à SIL 3. Pour le niveau d'intégrité de sécurité maximal SIL 4, des exigences supplémentaires de la série CEI 61508 doivent être appliquées pour la fonction de sécurité du FS-PLC.		

Tableau 2 – Niveaux d'intégrité de sécurité pour un mode de fonctionnement à sollicitation élevée/continue

Niveau d'intégrité de sécurité d'un système relatif à la sécurité	PFH de la fonction de sécurité	PFH de la contribution du FS-PLC
4[a]	$\geq 10^{-9}$ à $< 10^{-8}$	$< k\ 10^{-8}$
3	$\geq 10^{-8}$ à $< 10^{-7}$	$< k\ 10^{-7}$
2	$\geq 10^{-7}$ à $< 10^{-6}$	$< k\ 10^{-6}$
1	$\geq 10^{-6}$ à $< 10^{-5}$	$< k\ 10^{-5}$
NOTE En général, $0 < k < 0{,}15$		
[a] Cette partie s'applique à un FS-PLC ayant un niveau d'intégrité de sécurité inférieur ou égal à SIL 3. Pour le niveau d'intégrité de sécurité SIL 4, des exigences supplémentaires de la série CEI 61508 doivent être appliquées pour la fonction de sécurité du FS-PLC.		

L'exigence d'intégrité de sécurité pour le FS-PLC doit être spécifiée en termes de PFD ou de PFH, uniquement pour les défaillances aléatoires du matériel. Lorsque l'exigence d'intégrité de sécurité est spécifiée en termes de PFD, l'intervalle d'essai de sûreté nécessaire pour calculer cette PFD doit également être défini.

NOTE La PFD ou la PFH d'un système relatif à la sécurité est la somme des valeurs de la PFD ou de la PFH pour les capteurs, le sous-système logique et les actionneurs en tant que partie d'une fonction de sécurité. Pour consulter une illustration, voir Figure 4.

Les défaillances systématiques d'un FS-PLC doivent être résolues grâce aux techniques et mesures mentionnées en 9.4.6.

L'allocation de cette PFD ou PFH du FS-PLC doit être spécifiée par le fabricant du FS-PLC. Il est recommandé que cette allocation soit inférieure ou égale à 15 % (un facteur "*k*" de 0,15

dans les tableaux ci-dessus) de la PFD ou PFH du système électrique/électronique/électronique programmable relatif à la sécurité.

L'objectif est de permettre l'allocation du reste de la PFD ou de la PFH aux capteurs et aux actionneurs.

Une allocation supérieure à un niveau de 15 % pour le FS-PLC est autorisée sur la base d'une analyse plus rigoureuse de l'application et un accord entre le fabricant et le contrôleur indépendant, avec consultation de l'utilisateur.

Les exigences d'intégrité de sécurité et ces exigences de la fonction de sécurité du FS-PLC, pour la fonction du système électrique/électronique/électronique programmable relatif à la sécurité que le FS-PLC est censé fournir, doivent être documentées dans la spécification des exigences de conception du FS-PLC.

7 Planification de la conception, du développement et de la validation du FS-PLC

7.1 Généralités

Les exigences d'intégrité de sécurité et les exigences de la fonction de sécurité du FS-PLC, pour la fonction du système électrique/électronique/électronique programmable relatif à la sécurité que le FS-PLC est censé fournir, et spécifiées à l'Article 6, doivent être planifiées.

7.2 Exigences de segmentation

L'objectif de cette phase est de segmenter les exigences d'intégrité et de sécurité fonctionnelle système du FS-PLC en exigences d'intégrité et de sécurité fonctionnelle logicielles et en exigences d'intégrité et de sécurité fonctionnelle matérielles conformément à l'architecture documentée sélectionnée.

Après le partage des exigences d'intégrité et de sécurité fonctionnelle système du FS-PLC en:

- exigences d'intégrité et de sécurité fonctionnelle logicielle,
- exigences d'intégrité et de sécurité fonctionnelle matérielle, et
- documentation des plans d'évaluation.

Les Articles 9 et 10 définissent la partie matériel du FS-PLC (en phase de réalisation) et le logiciel du FS-PLC (en phase de réalisation).

Un plan de développement doit inclure un plan d'évaluation et un ensemble de plans de conception relatifs au matériel et au logiciel concernant les éléments appropriés de l'Annexe B de la CEI 61508-2:2010.

8 Architecture du FS-PLC

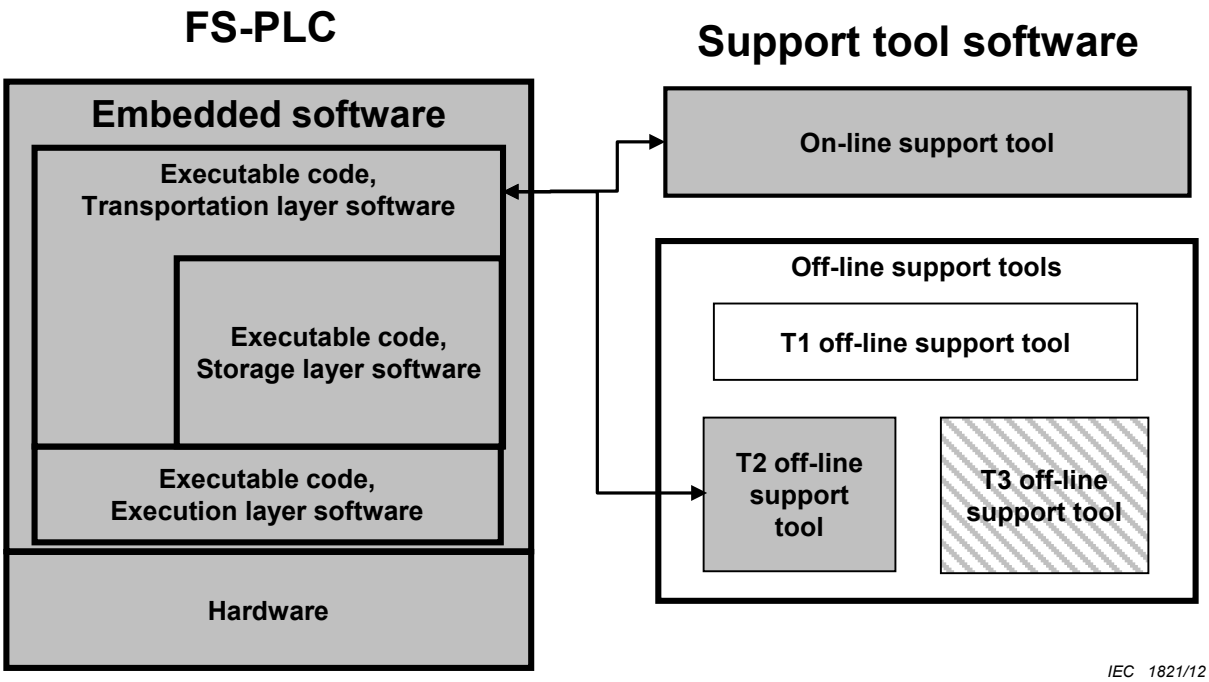
8.1 Généralités

L'objectif de l'Article 8 est de spécifier l'architecture de sécurité matérielle et logicielle du FS-PLC.

Selon la spécification des exigences de sécurité fonctionnelle système du FS-PLC, plusieurs architectures peuvent être évaluées afin de répondre aux besoins définis précédemment dans la spécification des exigences de sécurité fonctionnelle. Des compromis seront faits pour déterminer et définir où et comment seront exécutées les fonctions de sécurité requises du

FS-PLC. Ces décisions définiront ensuite l'ensemble de l'architecture du FS-PLC ainsi que les architectures matérielles et logicielles sous-jacentes.

Les exigences architecturales matérielles et logicielles doivent être documentées respectivement dans les documents d'exigences de sécurité fonctionnelle matérielle et logicielle.



Légende

Anglais	Français
Support tool software	Logiciel de l'outil de prise en charge
Embedded software	Logiciel embarqué
Executable code, transportation layer software	Code exécutable, logiciel de la couche de transport
Executable code, storage layer software	Code exécutable, logiciel de la couche de stockage
Executable code, execution layer software	Code exécutable, logiciel de la couche d'exécution
Hardware	Matériel
On-line support tool	Outil de prise en charge en ligne
Off-line support tools	Outil de prise en charge hors ligne
T1 off-line support tool	Outil de prise en charge hors ligne T1
T2 off-line support tool	Outil de prise en charge hors ligne T2
T3 off-line support tool	Outil de prise en charge hors ligne T3

Figure 5 – Relation entre le FS-PLC et les outils d'ingénierie

Les blocs gris, à la Figure 5, sont des domaines associés au FS-PLC et doivent être traités. Le bloc blanc n'est pas une partie relative à la sécurité du FS-PLC, c'est-à-dire sans interférence. Le bloc rayé indique la possibilité que cet élément soit considéré comme relatif à la sécurité en fonction de l'analyse de criticité. Si ce dernier est relatif à la sécurité, il doit être traité.

Les éléments figurant dans l'exemple, à la Figure 5, dans les blocs blancs et rayés sont donnés uniquement à titre d'illustration et peuvent ou non être déterminés comme relatifs à la sécurité dans l'application.

8.2 Architectures et sous-systèmes

Les sous-systèmes du FS-PLC peuvent comporter plusieurs architectures.

Le FS-PLC doit utiliser une architecture MooN composée de N canaux, pouvant tous contribuer au traitement de la fonction logique du FS-PLC. Au moins M canaux sont requis pour accomplir la fonction logique du FS-PLC. Le système exécute la fonction logique du FS-PLC si M canaux fonctionnent correctement. (N-M) définit la tolérance aux pannes du système, où les défaillances du canal (N-M+1) entraînent la défaillance de la fonction logique du FS-PLC. Voir l'Annexe B pour obtenir des exemples.

8.3 Communication de données

Un système FS-PLC possède généralement deux types de communications de données. L'un est la communication relative à la sécurité, et l'autre est la communication non relative à la sécurité.

La communication relative à la sécurité fonctionnelle utilisant des réseaux de terrain doit être conforme à la CEI 61784-3.

La communication relative à la sécurité utilisant d'autres réseaux que les réseaux de terrain doit être conforme à l'exigence de la CEI 61508-2:2010, 7.4.11.

Pour la communication non relative à la sécurité, se reporter à la CEI 61131-2.

Des mesures doivent être prises pour empêcher les communications de données prévisibles, valides ou non valides, a) d'affecter négativement le bon fonctionnement d'une fonction relative à la sécurité, ou b) d'éviter la conservation ou la mise en place d'un état de sécurité défini.

9 Planification de la conception, du développement et de la validation du matériel

9.1 Exigences matérielles générales

Les exigences de 8.3 sont issues des exigences matérielles spécifiques contenues dans la spécification des exigences de sécurité fonctionnelle du FS-PLC.

9.2 Spécification des exigences de sécurité fonctionnelle du matériel

Les exigences de sécurité fonctionnelle matérielles du FS-PLC doivent être telles que spécifiées dans et/ou issues de la spécification des exigences de sécurité fonctionnelle du FS-PLC.

Lorsque des fonctions non relatives à la sécurité sont accomplies dans le même FS-PLC que les fonctions relatives à la sécurité, des mesures appropriées doivent être mises en place pour empêcher les fonctions relatives à la sécurité d'être affectées négativement par les fonctions non relatives à la sécurité.

Les exigences de sécurité fonctionnelle matérielles du FS-PLC doivent être exprimées et structurées de manière à être:

- claires, précises, sans équivoque, vérifiables, évaluables par des essais, conservables et réalisables; et

- écrites pour faciliter la compréhension par les personnes susceptibles d'utiliser les informations à toutes les étapes du cycle de vie de sécurité du FS-PLC.

9.3 Planification de la validation de la sécurité matérielle

NOTE Cette phase du cycle de vie d'un FS-PLC est généralement accomplie parallèlement aux phases de conception et de développement du matériel, voir 9.4.

La planification de la validation du matériel est réalisée grâce à la spécification des étapes à effectuer pour démontrer la conformité à la spécification des exigences de sécurité fonctionnelle matérielles du FS-PLC (voir l'Article 6).

Le plan de validation de la sécurité fonctionnelle doit inclure les procédures à suivre pour s'assurer que chaque fonction de sécurité est correctement implémentée et a le niveau d'intégrité de sécurité maximal exigé, une description des paramètres d'essai et de l'environnement d'essai et les critères de succès/d'échec.

Les essais de type sont spécifiés à l'Article 12.

9.4 Conception et développement du matériel

9.4.1 Généralités

Le FS-PLC doit être conçu de manière à répondre aux exigences des spécifications des exigences de sécurité fonctionnelle matérielles.

Le matériel conçu et la documentation écrite au cours des phases de conception et de documentation du cycle de vie du FS-PLC doivent répondre à tous les éléments suivants:

a) les exigences relatives au niveau d'intégrité de sécurité maximal du matériel (SIL 1, 2 ou 3) basées sur la tolérance aux pannes matérielles et le taux de défaillance non dangereuse (Route 1_H de 7.4.4 et 7.4.4.2 de la CEI 61508-2:2010), y compris,
   - les contraintes architecturales sur l'intégrité de sécurité du matériel de 9.4.3, 9.4.3.1.2 et
   - les exigences sur la probabilité de défaillances matérielles dangereuses de 9.4.3.2.4;

b) les exigences sur l'intégrité de sécurité systématique, y compris,
   - les exigences sur la prévention des défaillances systématiques de 9.4.5, et
   - les exigences sur le contrôle des défaillances systématiques de 9.4.6.

c) les exigences sur le comportement du FS-PLC en matière de détection de panne de 9.4.2.

d) l'indépendance des fonctions relatives et non relatives à la sécurité à moins que tout le matériel du FS-PLC soit traité par rapport à la sécurité. L'indépendance doit être telle que les défaillances des parties non sécurisées ne doivent pas entraîner de défaillances dangereuses dans la partie sécurisée. La méthode de réalisation de cette indépendance et la justification de la méthode doivent être documentées.

9.4.2 Exigences pour le comportement du FS-PLC en matière de détection d'une panne

La détection d'une panne dangereuse au cours du fonctionnement du FS-PLC doit entraîner:

a) le passage de toutes les sorties, par des mesures intégrées, par exemple matériel ou logiciel embarqué, pouvant être affectées par la panne dans un état de sécurité défini dans le temps de réaction spécifié par le fabricant, ou

b) la notification (alarme) de la panne aux mesures d'application, par exemple au programme d'application, dans le temps de réaction spécifié par le fabricant de sorte que les mesures d'application, par exemple le programme d'application, puissent mettre en place l'action appropriée pour maintenir la sécurité.

NOTE L'action appropriée dépend de l'application et est déterminée par l'utilisateur et non par le fabricant du FS-PLC.

Au minimum, les pannes présentées dans le Tableau 3 doivent être détectées et notifiées (alarme) dans le programme d'application, sauf si

- la panne ne peut pas se produire dans le FS-PLC par conception, ou
- l'omission de la panne est justifiée par une évaluation technique écrite.

Tableau 3 – Pannes à détecter et à notifier (alarme) au programme d'application

Pannes à détecter et à notifier (alarme) au programme d'application
dépassement du temps de balayage – le temps de balayage est supérieur à la valeur maximale prédéfinie
les points d'entrée ou de sortie sont désactivés ou les contournements de maintenance sont en place
la détection des pannes est désactivée
condition de dépassement de température
défaillance d'un diagnostic à exécuter
tentative d'accès en écriture via un canal non autorisé
modes opérationnels du système dégradés – les modules/canaux redondants sont hors ligne ou en panne
perte du système ou de l'alimentation, y compris les sources redondantes
perte ou retard des communications externes relatives à la sécurité
division par zéro ou autre erreur logique détectée

9.4.3 Intégrité de sécurité du matériel

9.4.3.1 Tolérance aux pannes matérielles

9.4.3.1.1 Généralités

Lors de la conception du FS-PLC, la tolérance aux pannes matérielles relatives à la sécurité fonctionnelle doit être définie. La tolérance aux pannes matérielles, associée au taux de défaillance non dangereuse, permet la spécification de l'intégrité de sécurité (SIL 1, 2 ou 3) pouvant être déclarée conformément à Route 1_H, tel que décrit dans la CEI 61508-2.

9.4.3.1.2 Plus haut niveau d'intégrité de sécurité pouvant être déclaré

Dans le cadre de l'intégrité de sécurité matérielle, le plus haut niveau d'intégrité de sécurité pouvant être déclaré pour la fonction de sécurité est limité par la tolérance aux pannes matérielles et par le taux de défaillance non dangereuse des sous-systèmes accomplissant cette fonction de sécurité. Le Tableau 4 et le Tableau 5 spécifient le plus haut niveau d'intégrité de sécurité pouvant être déclaré pour une fonction de sécurité d'un FS-PLC utilisant un sous-système qui prend en compte la tolérance aux pannes matérielles et le taux de défaillance non dangereuse de ce sous-système. Les exigences du Tableau 4 et du Tableau 5 doivent être appliquées à chaque sous-système accomplissant une fonction de sécurité d'un FS-PLC et donc chaque partie du FS-PLC. Les Paragraphes 9.4.3.2.2 à 9.4.3.2.4 indiquent lequel du Tableau 4 ou du Tableau 5 s'applique à un sous-système spécifique. Les Paragraphes 9.4.3.2.5 et 9.4.3.2.6 spécifient d'où est dérivé le plus haut niveau d'intégrité de sécurité pouvant être déclaré pour une fonction de sécurité du FS-PLC. Conformément à ces exigences:

a) une tolérance aux pannes matérielles de N signifie que N+1 pannes pourraient entraîner une perte de la fonction de sécurité du FS-PLC. Lors de la détermination de la tolérance aux pannes matérielles, il ne doit être tenu aucun compte des autres mesures pouvant contrôler les effets des pannes, telles que les diagnostics, et

b) lorsqu'une panne mène directement à l'apparition d'une ou de plusieurs autres pannes, ces dernières sont considérées comme une panne unique;

c) lors de la détermination de la tolérance aux pannes matérielles, certaines pannes peuvent être exclues, selon le comportement physique du mode de défaillance dominant du composant. De telles exclusions de pannes doivent être justifiées et documentées;

NOTE 1 L'ISO 13849-2:2003 donne des exemples d'exclusions de pannes en fonction des différentes technologies.

d) le taux de défaillance non dangereuse d'un sous-système est défini par le rapport du taux moyen des défaillances non dangereuses plus les défaillances dangereuses du sous-système détectées sur le taux de défaillance moyen total du sous-système.

NOTE 2 Les contraintes architecturales ont été incluses afin de mettre en place une architecture suffisamment solide, en prenant en considération le niveau de complexité du sous-système. Le niveau d'intégrité de sécurité matérielle du système FS-PLC, issu de l'application de ces exigences, est le maximum autorisé à être déclaré même si, dans certains cas, un plus haut niveau d'intégrité de sécurité pourrait théoriquement être dérivé si une approche exclusivement mathématique était adoptée pour le système FS-PLC.

NOTE 3 L'architecture et le sous-système dérivés pour répondre aux exigences de tolérance aux pannes matérielles sont ceux utilisés dans les conditions de fonctionnement spécifiées. Les exigences de tolérance aux pannes peuvent être assouplies lorsque le système FS-PLC est réparé en ligne. Cependant, les paramètres clés relatifs à tout assouplissement doivent avoir préalablement été évalués (par exemple, durée moyenne de rétablissement par rapport à la probabilité d'une demande).

Tableau 4 – Intégrité de sécurité matérielle – sous-système peu complexe (type A)

	Tolérance aux pannes matérielles		
Taux de défaillances non dangereuses	**0**	**1**	**2**
<60 %	SIL 1	SIL 2	SIL 3
60 % à <90 %	SIL 2	SIL 3	SIL 4 [a]
90 % à <99 %	SIL 3	SIL 4 [a]	SIL 4 [a]
≥99 %	SIL 3	SIL 4 [a]	SIL 4 [a]
[a] Cette partie s'applique à un FS-PLC ayant un niveau d'intégrité de sécurité inférieur ou égal à SIL 3. Des exigences spéciales s'appliquent pour le niveau d'intégrité de sécurité maximal SIL 4. Voir série CEI 61508.			
NOTE Tableau issu de la CEI 61508-2:2010, Tableau 2.			

Tableau 5 – Intégrité de sécurité matérielle – sous-système très complexe (type B)

	Tolérance aux pannes matérielles		
Taux de défaillances non dangereuses	**0**	**1**	**2**
<60 %	Non autorisée	SIL 1	SIL 2
60 % à <90 %	SIL 1	SIL 2	SIL 3
90 % à <99 %	SIL 2	SIL 3	SIL 4 [a]
≥99 %	SIL 3	SIL 4 [a]	SIL 4 [a]
[a] Cette partie s'applique à un FS-PLC ayant un niveau d'intégrité de sécurité inférieur ou égal à SIL 3. Des exigences spéciales s'appliquent pour le niveau d'intégrité de sécurité maximal SIL 4. Voir série CEI 61508.			
NOTE Tableau issu de la CEI 61508-2:2010, Tableau 3.			

9.4.3.1.3 Exigences pour le comportement du FS-PLC en matière de détection d'une panne

La détection d'une panne dangereuse au cours du fonctionnement du FS-PLC doit entraîner une action spécifiée pour:

a) mettre en place ou maintenir l'état de sécurité défini par le fabricant, ou

b) si le FS-PLC a une tolérance aux pannes matérielles de un ou plus, réparer la partie en panne pendant la durée moyenne de dépannage (MRT) spécifiée dans l'application, lorsqu'un fonctionnement continu est autorisé, ou si le FS-PLC a une tolérance aux pannes matérielles de zéro et se trouve en mode de faible sollicitation, réparer la partie en panne pendant la durée moyenne de dépannage (MRT) spécifiée dans l'application. Le fonctionnement continu au cours de la réparation du FS-PLC exige la mise en place de mesures de réduction des risques supplémentaires par l'utilisateur.

9.4.3.1.4 Horloges de surveillance indépendantes

Tous les sous-systèmes qui utilisent un microprocesseur doivent inclure une fonction d'horloge de surveillance:

– distincte et fonctionnant indépendamment de l'état du microprocesseur,

– non affectée par un mécanisme de cause commune pouvant empêcher la mauvaise réinitialisation de l'horloge de surveillance lors de la réinitialisation du microprocesseur.

Il convient d'éviter les types de mécanismes de réinitialisation d'horloges de surveillance suivants:

a) utilisation d'une plage d'adresses E/S ou de mémoire, il convient d'utiliser une seule adresse,

b) autorisation à la fois d'opérations de lecture et d'écriture, il convient d'en utiliser une seule,

c) utilisation d'une adresse facilement accessible si le microprocesseur est bloqué dans une boucle,

d) utilisation d'une seule valeur maximale de temporisation, il convient de spécifier une plage avec une valeur minimale et maximale.

9.4.3.2 Décomposition d'un sous-système matériel

9.4.3.2.1 Généralités

NOTE 1 Il est rappelé au lecteur que la définition du terme «sous-système» utilisé dans cette partie est différente de celle donnée dans la CEI 61508-4. Voir 3.55.

Le paragraphe 9.4.3.1 définit les exigences pour le taux de défaillance non dangereuse (SFF) et la tolérance aux pannes en fonction du niveau d'intégrité de sécurité et du type de sous-système.

Deux types de sous-systèmes, définis en 9.4.3.2.2 et 9.4.3.2.3, sont détaillés ci-après avec les informations supplémentaires suivantes:

Les sous-systèmes de type A (peu complexes) sont généralement composés de composants discrets (par exemple, résistances, condensateurs, diodes, transistors) pour lesquels les modes de pannes et leurs effets sur le sous-système sont prévisibles et bien définis.

Les sous-systèmes de type B (très complexes) incluent généralement un ou plusieurs composants complexes ou programmables (par exemple, microprocesseurs, circuits intégrés spécifiques, modules FS-PLC) ayant des modes de pannes mal définis avec des effets imprévisibles sur le sous-système. (Pour ces composants, en l'absence de meilleures données, on suppose que 50 % de toutes les pannes conduisent à un état de sécurité et 50 % à un état dangereux.)

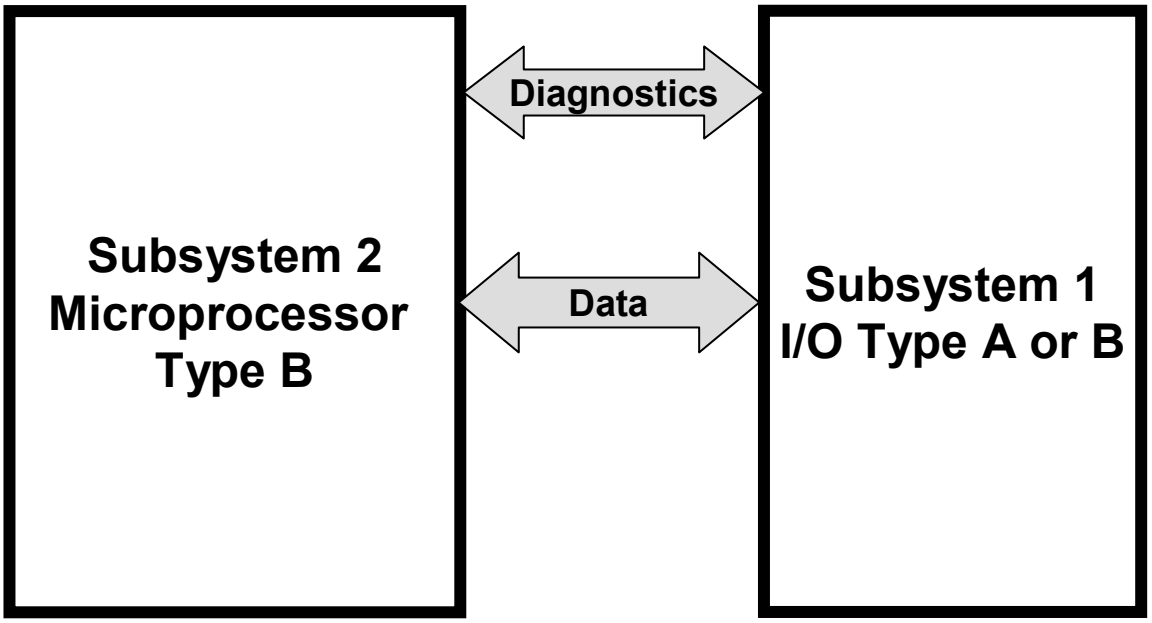
NOTE 2 Les circuits intégrés peu complexes sont ceux pour lesquels tous les modes de défaillances et effets de pannes sont connus.

Lors de l'évaluation d'un FS-PLC, le FS-PLC doit d'abord être décomposé en sous-systèmes. Chaque sous-système doit répondre aux exigences du Tableau 4 ou du Tableau 5, en ce qui

concerne le taux de défaillance non dangereuse (SFF) et la tolérance aux pannes nécessaires pour atteindre le niveau d'intégrité de sécurité spécifié.

Si deux sous-systèmes sont dépendants et si l'un d'eux fournit les diagnostics pour l'autre, le sous-système qui fournit les diagnostics doit d'abord répondre aux exigences du Tableau 4 ou du Tableau 5. Le sous-système fournissant les diagnostics peut ensuite être associé au deuxième sous-système pour répondre aux exigences du Tableau 4 ou du Tableau 5 pour les deux sous-systèmes ensemble.

NOTE 3 Exemple; les modules E/S du FS-PLC sont généralement composés d'un microprocesseur et d'une partie E/S, comme illustré à la Figure 6. L'élément processeur contrôle l'E/S et exécute souvent également les diagnostics. Dans un tel cas, l'élément processeur doit être traité en tant que sous-système de type B et l'E/S peut être un sous-système de type B ou de type A, selon les composants du sous-système.



Légende

Anglais	Français
Subsystem 2	Sous-système 2
Microprocessor	Microprocesseur
Type B	de type B
Diagnostics	Diagnostics
Data	Données
Subsystem 1	Sous-système 1
I/O Type A or B	E/S de type A ou B

Figure 6 – Décomposition du sous-système matériel

Prenons le cas d'un module E/S composé de deux sous-systèmes, l'un de type A ou B, appelé Sous-système 1 et l'autre de type B, appelé Sous-système 2. Ce module E/S est destiné à atteindre un niveau d'intégrité de sécurité SIL 3.

Supposons que le Sous-système 1 ait, à lui seul, une tolérance aux pannes de 1 et un taux de défaillance non dangereuse de 55 %. Supposons que le Sous-système 2 ait, à lui seul, une tolérance aux pannes de 1 et un taux de défaillance non dangereuse de 95 %.

Si le Sous-système 1 profite de l'élément processeur du Sous-système 2 pour mener des diagnostics, il peut atteindre une couverture de diagnostic et un taux de défaillance non dangereuse élevés (environ 100 %).

Cependant, lors de la combinaison des diagnostics, il faut prendre en considération un certain nombre d'éléments. Etant donné que les sous-systèmes 1 et 2 forment une série, ils doivent tous deux avoir un taux de défaillance non dangereuse (SFF) > 90 %. Cela signifie que les diagnostics du sous-système 1 doivent être ≥ 90 % si ce dernier contient des composants de type B et > 60 % s'il contient uniquement des composants de type A. La déclaration du type A sera difficile car les lignes de contrôle pour les diagnostics proviennent d'un sous-système de type B; ainsi l'interface de ces deux sous-systèmes doit avoir une couverture de diagnostic de 90 %. Pour déclarer une certaine couverture de diagnostic, cela doit être conforme à l'Annexe B de la CEI 61508-2:2010.

Le Tableau 5 requiert un taux de défaillance non dangereuse d'au moins 90 % pour que le module E/S atteigne un niveau d'intégrité de sécurité SIL 3.

Avant que le Sous-système 1 utilise le processeur du Sous-système 2 pour les diagnostics, la combinaison des Sous-systèmes 1 et 2 ne pouvait pas atteindre un taux de défaillance non dangereuse supérieur à 90 %. Une fois que le Sous-système 1 utilise le processeur du Sous-système 2 pour les diagnostics, la combinaison des Sous-systèmes 1 et 2 peut atteindre un taux de défaillance non dangereuse supérieur à 90 % et le module E/S peut donc atteindre le niveau d'intégrité de sécurité SIL 3.

9.4.3.2.2 Sous-système de type A

Un sous-système peut être de type A si, pour les composants requis pour accomplir la partie FS-PLC de la fonction de sécurité

a) les modes de défaillance de tous les composants constituants sont correctement définis; et

b) le comportement du sous-système en état de panne peut être complètement déterminé; et

c) il y a suffisamment de données de défaillance fiables provenant de l'expérience pratique pour voir que les taux de défaillance déclarés pour les défaillances dangereuses détectées et non détectées sont respectés (voir 9.4.8).

9.4.3.2.3 Sous-système de type B

Un sous-système doit être considéré de type B si, pour les composants requis pour accomplir la partie FS-PLC de la fonction de sécurité,

a) le mode de défaillance d'au moins un composant constituant n'est pas correctement défini; ou

b) le comportement du sous-système en état de panne ne peut pas être complètement déterminé; ou

c) il n'y a pas suffisamment de données de défaillance fiables provenant de l'expérience pratique pour étayer les déclarations des taux de défaillance relatifs aux défaillances dangereuses détectées et non détectées (voir 9.4.8).

NOTE 1 Cela signifie que si au moins l'un des composants d'un sous-système satisfait en lui-même aux conditions pour un sous-système de type B, ce sous-système est alors être considéré de type B et non de type A.

NOTE 2 Le FS-PLC est un sous-système complexe (type B). De même, le FS-PLC peut être composé de sous-systèmes de type A ou de type B.

9.4.3.2.4 Contraintes architecturales sur les sous-systèmes de type A et de type B

Le Tableau 4 et le Tableau 5 spécifient un taux de défaillances non dangereuses qui doit répondre à la spécification d'une déclaration de niveau d'intégrité de sécurité SIL 1, 2 ou 3, en fonction de la tolérance aux pannes matérielles. Les contraintes architecturales du Tableau 4 ou du Tableau 5 doivent s'appliquer à chaque sous-système accomplissant la partie FS-PLC de la fonction de sécurité. De cette manière:

a) les exigences de tolérance aux pannes matérielles doivent être respectées pour l'intégralité du système FS-PLC;

b) le Tableau 4 s'applique à chaque sous-système de type A faisant partie du système FS-PLC;

c) le Tableau 5 s'applique à chaque sous-système de type B faisant partie du système FS-PLC;

d) le Tableau 4 et le Tableau 5 s'appliquent au système FS-PLC comprenant des sous-systèmes de type A et de type B, car les exigences du Tableau 4 doivent s'appliquer aux sous-systèmes de type A et les exigences du Tableau 5 doivent s'appliquer aux sous-systèmes de type B.

9.4.3.2.5 Combinaisons de sous-systèmes en série

Dans un système FS-PLC où un certain nombre de fonctions de sécurité d'un élément sont implémentées via une combinaison d'éléments en série (comme illustré à la Figure 7), le niveau d'intégrité de sécurité maximal pouvant être déclaré pour la fonction de sécurité envisagée doit être déterminé par l'élément ayant atteint le plus bas niveau d'intégrité de sécurité pour le taux de défaillances non dangereuses mis en place pour une tolérance aux pannes matérielles de 0. Pour illustrer la méthode, prenons l'architecture présentée à la Figure 7, et étudions l'exemple ci-dessous.

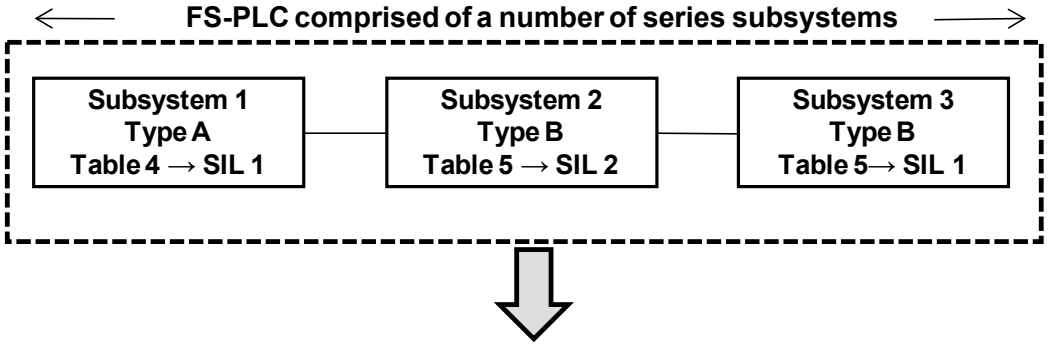
EXEMPLE (voir Figure 7) Prenons une architecture dans laquelle un certain nombre de fonctions de sécurité du sous-système sont effectuées par le canal unique des sous-systèmes 1, 2 et 3, comme illustré à la Figure 7 et les sous-systèmes répondent aux exigences du Tableau 4 et du Tableau 5, comme suit:

– le sous-système 1 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux de défaillances non dangereuses spécifique pour un SIL 1;

– le sous-système 2 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux spécifique de défaillances non dangereuses spécifique pour un SIL 2;

– le sous-système 3 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux de défaillances non dangereuses spécifique pour un SIL 1;

– les sous-systèmes 1 et 3 restreignent le niveau d'intégrité de sécurité maximal pouvant être déclaré, pour une tolérance aux pannes matérielles et un taux de défaillances non dangereuses SIL 1 uniquement.



Légende

Anglais	Français
FS-PLC comprised of an number of series subsystems	FS-PLC composé d'un certain nombre de sous-systèmes en série
Subsystem 1	Sous-système 1
Type A	Type A
Table 4 -> SIL 1	Tableau 4 -> SIL 1
Subsystem 2	Sous-système 2
Type B	Type B
Table 5 -> SIL 2	Tableau 5 -> SIL 2
Subsystem 3	Sous-système 3
Type B	Type B
Table 5 -> SIL 1	Tableau 5 -> SIL 1
FS-PLC meets the architectural constraints, for the safety function, of SIL 1	Le FS-PLC répond aux contraintes architecturales pour la fonction de sécurité de SIL 1

Figure 7 – Exemple: détermination du niveau d'intégrité de sécurité maximal pour l'architecture spécifiée

9.4.3.2.6 Combinaisons de sous-systèmes en parallèle

Dans un système FS-PLC dans lequel la fonction de sécurité est implémentée via plusieurs canaux de sous-systèmes (comme illustré à la Figure 8), le niveau d'intégrité de sécurité matérielle maximal pouvant être déclaré pour la fonction de sécurité envisagée doit être déterminé en:

a) regroupant la combinaison d'éléments en série pour chaque canal, puis en déterminant le niveau d'intégrité de sécurité maximal pouvant être déclaré pour la fonction de sécurité envisagée pour chaque canal (voir 9.4.3.2.5); et

b) sélectionnant le canal avec le plus haut niveau d'intégrité de sécurité atteint pour la fonction de sécurité envisagée, puis en ajoutant 1 niveau d'intégrité de sécurité pour déterminer le niveau d'intégrité de sécurité maximal pour la combinaison totale du sous-système.

c) Les exigences suivantes, au moins, doivent être respectées:

- la fonction de sécurité doit être effectuée dans chaque sous-système,
- l'analyse des défaillances de cause commune doit être réalisée selon le niveau d'intégrité de sécurité déclaré,
- le dispositif de décision à la sortie des sous-systèmes doit être conçu selon le niveau d'intégrité de sécurité déclaré,

- la réaction de défaillance du système combiné doit satisfaire aux exigences de la CEI 61508-2:2010, 7.4.8,
- la couverture de diagnostic (DC) du FS-PLC doit répondre aux exigences relatives au niveau d'intégrité de sécurité du système combiné,
- le logiciel/microprogramme utilisé dans le FS-PLC doit remplir les exigences relatives au niveau d'intégrité de sécurité du système combiné,

d) Hypothèses:

- une panne systématique de ce sous-système ne provoque pas de défaillance de la fonction de sécurité spécifiée mais provoque cette défaillance uniquement en combinaison avec une deuxième panne systématique d'un autre sous-système,
- une indépendance suffisante existe entre les deux sous-systèmes (justifiée par une analyse des défaillances de cause commune).

EXEMPLE Le regroupement et l'analyse de ces combinaisons peuvent être effectués de différentes manières. Pour illustrer l'une des méthodes possibles, prenons une architecture dans laquelle une fonction de sécurité spécifique du FS-PLC est accomplie par deux sous-systèmes, X et Y, où le sous-système X est composé des sous-systèmes 1, 2, 3 et 4, et le sous-système Y est composé d'un seul sous-système 5, comme illustré à la Figure 8. L'utilisation de canaux parallèles dans le sous-système X garantit que les sous-systèmes 1 et 2 implémentent la partie requise de la fonction de sécurité du FS-PLC du sous-système X indépendamment des sous-systèmes 3 et 4, et inversement. La fonction de sécurité du FS-PLC sera accomplie:

– en cas de panne dans le sous-système 1 ou 2, la combinaison des sous-systèmes 3 et 4 parvient à réaliser la partie requise de la fonction de sécurité du FS-PLC; ou

– en cas de panne dans le sous-système 3 ou 4, la combinaison des sous-systèmes 1 et 2 parvient à réaliser la partie requise de la fonction de sécurité du FS-PLC.

La détermination du niveau d'intégrité de sécurité maximal pouvant être déclarée pour la fonction de sécurité envisagée est détaillée dans les étapes suivantes.

Pour le sous-système X, conformément à la fonction de sécurité spécifiée envisagée du FS-PLC, chaque sous-système répond aux exigences du Tableau 4 et du Tableau 5, comme suit:

– le sous-système 1 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux de défaillances non dangereuses spécifique pour un SIL 3;

– le sous-système 2 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux de défaillances non dangereuses spécifique pour un SIL 2;

– le sous-système 3 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux de défaillances non dangereuses spécifique pour un SIL 2;

– le sous-système 4 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux de défaillances non dangereuses spécifique pour un SIL 1.

Les sous-systèmes sont combinés de manière à offrir un niveau d'intégrité de sécurité matérielle maximal pour la fonction de sécurité envisagée du FS-PLC, pour le sous-système X, comme suit:

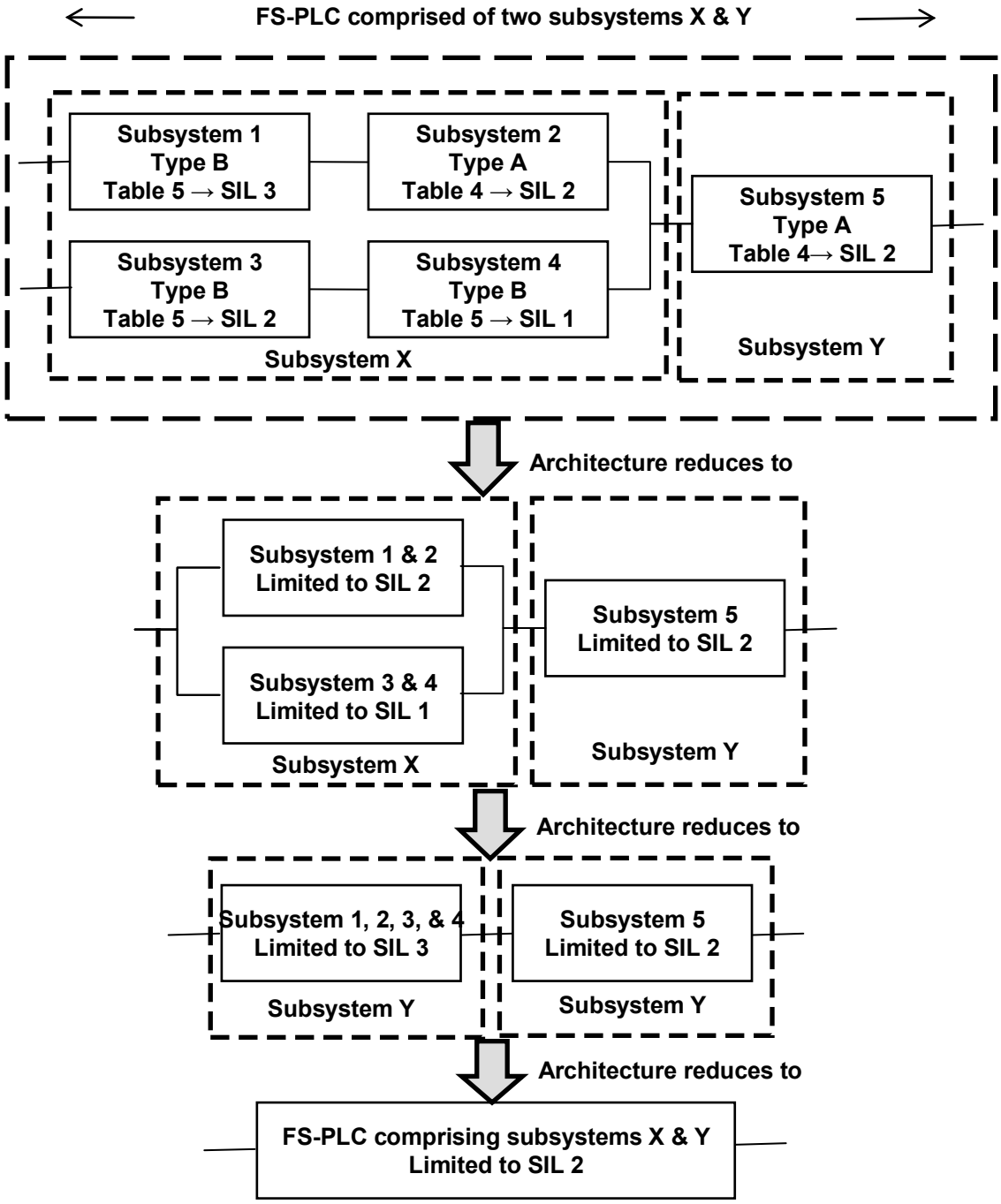
a) Combinaison des sous-systèmes 1 et 2: La tolérance aux pannes matérielles et le taux de défaillances non dangereuses atteints par la combinaison des sous-systèmes 1 et 2 (répondant chacun, respectivement, aux exigences pour un SIL 3 et un SIL 2) répondent aux exigences d'un SIL 2 (déterminé par le sous-système 2; voir 9.4.3.2.5);

b) Combinaison des sous-systèmes 3 et 4: La tolérance aux pannes matérielles et taux de défaillances non dangereuses atteints par la combinaison des sous-systèmes 3 et 4 (répondant chacun, respectivement, aux exigences pour un SIL 2 et un SIL 1) répondent aux exigences d'un SIL 1 (déterminé par le sous-système 4; voir 9.4.3.2.5);

c) Combinaison de la combinaison des sous-systèmes 1 et 2 et de la combinaison des sous-systèmes 3 et 4: le niveau d'intégrité de sécurité maximal pouvant être déclaré pour la fonction de sécurité envisagée du FS-PLC est déterminée par la sélection du canal ayant le plus haut niveau d'intégrité de sécurité atteint, puis par l'ajout de 1 niveau d'intégrité de sécurité afin de déterminer le niveau d'intégrité de sécurité maximal pour la combinaison totale des sous-systèmes. Dans ce cas, le sous-système comprend deux canaux parallèles avec une tolérance aux pannes matérielles de 1. Le canal ayant le plus haut niveau d'intégrité de sécurité pour la fonction de sécurité envisagée du FS-PLC est celui comprenant les sous-systèmes 1 et 2, qui répondaient aux exigences pour un SIL 2. Par conséquent, le niveau d'intégrité de sécurité maximal pour le sous-système, pour une tolérance de pannes matérielles de 1, est (SIL 2 + 1) = SIL 3 (voir 9.4.3.2.6).

Pour le sous-système Y, le sous-système 5 répond aux exigences, pour une tolérance aux pannes matérielles de 0 et un taux de défaillances non dangereuses spécifique pour un SIL 2.

Pour l'intégralité du FS-PLC (c'est-à-dire les deux sous-systèmes X et Y répondant respectivement aux exigences d'un SIL 3 et d'un SIL 2 pour la fonction de sécurité envisagée), le niveau d'intégrité de sécurité maximal pouvant être déclaré pour un FS-PLC est déterminé par le sous-système ayant atteint le plus bas niveau d'intégrité de sécurité (9.4.3.1.2). Par conséquent, dans cet exemple, le niveau d'intégrité de sécurité maximal pouvant être déclaré pour le FS-PLC, pour la fonction de sécurité envisagée, est SIL 2.



FS-PLC meets the architectural constraints, for the safety function, of SIL 2

IEC 1824/12

Légende

Anglais	Français
FS-PLC comprised of two subsystems X & Y	FS-PLC composé de deux sous-systèmes, X et Y
Subsystem 1	Sous-système 1
Type B	Type B
Table 5 -> SIL 3	Tableau 5 -> SIL 3

Anglais	Français
Subsystem 2	Sous-système 2
Type A	Type A
Table 4 -> SIL 2	Tableau 4 -> SIL 2
Subsystem 5	Sous-système 5
Type A	Type A
Table 4 -> SIL 2	Tableau 4 -> SIL 2
Subsystem 3	Sous-système 3
Type B	Type B
Table 5 -> SIL 2	Tableau 5 -> SIL 2
Subsystem 4	Sous-système 4
Type B	Type B
Table 5 - SIL 1	Tableau 5 -> SIL 1
Subsystem X	Sous-système X
Subsystem Y	Sous-système Y
Architecture reduces to	Architecture réduite à
Subsystem 1 & 2	Sous-systèmes 1 et 2
Limited to SIL2	Limité à SIL 2
Subsystem 5	Sous-système 5
Limited to SIL 2	Limité à SIL 2
Subsystem 3 & 4	Sous-systèmes 3 et 4
Limited to SIL 1	Limité à SIL 1
Subsystem X	Sous-système X
Subsystem Y	Sous-système Y
Architecture educes to	Architecture réduite à
Subsystem 1, 2, 3 & 4	Sous-systèmes 1, 2, 3 et 4
Limited to SIL 3	Limité à SIL 3
Subsystem 5	Sous-système 5
Limited to SIL 2	Limité à SIL 2
Subsystem Y	Sous-système Y
Architecture reduces to	Architecture réduite à
FS-PLC comprising subsystems X & Y	FS-PLC composé des sous-systèmes X et Y
Limited to SIL 2	Limité à SIL 2
FS-PLC meets the architectural constraints, for the safety function, of SIL 2	Le FS-PLC répond aux contraintes architecturales pour la fonction de sécurité de SIL 2

NOTE 1 Les sous-systèmes 1 et 2 implémentent la partie requise de la fonction de sécurité du sous-système X indépendamment des éléments 3 et 4, et inversement.

NOTE 2 Les sous-systèmes implémentant la fonction de sécurité du FS-PLC seront différents de l'intégralité du système FS-PLC en termes de classement des entrées et de résolution logique des sorties.

NOTE 3 Pour plus de détails sur l'interprétation de cette figure, voir l'exemple décrit ci-dessus.

NOTE 4 Le type A s'applique uniquement au sous-système d'un FS-PLC. Le type B peut s'appliquer au sous-système d'un FS-PLC ou au FS-PLC lui-même.

Figure 8 – Exemple de limitation sur l'intégrité de sécurité matérielle pour une fonction de sécurité à canaux multiples

9.4.4 Défaillances aléatoires du matériel

9.4.4.1 Généralités

La probabilité de défaillance dangereuse due à des défaillances aléatoires du matériel doit être inférieure ou égale à la mesure de défaillance cible telle que stipulée dans la spécification des exigences de sécurité fonctionnelle.

Les défaillances aléatoires du matériel pour une conception doivent être identifiées et traitées par une analyse des effets et des modes de défaillance (FMEA), une analyse par l'arbre de défaillance ou toutes autres méthodes acceptables (voir l'Annexe A). Les taux de défaillance de chaque composant doivent être estimés à partir d'une base de données de fiabilité reconnue. Chaque défaillance doit être classée dans l'une des catégories suivantes, à l'aide d'une analyse de couverture de diagnostic:

- détectée comme sécurisée,
- non détectée comme sécurisée,
- détectée comme dangereuse,
- non détectée comme dangereuse,
- sans effet.

Tous les calculs de fiabilité doivent utiliser une source unique pour les données de fiabilité des composants. Des données provenant de sources multiples peuvent être utilisées seulement si l'on peut démontrer que ces données ont été développées dans des conditions communes. Pour plus d'informations, voir l'Annexe D.

Une fois ces taux de défaillance déterminés, un modèle de fiabilité pour le FS-PLC doit être établi et une méthode de calcul doit être sélectionnée. Il s'agit d'un pré-requis à la détermination de la valeur PFD ou PFH des sous-systèmes, ainsi que le FS-PLC. L'Annexe B de la CEI 61508-6:2010 concerne les calculs des valeurs PFD et PFH, et doit être utilisée pour plusieurs architectures d'un FS-PLC; par exemple, 1oo1, 1oo2, 1oo2D (avec diagnostic), 2oo2 et 2oo3, etc.

Pour les systèmes complexes tels qu'un FS-PLC, un calcul de fiabilité basé sur des blocs-diagrammes de fiabilité ou un modèle de Markov est recommandé.

NOTE Lorsque des données appropriées sont disponibles, la défaillance est répartie entre les différents modes de défaillance prédominants: court-circuit, circuit ouvert, modification de valeur, etc.

9.4.4.2 Défaillances matérielles de cause commune

Là où l'architecture du FS-PLC inclut des canaux multiples (par exemple, des architectures 1oo2 ou 2oo3), les défaillances de cause commune doivent alors être prises en compte.

Une défaillance de cause commune est une défaillance résultant d'un ou plusieurs événements qui provoquent une défaillance coïncidente ou quasi coïncidente d'au moins deux canaux distincts dans un système à canaux multiples, donnant potentiellement lieu à la perte de la fonction de sécurité. Les défaillances de cause commune peuvent provenir d'une panne systématique (par exemple, une erreur de conception ou de spécification) ou d'une contrainte externe menant à une défaillance matérielle (par exemple, une température excessive).

Les taux de défaillance de cause commune doivent être estimés à l'aide d'une méthode reconnue. En règle générale, les méthodes de ce type appliquent une proportion du taux de défaillance aléatoire du matériel pour un canal, comme taux de défaillance de cause commune pour le système à canaux multiples. La valeur de la proportion (facteur bêta) est déterminée par un système d'évaluation basé sur le degré d'indépendance des canaux et la possibilité de détecter des pannes avant qu'elles n'affectent tous les canaux.

La pertinence de la méthode sélectionnée pour l'évaluation des défaillances de cause commune dans la conception du FS-PLC doit être justifiée.

NOTE L'Annexe E indique une méthode possible permettant d'évaluer les défaillances de cause commune. De plus amples informations sont disponibles dans l'Annexe D de la CEI 61508-6:2010.

9.4.4.3 Couverture de diagnostic matériel (DC)

La couverture de diagnostic d'un système FS-PLC peut être calculée comme suit:

- créer un modèle de fiabilité du FS-PLC à l'aide de sous-systèmes appropriés
- réaliser une analyse des effets et des modes de défaillance (FMEA) pour chaque composant de chaque sous-système
- catégoriser chaque mode de défaillance selon qu'il donne lieu à un effet de défaillance non dangereuse ou à un effet dangereux tel que défini par l'état de sécurité et les applications prévues du FS-PLC, tel que déclaré par le fabricant

  NOTE 1 Là où les données ne sont pas disponibles pour les composants très complexes, on peut supposer que 50 % des défaillances aléatoires du matériel sont sécurisées et que 50 % sont dangereuses. Cette hypothèse peut également être appliquée aux sous-systèmes; en règle générale, elle n'est toutefois pas utilisée.
- calculer le taux de défaillance des défaillances sécurisées (λ_S) et le taux de défaillance des défaillances dangereuses (λ_D), et ce pour chaque sous-système
- estimer le taux de défaillance des défaillances dangereuses qui sera détecté par des essais de diagnostic (λ_{DD}), et ce pour chaque sous-système
- calculer le taux de défaillance des défaillances dangereuses qui ne sera pas détecté par des essais de diagnostic (λ_{DU}), et ce pour chaque sous-système

  NOTE 2 $\lambda_D = \lambda_{DD} + \lambda_{DU}$.
- calculer la couverture de diagnostic (valeur moyenne DC) et la fraction de défaillance en sécurité (valeur moyenne SFF) pour chaque sous-système:

  $DC = \Sigma \lambda_{DD} / \Sigma \lambda_D = \Sigma \lambda_{DD} / [\Sigma \lambda_{DU} + \Sigma \lambda_{DD}]$
- lorsque l'un de ces taux de défaillance n'est pas constant, sa moyenne sur la période doit être estimée et utilisée dans les calculs de DC et de SFF.

La couverture de diagnostic pour le même sous-système par au moins deux méthodes différentes peut être utilisée pour déclarer une couverture de diagnostic supérieure aux valeurs généralement autorisées par la série CEI 61508. Les différentes méthodes doivent être indépendantes et n'être associées à aucun mode de défaillance de cause commune.

Le Tableau 6 répertorie les pannes ou les défaillances qui doivent, au minimum, être détectées dans le but d'atteindre la couverture de diagnostic indiquée.

Voir l'Annexe A de la CEI 61508-2:2010 pour obtenir une liste plus complète des techniques et mesures qui doivent, le cas échéant, être intégrées à un FS-PLC en vue de contrôler des défaillances aléatoires du matériel, systématiques, environnementales et opérationnelles. L'Annexe A de la CEI 61508-2:2010 fournit également des explications plus détaillées concernant ces techniques et mesures.

Tableau 6 – Pannes ou défaillances à considérer lors de la quantification de l'effet des défaillances aléatoires du matériel ou à prendre en compte pour la détermination du taux de défaillances non dangereuses

Composant	Voir Tableau(x) de la CEI 61508-2:2010 Annexe A	Exigences déclarées concernant la couverture de diagnostic		
		Faible (60 %)	Intermédiaire (90 %)	Elevée (99 %)
Dispositifs électromécaniques	A.2	Absence d'alimentation ou de non-alimentation; Contacts soudés	Absence d'alimentation ou de non-alimentation; Contacts individuels soudés	Absence d'alimentation ou de non-alimentation Contacts individuels soudés Absence de guidage positif des contacts (pour les relais, cette défaillance n'est pas supposée s'ils sont conçus et soumis à essai conformément à la norme EN 50205 ou norme équivalente) Pas d'ouverture correcte (pour les contacteurs de position, cette défaillance n'est pas supposée s'ils sont conçus et soumis à essai conformément à la CEI 60947-5-1 ou norme équivalente)
Matériel discret	A.3, A.7, A.9			
E/S numérique		Blocage[b]	Modèle de panne DC[c]	Modèle de panne DC[c]; Dérive[h] et oscillation
E/S analogique		Blocage[b]	Modèle de panne DC[c]; Dérive et oscillation	Modèle de panne DC[c]; Dérive et oscillation
Alimentation électrique		Blocage[b]	Modèle de panne DC[c]; Dérive et oscillation	Modèle de panne DC[c]; Dérive et oscillation
Bus	A.3 A.7 A.8			
Généralités		Blocage[b] des adresses	Temps écoulé Décodage d'une adresse erronée	Temps écoulé Décodage d'une adresse erronée
Unité de gestion de mémoire (MMU)		Blocage[b] des données ou des adresses	Modification des adresses provoquée par des erreurs logiques dans les registres MMU [d e] Modèle de panne DC[c] pour des données et des adresses;	Modification des adresses provoquée par des erreurs logiques dans les registres MMU [d e] Toutes les pannes affectant les données de la mémoire;
Accès direct à la mémoire (DMA)		Accès inexistant ou continu	Modification des informations provoquée par des erreurs logiques dans les registres DMA Heure d'accès erronée	Heure d'accès erronée
Arbitrage de bus[a]		Blocage[b] des signaux d'arbitrage	Arbitrage inexistant ou continu	Arbitrage inexistant, continu ou erroné

Composant	Voir Tableau(x) de la CEI 61508-2:2010 Annexe A	Exigences déclarées concernant la couverture de diagnostic		
		Faible (60 %)	Intermédiaire (90 %)	Elevée (99 %)
UC/processeur	A.4, A.10			Modèle de panne DC[c] pour des données et des adresses;
Registre, RAM interne		Blocage[b] pour des données et des adresses	Modèle de panne DC[c] pour des données et des adresses Modification des informations provoquée par des erreurs logiques	Croisement dynamique pour cellules de mémoire; Modification des informations provoquée par des erreurs logiques Adressage inexistant, erroné ou multiple
Codage et exécution (y compris registre à drapeaux)		Codage erroné ou absence d'exécution	Codage erroné ou exécution erronée	Absence d'hypothèse de défaillance formelle
Calcul d'adresse		Blocage[b]	Modèle de panne DC[c] Modification des informations provoquée par des erreurs logiques	Absence d'hypothèse de défaillance formelle
Compteur de programme, pointeur de pile		Blocage[b]	Modèle de panne DC[c] Modification des informations provoquée par des erreurs logiques	Modèle de panne DC[c] Modification des informations provoquée par des erreurs logiques
Gestion des interruptions **Interruption**	A.4	Interruptions inexistantes ou continues[f]	Interruptions inexistantes ou continues[f]; Croisement d'interruptions	Interruptions inexistantes ou continues[f]; Croisement d'interruptions
Réinitialisation de circuit	A.4	Blocage[b] L'état de réinitialisation n'est pas appliqué aux composants individuels.	Modèle de panne DC[c]; Dérive et oscillation L'état de réinitialisation n'est pas appliqué aux composants individuels.	Modèle de panne DC[c]; Dérive et oscillation L'état de réinitialisation n'est pas appliqué aux composants individuels.
Mémoire morte/mémoire invariable	A.5	Blocage[b] des données et des adresses	Modèle de panne DC[c] pour des données et des adresses	Toutes les pannes affectant les données de la mémoire
Mémoire vive/mémoire variable	A.6	Blocage[b] des données et des adresses	Modèle de panne DC[c] pour des données et des adresses; Modification des informations provoquée par des erreurs logiques	Modèle de panne DC[c] pour des données et des adresses; Croisement dynamique pour cellules de mémoire; Adressage inexistant, erroné ou multiple; Modification des informations provoquée par des erreurs logiques

Composant	Voir Tableau(x) de la CEI 61508-2:2010 Annexe A	Exigences déclarées concernant la couverture de diagnostic		
		Faible (60 %)	Intermédiaire (90 %)	Elevée (99 %)
Horloge (quartz, oscillateur, PLL)	A.11	Sous- ou surharmonique Fluctuation de période	Fréquence incorrecte Fluctuation de période	Fréquence incorrecte Fluctuation de période
Communication et mémoire de masse	A.12	Données ou adresses erronées; Aucune transmission	Toutes les pannes affectant les données de la mémoire; Données ou adresses erronées; Heure de transmission erronée; Séquence de transmission erronée	Toutes les pannes affectant les données de la mémoire; Données ou adresses erronées; Heure de transmission erronée; Séquence de transmission erronée

NOTE Pour les circuits intégrés spécifiques, ce tableau et les Tableaux A.2 à A.18 de la CEI 61508-2:2010 s'appliquent le cas échéant.

a L'arbitrage du bus est le mécanisme permettant de décider quel dispositif contrôle le bus.

b "Blocage" est une catégorie de pannes qui peut être décrite avec un "0" ou un "1" continu, ou encore par "on" (par exemple, au niveau des broches d'un composant).

c "Modèle de panne DC" (DC = courant continu) inclut les modes de défaillance suivants: pannes avec absence d'action, bloquée en position ouverte, ouverte ou sorties à haute impédance, de même que courts-circuits entre circuits de transmission. Pour les circuits intégrés, un court-circuit entre deux connexions (broches) est pris en compte.

d Il est connu que le taux d'erreurs logiques pour les semi-conducteurs faiblement alimentés est supérieur de plus d'un ordre de grandeur (50x..500x) au taux d'erreurs physiques (endommagement permanent du dispositif). Voir référence à la CEI 61508-7:2010, A.5.

e Les causes d'erreurs logiques sont les suivantes: particules alpha issues de la dégradation du package, neutrons, bruit externe de perturbations électromagnétique et diaphonie interne. L'effet des erreurs logiques ne peut être maîtrisé que par des mesures d'intégrité de sécurité lors de l'exécution. Des mesures d'intégrité de sécurité efficaces pour des défaillances aléatoires du matériel peuvent ne pas être efficaces pour les erreurs logiques. Exemple: Les essais de RAM, tels que walkpath, galpat, etc., ne sont pas efficaces, alors que les techniques de contrôle utilisant Parity et ECC avec une lecture récurrente des cellules de mémoire ou les techniques utilisant la redondance (et la comparaison ou le vote) peuvent l'être.

f Pas d'interruption signifie qu'aucune interruption ne se produit lorsqu'il faudrait qu'une ou plusieurs interruptions aient lieu. Interruptions continues signifient que des interruptions successives se produisent lorsqu'il faudrait qu'elles n'aient pas lieu.

9.4.4.4 Taux de défaillance non dangereuse matérielle (SFF)

Pour des éléments ou sous-systèmes complexes, une séparation de défaillances 50 % non dangereuses/50 % dangereuses est généralement acceptée (par exemple, éléments ou sous-systèmes sans diagnostic(s)).

Les composants "sans effet" ne doivent pas être inclus pour le calcul (par exemple, DEL, condensateurs à filtres multiples).

Le Tableau 6 indique les pannes ou défaillances à détecter en cours de fonctionnement ou à analyser dans la détermination du taux de défaillances dangereuses.

9.4.4.5 Calculs de l'aptitude du niveau d'intégrité de sécurité

Afin de déclarer un niveau d'intégrité de sécurité maximal spécifique pour un FS-PLC, les techniques qualitatives et les mesures spécifiées dans l'Annexe B de la CEI 61508-2 et les

valeurs quantitatives calculées utilisant les équations de l'Annexe B de la CEI 61508-6:2010 doivent être satisfaites.

L'intégration de ces techniques et mesures spécifiques au cours du cycle de vie du FS-PLC permet de traiter les défaillances systématiques. L'exécution des calculs de l'Annexe B de la CEI 61508-6:2010 permet de traiter les défaillances aléatoires du matériel.

Les éléments suivants se concentrent sur les calculs quantitatifs d'un niveau d'intégrité de sécurité maximal pour un FS-PLC. Cette séquence d'actions par le fabricant du FS-PLC simplifie le processus de calcul du niveau d'intégrité de sécurité:

a) déterminer le niveau d'intégrité de sécurité spécifié pour le ou les champs d'application prévus ("le niveau d'intégrité de sécurité cible"),

b) déterminer si la ou les applications prévues nécessiteront une faible sollicitation quant à la fonction de sécurité du FS-PLC ou une sollicitation élevée/continue quant à la fonction de sécurité du FS-PLC, ou les deux. Une faible sollicitation nécessitera un calcul de PFD, alors qu'une sollicitation élevée/continue nécessitera plutôt un calcul de PFH,

c) spécifier l'architecture pour le FS-PLC,

d) établir ce pourcentage des valeurs PFD ou PFH associé au niveau d'intégrité de sécurité du système qui sera alloué au FS-PLC (voir 6.3),

e) établir une durée moyenne de rétablissement (MTTR) et une durée moyenne de dépannage (MRT) pour le FS-PLC lors de la survenue d'une défaillance,

f) recommander un ou plusieurs intervalles d'essais de sûreté (T_1) pour le FS-PLC,

g) déterminer les taux de défaillance dangereuse pour le FS-PLC (détectées (λ_{DD}) et non détectées (λ_{DU})) en fonction des taux de défaillance des composants matériels (voir 9.4.4.3) et des calculs associés (voir l'Annexe B de la CEI 61508-6:2010),

h) calculer les pourcentages des défaillances de cause commune détectées (β_D) et non détectées (β). Voir l'Annexe E. (voir également l'Annexe D de la CEI 61508-6:2010),

i) utiliser les paramètres ci-dessus pour calculer les valeurs PFD et/ou PFH conformément à l'Annexe B de la CEI 61508-6:2010,

j) vérifier que la ou les valeurs calculées correspondent aux plages allouées appropriées par rapport aux Tableaux B.2, B.3, B.4, B.5, B.10, B.11, B.12 et B.13 de la CEI 61508-6:2010.

9.4.5 Exigences matérielles permettant d'éviter les défaillances systématiques

Les techniques et les mesures permettant d'éviter les défaillances systématiques lors du développement matériel décrites dans l'Annexe B de la CEI 61508-2:2010 doivent être utilisées.

9.4.6 Exigences matérielles pour le contrôle des pannes systématiques

9.4.6.1 Généralités

Les pannes systématiques sont des pannes liées à une cause qui ne peuvent être éliminées que par une modification de la conception ou du procédé de fabrication, du mode d'emploi, de la documentation ou d'autres facteurs correspondants.

9.4.6.2 Contrôle des pannes systématiques

Pour le contrôle des pannes systématiques, la conception du FS-PLC doit posséder des caractéristiques de conception qui rendent les systèmes relatifs à la sécurité du FS-PLC tolérants vis-à-vis:

- des pannes de conception résiduelle dans le matériel, à moins que la possibilité de pannes de conception matérielle puisse être exclue (voir Tableau A.15 de la CEI 61508-2:2010);

- des contraintes environnementales, y compris les perturbations électromagnétiques (voir Tableau A.16 de la CEI 61508-2:2010);
- des pannes de conception résiduelle dans le logiciel;
- des erreurs et autres effets provenant d'un processus de communication de données (voir 8.3).

9.4.6.3 Maintenabilité et testabilité

La maintenabilité et la testabilité doivent être prises en compte pendant les activités de conception et de développement pour faciliter l'implémentation de ces propriétés dans les systèmes relatifs à la sécurité finale intégrant le FS-PLC.

9.4.6.4 Interfaces avec l'homme

La conception du FS-PLC doit prendre en compte les capacités et les limites humaines, et être adaptée aux actions affectées aux opérateurs et au personnel de maintenance. La conception de toutes les interfaces doit respecter les bonnes pratiques sous l'angle du facteur humain et doit correspondre au niveau probable de formation ou de sensibilisation des opérateurs (par exemple, dans les applications de production de masse pour lesquelles l'opérateur ne dispose que d'une formation limitée).

NOTE L'objectif de conception consiste à éviter ou à éliminer les erreurs critiques prévisibles commises par les opérateurs ou le personnel de maintenance grâce à la conception chaque fois que cela est possible, ou à permettre une deuxième confirmation avant exécution.

9.4.7 Classification matérielle des pannes

Les pannes donnent lieu à des défaillances. L'objectif consiste à détecter et à signaler les pannes avant qu'elles n'aient pu entraîner une défaillance dangereuse. La détection d'une panne avant la survenue de pannes multiples est un concept clé, étant donné que les scénarios de pannes multiples peuvent devenir impossibles à analyser.

A moins d'être explicitement identifiés, les scénarios de pannes multiples ne sont pas pris en compte dans les analyses de pannes (par exemple, analyse par arbre de panne (AAP), analyse des effets et des modes de défaillance (FMEA)).

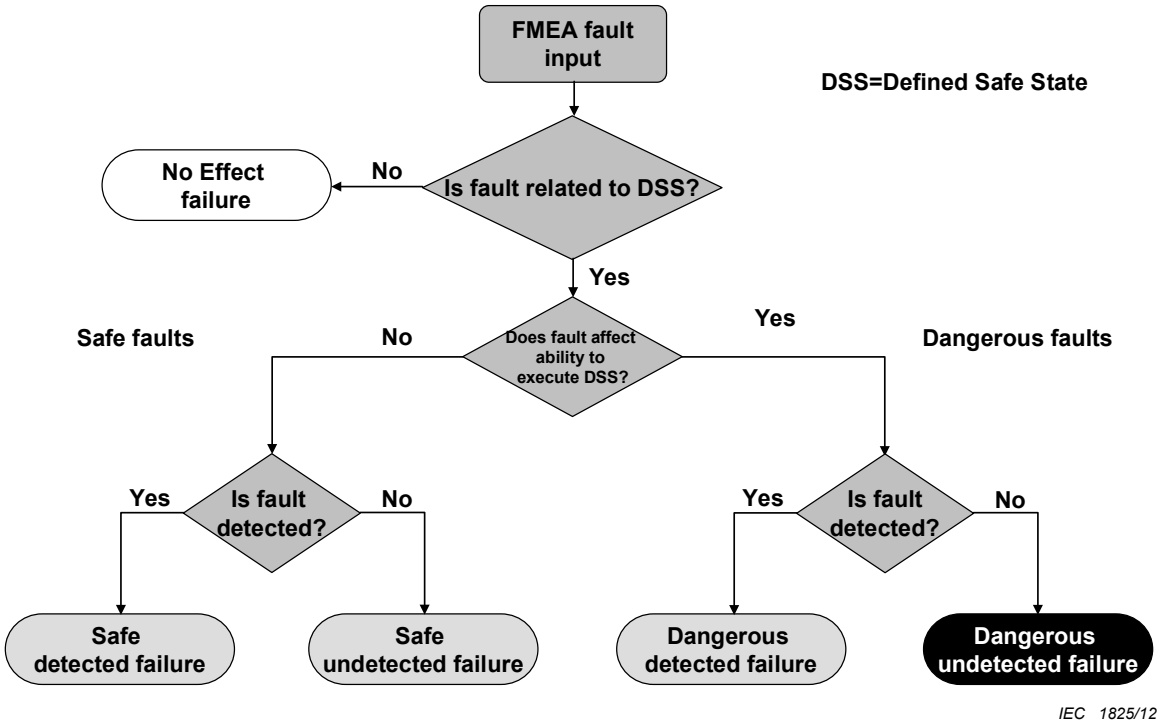
En règle générale, il existe cinq types de défaillances différents qui doivent être pris en compte pour l'analyse d'un FS-PLC. La classification de ces cinq défaillances dépend de la fonction de sécurité du FS-PLC, ainsi que de son architecture.

Le premier type de panne (panne sans effet) n'a aucun effet sur la fonction de sécurité du FS-PLC (par exemple, indicateur d'annonce). Il ne doit être inclus dans aucun calcul de PFD, PFH, etc. et ne doit pas contribuer à une SFF.

Si une défaillance n'affecte pas la fonction de sécurité du FS-PLC, elle est classée comme "défaillance sans effet". Une "défaillance sans effet" ne contribue pas au calcul du taux de défaillances non dangereuses (SFF).

Les quatre autres types de pannes sont considérés en regard de la fonction de sécurité du FS-PLC. Ceux-ci doivent être inclus dans les calculs de PFD, PFH, etc.

L'objectif de la Figure 9 consiste à aider ou guider le concepteur du FS-PLC à catégoriser correctement les pannes en vue d'une analyse de défaillance (FMEA, FTA).



Légende

Anglais	Français
FMEA fault input	Saisie de panne FMEA
No Effect failure	Défaillance sans effet
No	Non
Yes	Oui
DSS=Defined Safe State	ESD=Etat de sécurité défini
Safe faults	Pannes non dangereuses
Is fault related to DSS?	La panne est-elle liée à ESD?
Does fault affect ability to execute DSS?	La panne affecte-t-elle l'aptitude à exécuter une ESD?
Dangerous faults	Pannes dangereuses
Is fault detected?	La panne est-elle détectée?
Safe detected failure	Défaillance détectée non dangereuse
Safe undetected failure	Défaillance non détectée non dangereuse
Dangerous detected failure	Défaillance détectée dangereuse
Dangerous undetected failure	Défaillance non détectée dangereuse

Figure 9 – Classification des pannes et comportement du FS-PLC

Les moyens de diagnostic sont supposés être disponibles pour détecter et réagir à la ou aux pannes non dangereuses et/ou dangereuses.

Si une défaillance exécute fortuitement la fonction de sécurité du FS-PLC, il s'agit d'une défaillance non dangereuse non détectée. En revanche, si la défaillance n'exécute pas fortuitement la fonction de sécurité du FS-PLC mais qu'elle est détectée par des mesures de diagnostic, on suppose que le diagnostic donne lieu à une réaction adéquate du système conformément au 7.4.8 de la CEI 61508-2:2010 ou que la défaillance sera réparée (défaillance détectée non dangereuse). En cas de mode de fonctionnement à sollicitation élevée, la défaillance diagnostiquée doit donner lieu à une exécution automatique de la fonction de sécurité du FS-PLC ou à un état non dangereux. En cas de mode à faible sollicitation, une notification à l'opérateur suffit à lancer la réparation du système.

Si le système n'exécute pas fortuitement la fonction de sécurité du FS-PLC ou qu'il n'atteint pas un état de sécurité, la défaillance est classée comme défaillance dangereuse non détectée. De plus, une défaillance dangereuse pourrait être diagnostiquée (panne dangereuse détectée). Selon le mode de fonctionnement, voir 9.4.3.1.3 pour les actions spécifiées.

9.4.8 Implémentation matérielle

Le FS-PLC doit être implémenté en fonction de la conception matérielle du FS-PLC.

Au cours du processus de conception et de développement, les informations suivantes doivent être compilées par le fabricant du FS-PLC et doivent être disponibles en vue d'une évaluation:

a) spécification des fonctions et interfaces pouvant être utilisées par les fonctions de sécurité (par exemple, contraintes d'application, limitations de communication);

b) estimations des taux de défaillance aléatoire du matériel qui pourraient provoquer une défaillance dangereuse du système et qui sont détectées par des essais de diagnostic (voir 9.4.4);

c) estimations des taux de défaillance aléatoires du matériel qui pourraient provoquer une défaillance dangereuse du système et qui ne sont pas détectées par des essais de diagnostic (voir 9.4.4);

d) limites environnementales pour garantir la validité des taux de défaillance;

e) l'environnement mécanique et climatique (par exemple, vibrations, chocs, température, humidité) auquel le FS-PLC est destiné;

f) la durée de vie maximale déclarée par le fabricant du FS-PLC qui doit être de 20 ans ou moins, sauf si le fabricant du FS-PLC peut justifier une durée de vie prolongée en fournissant des preuves basées sur des calculs, montrant que les données de fiabilité sont valides pour cette durée de vie prolongée.

NOTE Certains composants individuels d'un FS-PLC ont des durées de vie inférieures à 20 ans. Les exemples typiques sont les suivants: batteries, condensateurs électrolytiques, DEL, etc. Si nécessaire, le remplacement périodique de ces composants est géré dans le cadre des procédures de maintenance normales spécifiées par le fabricant du FS-PLC. La limite de 20 ans concernant la durée de vie maximale vise à couvrir la majeure partie des composants du FS-PLC sans durée de vie connue.

g) méthode et intervalle des essais périodiques (ainsi que la base pour l'exigence) et/ou les exigences de maintenance;

h) couverture de diagnostic interne au FS-PLC;

i) intervalle d'essai de diagnostic interne au FS-PLC;

j) durée moyenne de rétablissement (MTTR) et durée moyenne de dépannage (MRT), si applicable;

k) taux de défaillance non dangereuse (SFF);

l) tolérance aux pannes matérielles;

m) limites d'application recommandées pour éviter les défaillances systématiques;

n) déclassements appliqués aux composants utilisés (voir 9.4.9);

o) niveaux d'intégrité de sécurité qui peuvent être déclarés pour les systèmes relatifs à la sécurité pour lesquels le FS-PLC sera utilisable;

p) révision matérielle du FS-PLC;

q) preuves documentaires qu'un FS-PLC a été validé (voir 9.7).

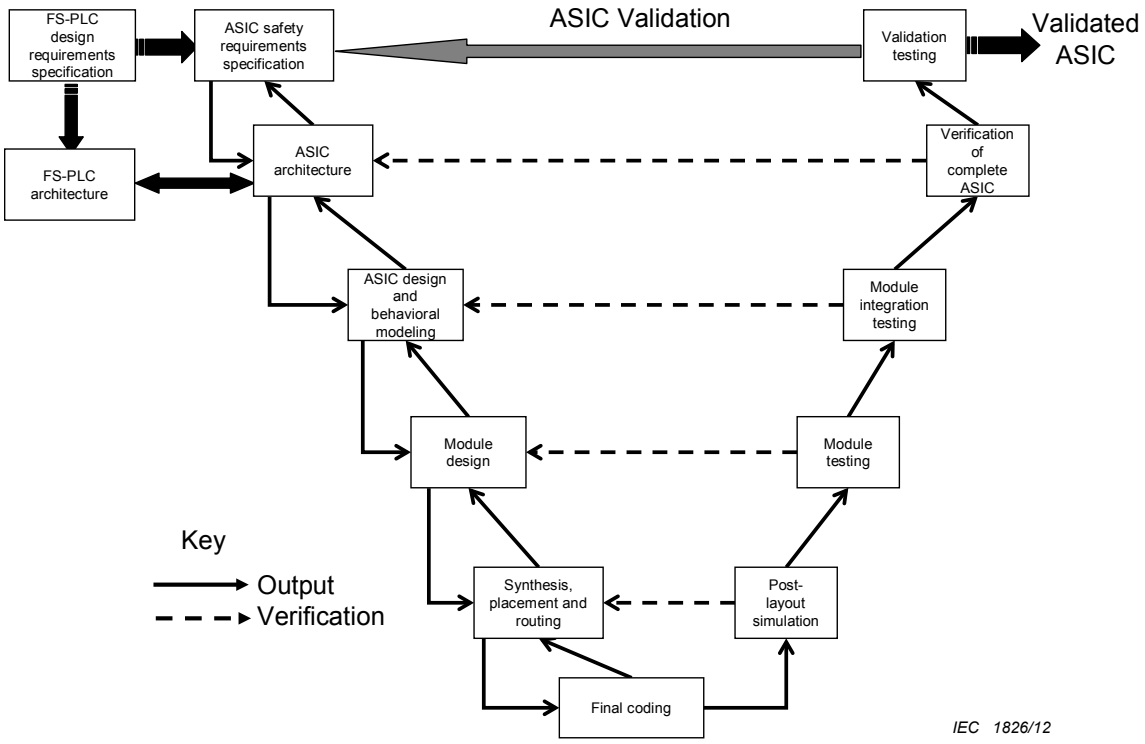
9.4.9 Déclassement des composants

Il est attendu que le fabricant utilise une bonne pratique d'ingénierie et qu'il implémente des principes de déclassement, y compris le déclassement des composants.

Les composants doivent fonctionner à des valeurs inférieures aux valeurs maximales spécifiées par le fabricant des composants dans les conditions de fonctionnement les plus défavorables: tension, courant, température, durée, etc. Dans les cas où cela n'est pas réalisable, la vérification de l'adéquation du composant sélectionné (ou uniquement disponible) pour la ou les applications prévues doit être exigée. Le composant doit être présumé non valable tant qu'il n'a pas été qualifié différemment.

9.4.10 Conception et développement des circuits intégrés spécifiques

Un modèle en V détaillé du cycle de développement des circuits intégrés pour la conception de circuits intégrés spécifiques est représenté à la Figure 10. Si un autre cycle de développement des circuits intégrés spécifiques est utilisé, il doit être spécifié comme faisant partie de la gestion des activités de sécurité fonctionnelle (voir 5.4).



Légende

Anglais	Français
ASIC Validation	Validation des circuits intégrés spécifiques
FS-PLC design requirements specification	Spécifications des exigences de conception du FS-PLC
ASIC safety requirements specification	Spécification des exigences de sécurité des circuits intégrés spécifiques
FS-PLC architecture	Architecture du FS-PLC
ASIC architecture	Architecture des circuits intégrés spécifiques
ASIC design and behavioural modelling	Conception des circuits intégrés spécifiques et modélisation du comportement
Module design	Conception des modules
Validation testing	Essais de validation
Validated ASIC	Circuit intégré spécifique validé
Verification of complete ASIC	Vérification de circuit intégré spécifique complet
Module integration testing	Essais d'intégration de modules
Module testing	Essais de modules
Key	Légende
Output	Sortie
Verification	Vérification
Synthesis, placement and routing	Synthèse, positionnement et routage
Post-layout simulation	Simulation post-conception
Final coding	Codage final

Figure 10 – Cycle de développement des circuits intégrés spécifiques (modèle en V)

9.4.11 Techniques et mesures permettant d'empêcher l'introduction de pannes dans les circuits intégrés spécifiques

Un groupe approprié de techniques et des mesures essentielles doivent être utilisés pour empêcher l'introduction de pannes au cours de la conception et du développement des circuits intégrés spécifiques. Selon la réalisation technique, une différenciation entre les circuits intégrés spécifiques numériques complets et semi-personnalisés, et les CI programmables par l'utilisateur (FPGA/PLD/CPLD) est nécessaire. Des techniques et des mesures adaptées qui prennent en charge la réalisation de propriétés pertinentes sont définies dans la CEI 61508-2.

9.5 Matériel, logiciel intégré et intégration du FS-PLC

La phase d'intégration du cycle de vie de sécurité d'un FS-PLC consiste essentiellement en des essais fonctionnels, ainsi qu'en des essais comportementaux ou statistiques. Ces essais doivent montrer que tous les modules, y compris leurs parties, interagissent correctement pour exécuter leur fonction prévue.

Les essais d'intégration du FS-PLC doivent documenter les informations suivantes:

- la version de la spécification d'essai utilisée;
- les critères d'acceptation des essais d'intégration;
- la version du FS-PLC faisant l'objet d'essais;
- les outils et équipements utilisés avec des données d'étalonnage;
- les résultats de chaque essai;
- les différences entre les résultats attendus et réels; et
- l'analyse réalisée et les décisions prises quant à la poursuite de l'essai ou à l'émission d'une demande de modification (dans les cas où des différences existeraient).

Les résultats de conception et de développement de matériel programmable sont inclus dans le logiciel embarqué, Figure 3, case 19, lorsque leur fonction de sécurité du FS-PLC et les exigences relatives au niveau d'intégrité de sécurité sont satisfaites.

Une fois que le matériel programmable et le logiciel embarqué ont été intégrés, des outils d’ingénierie et des résultats de conception et de développement de matériel non programmable le sont également, Figure 3, case 20. Au cours de cette intégration, la fonction de sécurité du FS-PLC et les exigences relatives au niveau d'intégrité de sécurité doivent être satisfaites.

Même si la séquence est présentée comme intégrant un matériel programmable avant un matériel non programmable, il ne s'agit pas là d'une exigence. La spécification d'essai doit définir la séquence.

9.6 Procédures de fonctionnement et de maintenance du matériel

9.6.1 Objectif

L’objectif des exigences de 9.6.2 consiste à permettre au fabricant du FS-PLC de développer des procédures pour s'assurer que la sécurité fonctionnelle requise du FS-PLC est maintenue au cours du fonctionnement et de la maintenance.

9.6.2 Exigences

Les procédures de fonctionnement et de maintenance du FS-PLC doivent être préparées et doivent spécifier les informations suivantes:

a) les actions de routine qu’il est nécessaire d’exécuter pour maintenir la sécurité fonctionnelle "conforme à la conception" du FS-PLC, y compris le remplacement de

routine des composants présentant une durée de vie prédéfinie (par exemple, ventilateurs, batteries, etc.)

- mise à jour et remplacement du logiciel embarqué,
- remplacement du logiciel d'application total ou partiel,
- mises à jour et remplacement du matériel;

b) les actions et contraintes nécessaires (par exemple, lors de l'installation, démarrage, fonctionnement normal, essais individuels, perturbations prévisibles, pannes ou défaillances et arrêt) pour empêcher un état non sécurisé et/ou réduire les conséquences d'un événement dangereux;

c) les procédures et la documentation lors de la survenue de pannes ou de défaillances dans le FS-PLC, y compris

- procédures pour diagnostics et réparations de pannes,
- mode opérationnel lors de la défaillance,
- indications de DEL/diagnostic,
- registres de statut/diagnostic,
- procédures permettant de signaler des défaillances,
- procédures permettant d'analyser des défaillances,
- procédures de revalidation;

d) les procédures et la documentation permettant d'appliquer une maintenance sur le FS-PLC doivent être spécifiées dans les exigences concernant le rapport de maintenance.

e) les outils nécessaires à l'analyse de défaillance, à la maintenance et à la revalidation, ainsi qu'aux procédures permettant d'appliquer une maintenance sur les outils et les équipements.

NOTE 1 Les procédures de fonctionnement et de maintenance du FS-PLC incluent les procédures de modifications logicielles (voir Article 15).

Le fabricant du FS-PLC doit mettre à niveau, si nécessaire, les procédures de fonctionnement et de maintenance basées sur des entrées telles que (1) les résultats d'audits de sécurité fonctionnelle réalisés par des utilisateurs du FS-PLC, (2) les essais effectués sur le FS-PLC et (3) les rapports périodiques.

Les actions de maintenance de routine exigées pour maintenir la sécurité fonctionnelle (conforme à la conception) du FS-PLC doivent être déterminées par une méthode systématique. Par exemple par:

- examen d’arbres de panne,
- analyse des effets et des modes de défaillance.

NOTE 2 La prise en compte des facteurs humains constitue une partie clé de la détermination des actions nécessaires et de la ou des interfaces appropriées avec le FS-PLC.

NOTE 3 Des essais de sûreté sont effectués à la fréquence nécessaire pour atteindre la mesure de défaillance cible.

NOTE 4 La fréquence des essais de sûreté, l'intervalle des essais de diagnostic et la durée de la réparation ultérieure dépendent de plusieurs facteurs (voir l'Annexe B de la CEI 61508-6:2010), y compris;

- la mesure de défaillance cible associée au niveau d'intégrité de sécurité,
- l’architecture,
- la couverture de diagnostic des essais de diagnostic, et
- le taux de demande attendu.

NOTE 5 Il est probable que la fréquence des essais de sûreté et l'intervalle des essais de diagnostic aient une importance capitale quant à la réalisation de l'intégrité de sécurité matérielle. L'une des principales raisons

d'effectuer une analyse de fiabilité matérielle (voir 9.4.3.2.2) est de s'assurer que les fréquences des deux types d'essais sont appropriées pour l'intégrité de sécurité matérielle cible.

Les procédures de fonctionnement et de maintenance du FS-PLC doivent être évaluées quant à leur impact éventuel sur l'équipement commandé.

Pour éviter les pannes et les défaillances lors des procédures de fonctionnement et de maintenance du FS-PLC, un groupe approprié de techniques et de mesures conforme au Tableau B.4 de la CEI 61508-2:2010 doit être utilisé.

9.7 Validation de la sécurité du matériel

9.7.1 Généralités

Le résultat de la phase de validation doit inclure: des références spécifiques au plan de validation (9.3), des exigences spécifiques du FS-PLC, un équipement d'essai utilisé lors de la validation, des données d'étalonnage d'équipement d'essai et des résultats pour chaque essai.

Cette phase du cycle de vie est effectivement exécutée au cours de plusieurs autres phases du cycle de vie. Par exemple, lors de la conception et du développement, les sorties doivent faire l'objet d'essais pour s'assurer de leur exactitude et de leur cohérence avec les entrées. De plus, il doit être démontré que les pannes et les défaillances spécifiques traitées en 9.4.4.3 sont détectées.

L'objectif des exigences de cette phase consiste à confirmer que le FS-PLC satisfait, en tous points, aux exigences pour la sécurité fonctionnelle en termes de fonctions de sécurité requises et d'intégrité de sécurité (voir 9.1).

9.7.2 Exigences

La validation du FS-PLC doit être effectuée conformément à un plan préparé de validation de la sécurité (voir 9.3).

NOTE 1 La validation d'un FS-PLC, système relatif à la sécurité électronique et programmable, comprend la validation du matériel et du logiciel. Les exigences pour la validation du logiciel se trouvent dans l'Article 10.

Tous les équipements de mesure d'essai utilisés pour la validation doivent être étalonnés conformément à une norme positionnée par rapport à une norme nationale, si elle existe, ou à une procédure dûment reconnue. Le bon fonctionnement de tous les équipements d'essai doit être vérifié.

Chaque fonction de sécurité spécifiée dans les exigences pour le FS-PLC (voir Article 6), et toutes les procédures de fonctionnement et de maintenance du FS-PLC doivent être validées par un essai et/ou une analyse.

La documentation appropriée des essais de validation de la sécurité du FS-PLC doit être produite et doit stipuler pour chaque fonction de sécurité

a) la version du plan de validation de la sécurité du FS-PLC en cours d'utilisation;
b) la fonction de sécurité soumise à l'essai (ou à l'analyse), ainsi que les références spécifiques à l'exigence spécifiée au cours de la planification de la validation de la sécurité du FS-PLC;
c) les outils et équipements utilisés, ainsi que les données d'étalonnage;
d) les résultats de chaque essai;
e) les différences entre les résultats attendus et les résultats réels.

NOTE 2 Une documentation séparée n'est pas nécessaire pour chaque fonction de sécurité, mais les informations des points a) à e) s'appliquent à toutes les fonctions de sécurité. Lorsque des informations ne sont pas identiques pour des fonctions de sécurité différentes, les différences sont indiquées.

Lorsque des différences existent (c'est-à-dire que les résultats réels diffèrent des résultats attendus dans une proportion dépassant les tolérances spécifiées), les résultats des essais de validation de la sécurité du FS-PLC doivent être documentés, y compris

1) l'analyse réalisée; et
2) la décision prise quant à la poursuite de l'essai ou à l'émission d'une demande de modification et au retour à une partie antérieure de l'essai de validation.

Le fabricant du FS-PLC ne doit mettre que les résultats des essais de validation de la sécurité du FS-PLC à la disposition du développeur de l'équipement commandé ou du système électrique/électronique/électronique programmable relatif à la sécurité nécessaires pour leur permettre de satisfaire aux exigences concernant la validation de la sécurité générale dans la CEI 61508-1.

Pour éviter les pannes au cours de la validation de la sécurité du FS-PLC, un groupe approprié de techniques et de mesures (voir la CEI 61508-2) doit être utilisé.

9.8 Vérification du matériel

9.8.1 Objectif

L'objectif de 9.8.1 consiste à confirmer que les activités requises de chaque phase sont réalisées et que les résultats sont enregistrés.

NOTE A des fins pratiques, toutes les activités de vérification du matériel ont été rassemblées en 9.8. Cependant, elles sont en réalité exécutées sur plusieurs phases.

9.8.2 Exigences

La vérification des éléments livrables de chaque phase du cycle de vie relatif au matériel du FS-PLC doit être planifiée, exécutée et documentée. Ces vérifications doivent être basées sur les entrées spécifiées dans la phase du cycle de vie. Les techniques/outils utilisés dans la vérification incluent, par exemple:

- les examens de la documentation de la phase,
- les examens de conception,
- les essais fonctionnels et
- les essais environnementaux.

NOTE Il ne faut pas confondre la vérification avec l'étalonnage ou la validation.

10 Conception et développement du logiciel du FS-PLC

10.1 Généralités

Les exigences de l'Article 10 sont issues des exigences logicielles spécifiques contenues dans la spécification des exigences de sécurité fonctionnelle du FS-PLC.

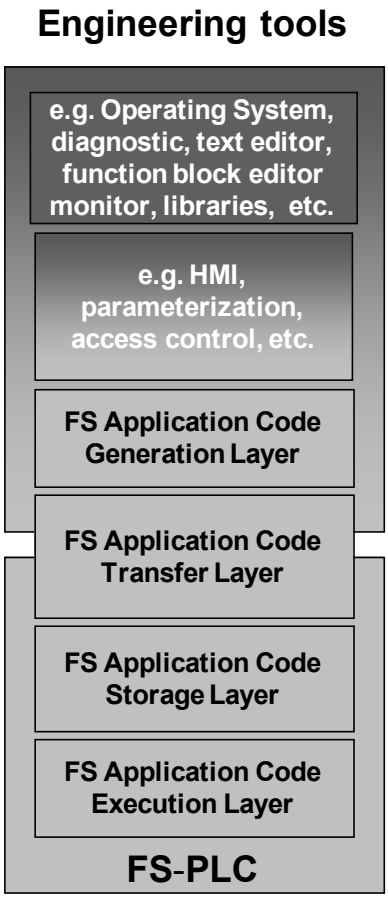
L'Article 10 concerne le logiciel embarqué du FS-PLC, les outils d'ingénierie et les outils logiciels de développement d'applications, mais exclut les logiciels d'application utilisateur.

La Figure 11 présente le modèle de logiciel de référence de base utilisé dans la présente partie. Le modèle de référence est un exemple d'implémentation du logiciel de sécurité fonctionnelle; d'autres architectures sont également possibles.

En règle générale, les outils d'ingénierie incluent un générateur de code de l'application de la sécurité fonctionnelle et une interface homme-machine pour éditer le code source de l'application de la sécurité fonctionnelle et contrôler le statut du FS-PLC. Une analyse de l'impact pertinent quant à la sécurité des outils d'ingénierie doit être exécutée.

Le logiciel embarqué du FS-PLC reçoit le code de l'application de la sécurité fonctionnelle par le biais de la couche de transfert du code de l'application de la sécurité fonctionnelle et le range dans la couche de stockage de l'application de la sécurité fonctionnelle.

La couche d'exécution du code de l'application de la sécurité fonctionnelle charge le code de l'application de la sécurité fonctionnelle à partir de la couche de stockage de l'application de la sécurité fonctionnelle, puis l'exécute.



Légende

Anglais	Français
Engineering tools	Outils d'ingénierie
e.g. Operation System, diagnostic, text editor, function block editor, monitor, libraries, etc.	par exemple, système d'exploitation, diagnostic, éditeur de texte, éditeur de bloc de fonction, écran, bibliothèques, etc.
e.g. HMI, parameterization, access control, etc.	par exemple, HMI, paramétrage, contrôle d'accès, etc.
FS Application Code Generation Layer	Couche de génération du code de l'application de la sécurité fonctionnelle
FS Application Code Transfer Layer	Couche de transfert de code de l'application de la sécurité fonctionnelle
FS Application Code Storage Layer	Couche de stockage du code de l'application de la sécurité fonctionnelle
FS Application Code Execution Layer	Couche d'exécution du code de l'application de la sécurité fonctionnelle
FS-PLC	FS-PLC

Figure 11 – Modèle du FS-PLC et couches pour les outils d'ingénierie

Les exigences logicielles du FS-PLC dérivées des exigences logicielles spécifiques, incluses dans la spécification des exigences de sécurité fonctionnelle du FS-PLC, seront, dans la plupart des cas, satisfaites par une combinaison formée par le logiciel embarqué et les outils d'ingénierie. C'est la combinaison de ces deux types d'éléments qui est requise pour fournir les caractéristiques qui correspondent aux paragraphes suivants. Cette distinction exacte entre le logiciel embarqué et les outils d'ingénierie dépend de l'architecture choisie du système.

10.2 Exigences

Toutes les exigences de la CEI 61508-3 s'appliquent au logiciel du FS-PLC et aux outils de prise en charge en ligne. Il s'agit d'outils logiciels pouvant influencer directement le système relatif à la sécurité au cours de son exécution.

10.3 Classification des outils d'ingénierie

Les outils d'ingénierie du FS-PLC doivent être rangés dans les classes suivantes:

- T1: ne génère aucune sortie pouvant directement ou indirectement contribuer au code exécutable (y compris les données) du système relatif à la sécurité;
- T2: prend en charge l'essai ou la vérification de la conception ou du code exécutable, des erreurs dans l'outil peuvent ne pas permettre de détecter des défauts, mais ne peuvent pas créer directement des erreurs dans le logiciel exécutable;
- T3: génère des sorties pouvant directement ou indirectement contribuer au code exécutable du système relatif à la sécurité.

NOTE 1 Les exemples de T1 incluent: Editeur de texte ou les outils de conception ou de prise en charge des exigences sans capacité de génération de code automatique; outils de contrôle de configuration.

NOTE 2 Les exemples de T2 incluent: Générateur de faisceaux d'essai; outil de mesure de couverture d'essai; outil d'analyse statique.

NOTE 3 Les exemples de T3 incluent: Optimiseur dans lequel la relation entre le programme de code source et le code exécutable généré n'est pas évident; compilateur intégrant un package d'exécution au code exécutable.

NOTE 4 Cette classification est réalisée d'après la CEI 61508-4:2010, 3.2.11.

Des exemples de répartition des outils d'ingénierie du FS-PLC dans des classes se trouvent dans le Tableau 7. Cette distinction exacte entre le logiciel embarqué et les outils d'ingénierie dépend de l'architecture du système sélectionné.

Tableau 7 – Exemples de classifications d'outils

Classe d'outils[a]	Classe	Raisonnement
Outils d'ingénieries – PC, système d'exploitation diagnostic, éditeur de texte, éditeur de bloc de fonction, écran, bibliothèques, etc.	T1	La sortie du ou des outils est vérifiée et validée par l'utilisateur avant toute utilisation dans un FS-PLC
Outils d'ingénieries – HMI, paramétrage, contrôle d'accès, etc.	T1	Ne génère aucune sortie pouvant directement ou indirectement contribuer au code exécutable (y compris les données) du système relatif à la sécurité
Outils d'ingénieries – Couche de génération du code d'application de la sécurité fonctionnelle, HMI, paramétrage	T3	Génère des sorties pouvant directement ou indirectement contribuer au code exécutable du FS-PLC
Outils d'ingénieries – Couche de transfert du code d'application de la sécurité fonctionnelle	T3	Peut directement ou indirectement contribuer au code exécutable du système relatif à la sécurité
FS-PLC – Couche de stockage du code d'application	n/a	Microprogramme système intégré
FS-PLC – Couche d'exécution du code d'application	n/a	Microprogramme système intégré
[a] Les outils peuvent avoir des classifications différentes en fonction de leur capacité de génération de sortie ou de code.		

Une fois cette classification déterminée, les exigences applicables de la CEI 61508-3 doivent être respectées.

10.4 Planification de la validation de la sécurité logicielle

NOTE 1 Cette phase du cycle de vie d'un FS-PLC est généralement accomplie parallèlement aux exigences de conception et de développement du logiciel, voir 10.2.

NOTE 2 Voir le 7.3.2.2 de la CEI 61508-3:2010.

La planification de la validation du logiciel est réalisée grâce à la spécification des étapes à effectuer pour démontrer la conformité à la spécification des exigences de sécurité fonctionnelle logicielles du FS-PLC (voir Article 6).

Le plan de validation de la sécurité fonctionnelle doit inclure les procédures à suivre, une description de l'environnement d'essai et des critères de succès/d'échec.

11 Validation de la sécurité du FS-PLC

L'objectif de l'Article 11 consiste à s'assurer que le système FS-PLC satisfait, en tous points, aux exigences relatives à la sécurité fonctionnelle en termes de fonctions de sécurité requises et d'intégrité de sécurité définies à l'Article 6.

Le fabricant doit développer et exécuter un plan de validation à partir des informations définies aux Articles 6 et 12.

Un rapport de validation doit être développé et conservé par le fabricant du FS-PLC. Ce rapport doit inclure des rapports d'essai de type. Ces rapports d'essai de type doivent couvrir les essais minimaux au niveau du système FS-PLC spécifiés aux Articles 12 à 13.2.

Le fabricant du FS-PLC doit soumettre ce dernier à une évaluation de la sécurité réalisée par une organisation/un service indépendant pour un développement de SIL 3, tel que spécifié à l'Article 14, (voir Tableau 5 de la CEI 61508-1:2010).

12 Essais de type du FS-PLC

12.1 Généralités

Les essais de type du système FS-PLC doivent être effectués pour s'assurer que ce dernier fonctionne tel que spécifié dans les environnements auxquels il est destiné.

Les essais de type doivent couvrir les essais minimaux au niveau du système FS-PLC spécifiés de 12.2 à 12.5 et doivent suivre le plan de validation du FS-PLC évoqué en 9.3.

Un rapport d'essai de type doit être rédigé et conservé par le fabricant du FS-PLC.

12.2 Exigences d'essai de type

Dans le cadre des campagnes d'essai du système FS-PLC, une procédure de vérification de bon fonctionnement (PVBF) et un programme d'essai PVBF doivent être fournis. Dans la mesure du possible, la PVBF doit être entièrement automatisée et intégrée dans le cadre du programme d'essai PVBF, et les instruments externes ainsi que les étapes d'essais manuels doivent être réduits dans le cadre de la PVBF. Sauf spécification contraire, ces exigences doivent être vérifiées au cours des essais de type: climatiques, mécaniques, CEM, tolérance aux pannes, etc.

Le programme d'essai PVBF et la PVBF doivent être utilisés pour vérifier:

a) la configuration correcte de l'équipement FS-PLC à l'essai (EUT);
b) le bon fonctionnement de l'EUT du FS-PLC avant, pendant et après les essais de type, tel que spécifié au Tableau 8;
c) au cours des essais, sauf spécification contraire, (voir Tableau 8, sécurité fonctionnelle des critères de performances), les événements suivants ne doivent pas se produire:
    i) destruction du matériel,
    ii) modification fortuite du système d'exploitation et des programmes d'essai et/ou altération de leur exécution,
    iii) modification fortuite des données système et d'application stockées ou échangées,
    iv) comportement erratique ou fortuit de l'EUT du FS-PLC. Par exemple:
        1) dérive de l'exactitude du point E/S analogique par rapport aux limites spécifiées,
        2) dérive des temps de réponse de communication et des taux d'erreur minimaux par rapport aux limites spécifiées,
        3) dérive de l'analyse du système et des temps de réponse au-delà des limites calculées dans les cas les plus défavorables,
        4) dérive des temporisateurs de programmes de commande par rapport aux limites spécifiées,
        5) échec de l'exécution d'une analyse,
        6) perte de l'heure locale correcte,
d) tous les différents modes opérationnels du système significatifs pour une implémentation typique du FS-PLC telle qu'un démarrage et un arrêt, un redémarrage à froid/à chaud, "exécution normale", "arrêt normal", "programmation/contrôle via HMI externe", etc.
e) conditions d'initialisation et de réinitialisation de tous les composants du système lors du démarrage et de l'arrêt contrôlés.

Gardez à l'esprit les limitations des instruments qui empêchent la vérification en temps réel de tout ou partie de ces éléments lors des essais de type. Par exemple, lorsque l'on tente de vérifier les limites d'exactitude publiées et que les sorties analogiques sont rebouclées aux entrées analogiques. Dans ce type de cas, les limites spécifiées des essais de vérification du système sont aussi réduites que possible. Autres exemples: modes de fonctionnement, conditions d'initialisation et de réinitialisation, etc.

La PVBF doit, le cas échéant, employer l'EUT du FS-PLC de sorte que:

a) toutes les fonctions et parties pertinentes de l'EUT du FS-PLC doivent fonctionner afin que les chemins d'informations à destination/provenant de chaque type de module/fonction soient employés et contrôlés quant à l'intégrité de leur comportement;

b) un sous-ensemble nécessaire et suffisant des canaux E/S et de communication, ainsi que de leurs caractéristiques, spécifié par le fabricant, doit être employé et contrôlé quant à l'intégrité de son comportement; (Voir 2.2 de la CEI 61131-2:2007);

c) tous les moyens de retour d'informations pertinentes relatives au statut de système interne et externe, tels que les écrans DEL, les signaux d'alarme ou les alarmes système, doivent être employés et l'intégrité de leur comportement contrôlée;

   NOTE Les limitations des instruments empêchent parfois la vérification en temps réel d'une partie des fonctions du système (par exemple, indicateurs de panneau avant ou pendant les essais de niveau élevé).

d) le programme d'essai PVBF/la PVBF doit exercer l'EUT du FS-PLC afin de refléter, dans la mesure du possible, les conditions de temps de réponse les plus défavorables: modification rapide des entrées et des sorties, communications externes continues, communications poste-à-poste continues, etc. La mesure des temps de réponse, le cas échéant, doit prendre en compte les activités suivantes du système, dont l'exécution peut prendre plus de temps:

   i) énoncés d'impression conditionnelle,

   ii) manipulations d'ensembles ou calculs de virgules flottantes conditionnels,

   iii) salve d'événements, plusieurs points E/S modifiés simultanément,

   iv) salve de messages de communication à partir de sources externes,

   v) contrôle à distance des points E/S au cours d'une salve d'événements provoquant une salve correspondante de messages générés en interne,

   vi) perte d'une liaison de communication à partir d'éléments ouverts, de courts-circuits ou d'un brouillage électromagnétique donnant lieu à des dépassements du temps de latence internes ou à des réponses erronées,

   vii) comportement lors de l'application ou en présence d'une panne aléatoire unique du matériel donnant lieu à des dépassements des temps de latence internes ou à des réponses erronées;

e) au cours des essais de type, l'EUT du FS-PLC doit être exercé avec des sources d'alimentation électrique aux niveaux spécifiés dans la CEI 61131-2 (tension, fréquence, etc.).

Au cours des essais de type, la PVBF doit pouvoir vérifier l'intégrité des performances par rapport aux critères suivants lors de leur soumission aux diverses conditions/restrictions requises ci-dessous.

Tableau 8 – Critères de performances

Critères de performances	Fonctionnement pendant l'essai	Fonctionnement après l'essai
A	Le système FS-PLC doit continuer à fonctionner comme prévu. Aucune dégradation ou perte de fonction ou de performances.	Le système FS-PLC doit continuer à fonctionner comme prévu.
B	Il est permis que les performances du FS-PLC se dégradent comme suit: 1) il est admis que des valeurs analogiques ne varient pas ± que le % de la déviation maximale spécifié par le fabricant, 2) alarmes système du FS-PLC parasites en l'absence de modification d'état: par exemple, de redondant à non redondant, 3) un changement d'état intentionnel Les éléments suivants ne sont pas autorisés: • perte de contrôle ou modification du mode de fonctionnement fortuite: c'est-à-dire, perte de données, perte de communication, modifications d'états E/S numériques, de redondant à non redondant. • perte irréversible de données stockées. • modification des temps de réponse du système FS-PLC les plus défavorables (voir la NOTE 1).	Le système FS-PLC doit continuer à fonctionner comme prévu. La dégradation temporaire des performances doit être auto-récupérable.
C	La perte de fonction du FS-PLC est autorisée mais sans destruction du matériel ou du logiciel (programme ou données).	Le système FS-PLC doit continuer à fonctionner comme attendu automatiquement, après un redémarrage manuel ou des cycles de mise hors/sous tension.
SF	Fonctions de l'EUT du FS-PLC destinées à l'application de sécurité: 1) Identiques aux critères de performances A, ou 2) Peuvent être perturbées de manière temporaire ou permanente si l'EUT réagit à une perturbation d'une façon détectable et qu'il conserve ou atteint (dans un laps de temps spécifié) un ou plusieurs états définis du FS-PLC. Il est permis que des fonctions non destinées à des applications de sécurité soient perturbées de manière temporaire ou permanente	La destruction de composants relatifs à la sécurité est autorisée si l'état défini de l'EUT du FS-PLC est conservé ou atteint dans un laps de temps spécifié. La destruction des composants non relatifs à la sécurité est autorisée.

NOTE 1 Les temps de réponse du système FS-PLC incluent la durée maximale entre une modification d'étape sur un point d'entrée quelconque du système FS-PLC et une modification d'étape d'un point de sortie quelconque du système FS-PLC, de même qu'entre une modification d'étape sur un point d'entrée quelconque du système FS-PLC et une modification d'étape sur un point de sortie quelconque d'un autre système FS-PLC via une liaison poste-à-poste.

NOTE 2 Source: modification du 6.2 de la CEI 61326-3-1:2008 et du 8.3.2 de la CEI 61131-2:2007.

12.3 Exigences d'essai climatiques

Pour les exigences d'essai climatique, voir la CEI 61131-2.

Avant et après chaque essai de résistance environnementale, l'EUT du FS-PLC doit être vérifié quant à son bon fonctionnement via la PVBF. De plus, au cours de chaque essai de type d'immunité, l'EUT du FS-PLC doit être vérifié quant à son bon fonctionnement via la PVBF.

Des essais particuliers dans des conditions plus sévères que celles de la CEI 61131-2 doivent faire l'objet d'un accord entre le fabricant et l'utilisateur.

12.4 Exigences d'essai mécanique

Pour les exigences d'essai mécanique, voir la CEI 61131-2.

Avant et après chaque essai de résistance mécanique, l'EUT du FS-PLC doit être vérifié quant à son bon fonctionnement via la PVBF. De plus, au cours de chaque essai de type d'immunité, l'EUT du FS-PLC doit être vérifié quant à son bon fonctionnement via la PVBF.

Des essais particuliers dans des conditions plus sévères que celles de la CEI 61131-2 doivent faire l'objet d'un accord entre le fabricant et l'utilisateur.

12.5 Exigences d'essai CEM

12.5.1 Généralités

La CEI/TS 61000-1-2 doit être consultée afin de trouver une méthodologie pour la réalisation de la sécurité fonctionnelle du point de vue des phénomènes électromagnétiques. Cependant, étant donné que les niveaux réels des essais électromagnétiques ne sont pas indiqués ici, les exigences d'essai de 12.5.2 ou de 12.5.3 doivent être utilisées.

Ces exigences ne s'appliquent pas aux fonctions non relatives à la sécurité des équipements ou des systèmes.

Avant, pendant et après chaque essai d'immunité CEM, le système FS-PLC à l'essai doit être vérifié quant à son bon fonctionnement via la PVBF, comme spécifié par les critères de performance et le Tableau 8. Les exigences d'essai d'émissions pour un FS-PLC sont identiques à celles spécifiées dans la CEI 61131-2. Au cours de chaque essai d'émission, le système FS-PLC à l'essai doit être exercé pour simuler un environnement système type. Cela peut être réalisé en utilisant les parties automatisées de la PVBF pour employer le système.

12.5.2 Environnement CEM général

Ce paragraphe 12.5.2 spécifie les exigences d'immunité CEM pour un FS-PLC destiné à être utilisé dans un environnement CEM général, c'est-à-dire un environnement sans restrictions ni contrôles relatifs aux phénomènes CEM.

Les niveaux élevés des essais d'immunité du Tableau 9 et du Tableau 10 ne sont relatifs qu'aux aspects de la sécurité fonctionnelle. Ils ne sont pas applicables pour l'évaluation des aspects de fiabilité et de disponibilité. Les niveaux élevés des essais d'immunité ne s'appliquent qu'aux fonctions relatives à la sécurité présentant un critère de performances spécifique pour la sécurité fonctionnelle (critère de performances SF). Les niveaux élevés des essais d'immunité sont les valeurs d'essai maximales. Des essais supplémentaires avec des valeurs plus élevées ne sont pas exigés en vue de la conformité à la présente norme.

Le Tableau 9 et le Tableau 10 contiennent toutes les exigences d'immunité CEM de la CEI 61131-2.

Tableau 9 – Niveaux d'immunité des essais pour l'accès enveloppe dans un environnement CEM général

Phénomène environnemental	Norme de base	Essai	Niveau des essais	Critères de performances
Décharge électrostatique	CEI 61000-4-2	Contact	±6 kV [a]	SF
		Air	±8 kV [a]	
Fréquences radioélectriques Champ électromagnétique Amplitude modulée	CEI 61000-4-3	2,0 GHz - 2,7 GHz	3 V/m[b]	SF
		1,4 GHz - 2,0 GHz	10 V/m	
		80 GHz - 1,0 GHz	20 V/m[b]	
Champs magnétiques à fréquence industrielle	CEI 61000-4-8	50Hz / 60 Hz	30 A/m[c] Aucun niveau d'essai accru ne s'applique.	SF

a Les niveaux doivent être appliqués conformément aux conditions environnementales décrites dans la CEI 61000-4-2 pour les parties pouvant être accessibles par des personnes autres que le personnel travaillant conformément aux procédures définies pour la commande de l'ESD, mais pas pour l'équipement dont l'accès est exclusivement limité au personnel dûment formé.

b Ces valeurs (supérieures à celles de la CEI 61131-2) doivent être appliquées dans des gammes de fréquence utilisées pour les émetteurs mobiles en général, sauf lorsque des mesures fiables sont effectuées pour éviter d'utiliser un équipement de ce type situé à proximité. Les fréquences ISM doivent être prises en compte individuellement.

c Uniquement applicables aux équipements contenant des dispositifs sensibles aux champs magnétiques.

Tableau 10 – Niveaux d'immunité des essais dans un environnement CEM général

	Phénomène environnemental	**Transitoires rapides en salves**	**Ondes de choc à haute énergie (NOTE)**	**Perturbations radioélectriques**	
	Norme de base	**CEI 61000-4-4**	**CEI 61000-4-5**	**CEI 61000-4-6**	
	Critères de performances	**SF**	**SF**	**SF**	
Interface/port (appellation)	**Interface/port spécifique**	**Niveau des essais**	**Niveau des essais[f]**	**Niveau des essais**	**Valeurs dérivées de**
Puissance de l'équipement (F) et puissance E/S (J) et sortie de puissance auxiliaire (K)	alimentation alternative	3 kV[a] (5/50 ns, 5 kHz)	4 kV CM 2 kV DM	10 V[b] 15 kHz à 80 MHz	CEI 61326-3-1:2008 Tableau 1b
	alimentation continue[e]	3 kV[a] (5/50 ns, 5 kHz)	2 kV CM[,c] 1 kV DM	10 V[b] 15 kHz à 80 MHz	CEI 61326-3-1:2008 Tableau 1c
E/S (C et D)	E/S générale	2 kV[a,d] (5/50 ns, 5 kHz)	2 kV CM	10 V[b] 15 kHz à 80 MHz	CEI 61326-3-1:2008 Tableau 1d
	E/S directement connectée aux réseaux d'alimentation électrique	3 kV[a] (5/50 ns, 5 kHz)	4 kV CM 2 kV DM	10 V[b] 15 kHz à 80 MHz	CEI 61326-3-1:2008 Tableau 1e
Mise à la terre fonctionnelle (H)	-	2 kV[a] (5/50 ns, 5 kHz)	Aucun essai	3 V	CEI 61326-3-1:2008 Tableau 1f
Le niveau d'immunité exigé peut être atteint par le biais de l'utilisation de dispositifs de protection externes.					

a Pour les équipements destinés à être utilisés dans des applications SIL 3, la durée de l'essai au niveau le plus élevé doit être accrue par un facteur de 5, comparativement à la durée indiquée dans la norme de base.
b Les valeurs (supérieures à celles de la CEI 61131-2) doivent être appliquées dans des gammes de fréquence utilisées pour les émetteurs mobiles en général, sauf lorsque des mesures fiables sont effectuées pour éviter d'utiliser un équipement de ce type situé à proximité. Les fréquences ISM doivent être prises en compte individuellement.
c Uniquement dans le cas de lignes au sein d'un immeuble dont la longueur est supérieure à 30 m ou qui se prolongent au-delà de l'immeuble (y compris les lignes des installations extérieures).
d Uniquement dans le cas de lignes >3 m.
e Les connexions CC entre différentes parties d'un équipement/système non connectées à un réseau de distribution CC sont traitées en tant que ports de signal/contrôle E/S.
f DM = mode différentiel, CM = mode commun

12.5.3 Environnement CEM spécifié

Le paragraphe 12.5.3 spécifie les exigences d'immunité CEM pour un FS-PLC destiné à être utilisé dans l'environnement CEM spécifié par le fabricant du FS-PLC.

Les exigences d'immunité CEM spécifiées dans le Tableau 11 et le Tableau 12 incluent les exigences de la CEI 61131-2.

L'environnement d'application industrielle avec un environnement électromagnétique spécifié inclut généralement les caractéristiques suivantes:

- zone industrielle à accès limité;
- utilisation limitée d'émetteur mobile;
- câbles dédiés pour alimentation électrique et lignes de contrôle, de signal ou de communication;

- séparation entre l'alimentation électrique et les câbles de contrôle, de signal ou de communication;
- usine principalement composée de structures métalliques;
- protection contre les surtensions/la foudre grâce à des mesures appropriées (par exemple, structures métalliques d'un immeuble ou utilisation de dispositifs de protection);
- il est admis que des systèmes de chauffage par tuyauterie fonctionnant grâce à l'alimentation alternative principale soient présents;
- absence de poste à haute tension à proximité de zones sensibles;
- présence d'équipement ISM CISPR 11 Groupe 2 n'utilisant des fréquences ISM qu'à basse puissance;
- personnel compétent;
- maintenance périodique des équipements et des systèmes;
- instructions de montage et d'installation pour les équipements et les systèmes.

Une description plus détaillée des caractéristiques types susmentionnées est fournie à l'Annexe B de la CEI 61326-3-2:2008.

Tableau 11 – Niveaux d'essais d'immunité pour les essais enveloppe dans un environnement CEM spécifié

Phénomène environnemental	Norme de base	Essai	Niveau des essais	Critères de performances
Décharge électrostatique	CEI 61000-4-2	Contact	±6 kV [a]	A
		Air	±8 kV [a]	
Fréquences radioélectriques Champ électromagnétique Amplitude modulée	CEI 61000-4-3	2,0 GHz - 2,7 GHz	3 V/m	A
		1,4 GHz - 2,0 GHz	10 V/m	
		80 MHz -1,0 GHz	10 V/m[b]	
Champs magnétiques à fréquence industrielle	CEI 61000-4-8	50 Hz /60 Hz	100 A/m[c]	A

a Les niveaux doivent être choisis conformément aux conditions environnementales décrites dans l'Annexe A de la CEI 61000-4-2:2008 et appliqués aux parties pouvant être accessibles par des personnes autres que le personnel travaillant conformément aux procédures définies pour la commande de l'ESD, mais pas pour l'équipement dont l'accès est exclusivement limité au personnel dûment formé.

b Sauf pour les bandes de fréquence de diffusion UIT 87 MHz à 108 MHz, 174 MHz à 230 MHz et 470 MHz à 790 MHz, pour lesquelles le niveau doit être de 3 V/m.

c Uniquement applicables aux équipements contenant des dispositifs sensibles aux champs magnétiques.

Tableau 12 – Niveaux d'essais d'immunité dans un environnement CEM spécifié

	Phénomène environnemental	**Transitoires rapides en salves**	**Ondes de choc à haute énergie (NOTE)**	**Perturbations radioélectriques**	
	Norme de base	**CEI 61000-4-4**	**CEI 61000-4-5**	**CEI 61000-4-6**	
	Critères de performances	**A**	**A**	**A**	
Interface/Port (appellation)	**Interface/port spécifique**	**Niveau des essais**	**Niveau des essais[f]**	**Niveau des essais**	**Valeurs dérivées de**
Puissance de l'équipement (F) et puissance E/S (J) et sortie de puissance auxiliaire (K)	alimentation alternative	2 kV (5/50 ns, 5 kHz)	2 kV CM 1 kV DM	10 V[a] 10 kHz à 80 MHz	CEI 61326-3-2:2008 Tableau 1b
	alimentation continue[e]	2 kV (5/50 ns, 5 kHz)	1 kV CM 0,5 kV DM	10 V[a] 10 kHz à 80 MHz	CEI 61326-3-2:2008 Tableau 1c
signal/contrôle E/S (C et D)	E/S générale	1 kV[b] (5/50 ns, 5 kHz)	1 kV CM[c] (NOTE)	10 V[b, d] 10 kHz à 80 MHz	CEI 61326-3-2:2008 Tableau 1d
	E/S directement connectée aux réseaux d'alimentation électrique	2 kV (5/50 ns, 5 kHz)	2 kV CM 1 kV DM	10 V[d] 10 kHz à 80 MHz	CEI 61326-3-2:2008 Tableau 1e
Mise à la terre fonctionnelle (H)	-	2 kV[b] (5/50 ns, 5 kHz)	1 kV CM[c] (NOTE)	10 V[d] 10 kHz à 80 MHz	CEI 61326-3-2:2008 Tableau 1f

NOTE Les critères de performances SF sont autorisés.

a Dans la gamme de fréquences 10 kHz à 150 kHz, l'impédance du réseau de couplage/découplage doit être conforme aux exigences d'impédance asymétrique de la CEI 61000-4-6 à une fréquence de 150 kHz. L'étalonnage doit être effectué conformément à la CEI 61000-4-6. Un découplage suffisant peut être démontré si le critère d'impédance est satisfait avec le port AE court-circuité.

b Uniquement dans le cas de lignes >3 m.

c Uniquement dans le cas de lignes au sein d'un immeuble dont la longueur est supérieure à 30 m ou qui se prolongent au-delà de l'immeuble (y compris les lignes des installations extérieures)

d Dans la gamme de fréquences 10 kHz à 150 kHz, l'impédance du réseau de couplage/découplage doit être conforme aux exigences d'impédance asymétrique de la CEI 61000-4-6 à une fréquence de 150 kHz. L'étalonnage doit être effectué conformément à la CEI 61000-4-6. Un découplage suffisant peut être démontré si le critère d'impédance est satisfait avec le port AE court-circuité, puis en circuit ouvert.

e Les connexions CC entre différentes parties d'un équipement/système non connectées à un réseau de distribution CC sont traitées en tant que ports de signal/contrôle E/S.

f DM = mode différentiel, CM = mode commun

13 Vérification du FS-PLC

13.1 Plan de vérification

Le plan de vérification du FS-PLC doit être exécuté et doit contenir au moins les éléments suivants:

- examen de la spécification des exigences;
- examen des processus de conception;
- examen de la conception du matériel (par exemple: schéma du circuit, nomenclature);
- examen de la conception du logiciel embarqué;
- examen de l'adéquation des outils d'ingénierie, uniquement pour les parties pertinentes de la sécurité fonctionnelle. Voir Figure 5;
- examen de la spécification d'essai (essai de module, essai d'intégration);

- examen de la spécification des essais du système et des essais de type;
- analyse des effets et des modes de défaillance (FMEA);
- examen des résultats d'essais (par exemple: essai de module, essai d'intégration, essai du système et essai de type);
- essai de défaillance du matériel (par exemple, simulation, physique);
- analyse de criticité;
- essai de défaillance du logiciel embarqué (par exemple, simulation);
- examen de la méthode de calcul des données de fiabilité (exemple: analyse de cause commune, modélisation de Markov, calcul de Markov).

Ces examens doivent être indépendants et documentés.

13.2 Exigences des essais de génération de panne

Un essai de génération de panne correspond à la génération délibérée d'une panne afin de déterminer son effet sur le fonctionnement du FS-PLC.

Les essais de génération de panne doivent être effectués dans le cadre des essais de vérification avec les objectifs suivants:

- pour vérifier que les effets de la défaillance prévus lors de la FMEA du matériel sont corrects, et donc que leurs taux de défaillance sont inclus dans la classification des pannes correcte (voir 9.4.7);
- pour vérifier que les essais de diagnostic lors de l'exécution réagissent comme prévu lors de la conception;
- pour vérifier que la réaction concernant les pannes du FS-PLC est comme prévue lors de la conception;
- pour vérifier que les processus de maintenance en ligne autorisés (par exemple, échange d'un module) fonctionnent comme prévu lors de la conception.

Les essais de génération de panne peuvent être exécutés au niveau d'un composant ou d'un niveau plus élevé sur un élément ou un sous-système.

Voici quelques exemples d'essais de génération de panne au niveau d'un composant:

– positionnement d'un composant en circuit ouvert;
– positionnement d'un composant en court-circuit;
– blocage d'une sortie CE numérique à l'état incorrect.

Voici quelques exemples d'essais de génération de panne au niveau d'un élément ou d'un sous-système:

a) retrait ou insertion d'un module lors de l'exécution;
b) simulation d'une sur- ou sous-tension du rail de tension;
c) corruption des données transférées entre des éléments ou des sous-systèmes.

Le Tableau 13 présente l'efficacité exigée des essais de génération de panne, en fonction du niveau d'intégrité de sécurité cible et de la couverture de diagnostic exigée.

En cas de faible efficacité, des essais doivent être appliqués au moins au niveau d'un élément ou d'un sous-système, y compris des connexions de données entre différentes unités.

En cas d'efficacité moyenne et élevée, des essais doivent également être appliqués au niveau d'un composant, et ce avec suffisamment de rigueur pour vérifier la couverture de diagnostic déclarée. Des essais doivent être appliqués

- là où l'effet de défaillance prévu par la FMEA n'est pas clarifié par l'inspection;
- la où le taux de défaillance de l'effet de défaillance est significatif;
- la où des essais de diagnostic lors de l'exécution sont destinés à détecter la panne.

NOTE La rigueur requise des essais de génération de panne dépend de la couverture de diagnostic déclarée, de l'efficacité de la FMEA, de l'architecture du FS-PLC, etc.

La PVBF doit être utilisée pour vérifier le bon fonctionnement du FS-PLC

- avant d'effectuer un essai de génération de panne;
- au cours d'un essai de génération d'une panne, si la réaction attendue consiste à continuer de fonctionner normalement;
- après la restitution consécutive à un essai de génération de panne.

Avant, pendant et après chaque essai de génération de panne, l'EUT du FS-PLC doit être vérifié quant à son bon fonctionnement en utilisant la PVBF.

Tableau 13 – Essai de tolérance aux pannes, efficacité exigée

Efficacité exigée des essais de génération de panne			
Couverture de diagnostic exigée	SIL1	SIL2	SIL3
<90 %	Faible	Faible	Moyenne
≥90 %	Elevée	Elevée	Elevée

La méthode d'application des essais de génération de panne, les essais spécifiques à appliquer et les résultats exigés de chaque essai doivent être stipulés dans le plan des essais de vérification. La quantité et la rigueur des essais de génération de panne doivent être acceptées par le fabricant du FS-PLC ainsi que par le contrôleur, et ce, en tenant compte de la complexité du FS-PLC, de son application prévue et de son niveau d'intégrité de sécurité.

Après la sortie du produit, il peut être nécessaire de répéter certains essais de génération de panne pour vérifier une modification ou une amélioration du produit. Le domaine d'application du nouvel essai exigé doit être déterminé comme faisant partie de l'analyse de l'impact de la modification.

13.3 Comparaison des produits «tels que qualifiés» et «tels qu'expédiés»

Le fabricant doit prendre des mesures pour garantir que tous les produits expédiés à un client donné sont de qualité supérieure ou égale à celle des unités utilisées lors des essais de type.

NOTE La liste suivante contient des exemples de techniques pouvant être utilisées:

a) lors de l'utilisation de marges conventionnelles lors des essais de type. Par exemple:

   1) température de fonctionnement: 10 °C au-delà des spécifications publiées supérieures et inférieures,

   2) humidité de fonctionnement: 30 % au-dessus de la limite de fonctionnement supérieure ou 95 % HR, selon la donnée la plus importante,

   3) vibrations de fonctionnement: 30 % au-dessus de la limite "g" publiée,

   4) CEM (immunité): 50 % au-dessus de la limite publiée;

b) lors de l'utilisation d'essais supplémentaires au cours des essais de type: essais de la durée de vie hautement accélérés (HALT), etc.;

c) lors d'essais avec des unités supplémentaires au cours des essais de type;

d) lors de 100 % des essais de toutes les unités expédiées ou détermination par le biais d'une analyse des caractéristiques critiques du système et 100 % des essais de celles-ci;

e) lors de l'utilisation d'essais supplémentaires pendant la fabrication: essais de niveau accru hautement accélérés (HAST), etc.;

f) contrôles, évaluations, analyses, etc. d'assurance qualité supplémentaires;

g) interdiction de toute modification apportée à la conception, aux composants ou aux matériaux autres que ceux concernant le produit dont le type est à l'essai;

h) exécution d'une analyse formelle de l'impact des modifications.

14 Evaluation de la sécurité fonctionnelle

14.1 Objectif

L'objectif des exigences de 14.1 consiste à spécifier les activités nécessaires pour faire des recherches et porter un jugement sur l'adéquation de la sécurité fonctionnelle atteinte par le FS-PLC et la conformité aux paragraphes pertinents de la présente Norme atteinte par le FS-PLC. Cet objectif consiste également à déterminer si la conformité aux paragraphes pertinents de la présente partie a été atteinte.

Une évaluation de la sécurité fonctionnelle du FS-PLC doit être réalisée afin de garantir que le niveau nécessaire de sécurité a été atteint. Ses résultats doivent être présentés dans un rapport d'évaluation de la sécurité. Le rapport doit décrire les activités effectuées par le contrôleur de la sécurité pour déterminer comment le système/sous-système/équipement FS-PLC (matériel et logiciel) a été conçu pour satisfaire à ses exigences spécifiées, et qu'il spécifie éventuellement des conditions supplémentaires pour le fonctionnement du système/sous-système/équipement.

Le contrôleur/l'équipe d'évaluation doit au moins être indépendant(e) de l'équipe de développement du FS-PLC.

14.2 Exigences d’évaluation

14.2.1 Preuves et documentation concernant l’évaluation

L'évaluation doit fournir des éléments prouvant que toutes les étapes nécessaires de vérification et de validation sont effectuées pour prouver que:

a) les mesures permettant d'éviter les défaillances (activités de gestion de la sécurité fonctionnelle) sont appropriées pour le niveau d'intégrité de sécurité exigé,

b) les mesures permettant de contrôler les défaillances matérielles et logicielles sont appropriées pour le niveau d'intégrité de sécurité exigé.

L'évaluation de la sécurité fonctionnelle doit être basée sur l'évaluation de la documentation suivante:

- spécification des exigences du système (ou sous-système/équipement) FS-PLC;
- définition du système/sous-système/équipement;
- plan de vérification et de validation;
- plan de sécurité;
- rapport de gestion de la sécurité fonctionnelle conformément à la CEI 61508-1 et à la présente Norme (preuves de gestion de la sécurité);
- rapport de mesures techniques conformément à la CEI 61508-2 et à la CEI 61508-3 et à la présente norme; plan(s) d'essai et rapport(s);
- conformité aux exigences CEM et environnementales;
- conformité aux exigences de la CEI 61131-2.

14.2.2 Méthode d'évaluation

1) Une ou plusieurs personnes doivent être désignées pour effectuer une ou plusieurs évaluations de la sécurité fonctionnelle afin de porter un jugement sur l'adéquation des éléments suivants:
   a) la sécurité fonctionnelle atteinte par le FS-PLC, au sein de son environnement particulier, relativement aux paragraphes pertinents de la présente Norme;
   b) la conformité aux paragraphes pertinents de la présente Norme, atteinte en cas d'éléments/de sous-systèmes.
2) Les personnes effectuant une évaluation de la sécurité fonctionnelle doivent avoir accès à toutes les personnes impliquées dans toutes les activités de cycle de vie de sécurité du FS-PLC, ainsi que toutes les informations et équipements pertinents (matériel et logiciel).
3) Une évaluation de la sécurité fonctionnelle doit être appliquée à toutes les phases du cycle de vie général, y compris la documentation, la vérification et la gestion de la sécurité fonctionnelle.
4) Les personnes effectuant une évaluation de la sécurité fonctionnelle doivent tenir compte des activités réalisées et des résultats obtenus lors de chaque phase du cycle de vie de sécurité général et déterminer si la sécurité fonctionnelle adéquate a été atteinte en fonction des objectifs et des exigences de la présente Norme.
5) Les compétences du contrôleur/de l'équipe d'évaluation doivent être pertinentes pour le développement matériel et logiciel du FS-PLC; elles doivent également être documentées.
6) Toutes les déclarations pertinentes de conformité effectuées par des fournisseurs et d'autres parties responsables de la réalisation de la sécurité fonctionnelle doivent être incluses à l'évaluation de la sécurité fonctionnelle.
7) Une évaluation de la sécurité fonctionnelle peut être effectuée après chaque phase du cycle de vie de sécurité général du FS-PLC, ou après un certain nombre de phases du cycle de vie de sécurité.
8) Une évaluation de la sécurité fonctionnelle doit inclure une évaluation des éléments prouvant qu'un ou plusieurs audits de sécurité fonctionnelle ont été réalisés (intégralement ou partiellement) de manière pertinente par rapport à son domaine d'application.
9) Si elle est effectuée de manière incrémentale, chaque évaluation de la sécurité fonctionnelle doit au moins tenir compte des éléments suivants:
   a) le travail effectué depuis la précédente évaluation de la sécurité fonctionnelle;
   b) les plans ou stratégies permettant d'implémenter d'autres évaluations de la sécurité fonctionnelle;
   c) les recommandations des précédentes évaluations de la sécurité fonctionnelle et le degré des modifications effectuées afin de les satisfaire.
10) Chaque évaluation de la sécurité fonctionnelle doit être planifiée par le fabricant. Le plan doit spécifier toutes les informations nécessaires pour faciliter une évaluation efficace, y compris:
   a) le domaine d'application de l'évaluation de la sécurité fonctionnelle;
   b) les organisations impliquées;
   c) les ressources requises;
   d) les personnes chargées de procéder à l'évaluation de la sécurité fonctionnelle et leurs compétences;
   e) le niveau d'indépendance des personnes chargées de procéder à l'évaluation de la sécurité fonctionnelle;
   f) les résultats de l'évaluation de la sécurité fonctionnelle;
   g) la manière dont l'évaluation de la sécurité fonctionnelle fait référence, et doit être intégrée, aux autres évaluations de la sécurité fonctionnelle;
   h) à quel moment, au cours du cycle de vie de sécurité du FS-PLC, la ou les évaluations seront effectuées.

11) Avant qu'une évaluation de la sécurité fonctionnelle ne soit réalisée, son plan doit être approuvé par les personnes chargées de l'effectuer et par celles responsables de la gestion de la sécurité fonctionnelle.

12) A la fin d'une évaluation de la sécurité fonctionnelle, les personnes chargées de procéder à l'évaluation doivent documenter, conformément aux plans et termes de référence de l'évaluation:

    a) les activités réalisées;

    b) les résultats obtenus;

    c) les conclusions effectuées;

    d) un jugement concernant l'adéquation de la sécurité fonctionnelle, conformément aux exigences de la présente Norme;

    e) les recommandations provenant de l'évaluation, y compris celles concernant l'acceptation, l'acceptation qualifiée ou le refus.

13) Les résultats pertinents de l'évaluation de la sécurité fonctionnelle d'un élément conforme doivent être mis à la disposition des personnes ayant des responsabilités concernant les activités de cycle de vie général du FS-PLC, y compris les concepteurs et les contrôleurs du FS-PLC.

14) Le résultat de l'évaluation de la sécurité fonctionnelle d'un élément conforme doit inclure les informations suivantes pour faciliter la réutilisation des résultats de l'évaluation dans le cadre d'un système plus important:

    a) l'identification précise de l'élément conforme comprenant la version de ses matériels et logiciels;

    b) les conditions supposées au cours de l'évaluation;

    c) la référence aux preuves concernant la documentation sur lesquelles la conclusion de l'évaluation a été basée;

    d) les procédures, méthodes et outils utilisés pour évaluer la capacité systématique avec la justification de son efficacité;

    e) les procédures, méthodes et outils utilisés pour évaluer l'intégrité de sécurité matérielle avec la justification de l'approche adoptée et la qualité des données

    f) les résultats de l'évaluation obtenus relativement aux exigences de la présente Norme et à la spécification des caractéristiques de sécurité de l'élément conforme dans son manuel de sécurité;

15) Les personnes chargées de procéder à une évaluation de la sécurité fonctionnelle doivent être compétentes quant aux activités à réaliser, et ce conformément aux exigences données en 5.4.2.2.2 et en 5.4.2.2.3.

14.3 Informations de l'évaluation du FS-PLC

Les informations du Tableau 14 doivent être actualisées par le fabricant du FS-PLC.

Tableau 14 – Informations de l'évaluation de la sécurité fonctionnelle

Phase du cycle de vie de sécurité du FS-PLC	Informations
Concept	Description (concept du FS-PLC)
Définition du domaine d'application du FS-PLC	Description (définition du domaine d'application du FS-PLC)
Exigences de sécurité fonctionnelle du FS-PLC	Spécification (exigences de sécurité fonctionnelle du FS-PLC, comprenant les éléments suivants: fonctions de sécurité du FS-PLC et intégrité de sécurité du FS-PLC)
Allocation des exigences de sécurité fonctionnelle	Description (allocation des exigences de sécurité fonctionnelle)
Planification du fonctionnement et de la maintenance du FS-PLC	Plan (fonctionnement et maintenance du FS-PLC)
Planification de la vérification et de la validation de la sécurité du FS-PLC	Plan (vérification et validation de la sécurité du FS-PLC)
Réalisation	Documentation concernant la conception et le développement (voir la CEI 61508-2 et la CEI 61508-3)
Vérification et validation de la sécurité du FS-PLC	Rapport (vérification et validation de la sécurité du FS-PLC)
Fonctionnement et maintenance du FS-PLC	Procédures de fonctionnement et de maintenance du FS-PLC
Modification du FS-PLC	Demande (modification du FS-PLC); Rapport (modification du FS-PLC) et amélioration de l'analyse de l'impact (modification du FS-PLC);
Concerne l'ensemble des phases	Plan (sécurité); Plan (vérification); Rapport (vérification); Plan (évaluation de la sécurité fonctionnelle); Rapport (évaluation de la sécurité fonctionnelle)

14.4 Indépendance

Le niveau minimal d'indépendance des personnes chargées de procéder à une évaluation de la sécurité fonctionnelle doit être tel que spécifié dans le Tableau 15. Le Tableau 15 doit être interprété comme suit:

- X: le niveau d'indépendance spécifié correspond au niveau minimal pour le niveau d'intégrité de sécurité/la capacité systématique spécifié. Si un niveau d'indépendance inférieur est adopté, le motif de son utilisation doit alors être détaillé;
- X1 et X2;
- Y: le niveau d'indépendance spécifié est considéré comme insuffisant pour le niveau d'intégrité de sécurité/la capacité systématique spécifié.

Dans le cadre du Tableau 15, seules les cellules contenant X, X1, X2 ou encore Y doivent être utilisées comme base pour la détermination du niveau d'indépendance. Pour les cellules contenant X1 ou X2, X1 ou X2 est applicable (mais pas les deux), en fonction d'un nombre de facteurs spécifiques à la conception du FS-PLC. Il convient de détailler le motif de la sélection de X1 ou de X2. Les facteurs qui feront que X2 sera plus approprié que X1 sont les suivants:

– manque d'expérience préalable avec une conception similaire;
– degré de complexité plus important;
– degré d'innovation de la conception plus important;
– degré d'innovation de la technologie plus important.

NOTE 1 Selon l'organisation et l'expertise de l'entreprise, l'exigence concernant les personnes et les services indépendants est satisfaite, dans certains cas, par le biais d'une organisation externe. A l'inverse, les entreprises disposant d'organisations internes compétentes en évaluation des risques et en application des systèmes relatifs à la sécurité, indépendantes et distinctes (par l'intermédiaire des cadres et d'autres ressources) des personnes responsables du développement principal, utilisent, dans certains cas, leurs propres ressources pour satisfaire aux exigences pour une organisation indépendante.

NOTE 2 Voir 3.8.11, 3.8.12 et 3.8.13 de la CEI 61508-4:2010 pour obtenir respectivement des définitions de personnes indépendantes, de services indépendants et d'organisations indépendantes.

NOTE 3 Les personnes chargées de procéder à une évaluation de la sécurité fonctionnelle sont prudentes lorsqu'elles prodiguent des conseils sur des éléments du domaine d'application de l'évaluation, étant donné que cela pourrait compromettre leur indépendance. Il est souvent approprié de prodiguer des conseils sur les aspects qui pourraient faire l'objet d'un jugement de sécurité inadéquate, tel qu'un manque de preuves. Cependant, il est généralement inapproprié de prodiguer des conseils ou de faire des recommandations concernant des solutions spécifiques pour ces (ou d'autres) problèmes.

Dans le cadre du Tableau 15, les niveaux d'indépendance minimaux doivent être basés sur la capacité systématique la plus élevée déclarée pour le FS-PLC spécifiée dans les termes du niveau d'intégrité de sécurité.

Tableau 15 – Niveaux d'indépendance minimum des personnes chargées de procéder à l'évaluation de la sécurité fonctionnelle

Niveau d'indépendance minimal	Niveau d'intégrité de sécurité/capacité systématique			
	1	2	3	4
Personne indépendante	X	X1	Y	Y
Service indépendant		X2	X1	Y
Organisation indépendante			X2	X

15 Procédures de fonctionnement, de maintenance et de modification du FS-PLC

15.1 Objectif

L'objectif de 15.1 consiste à s'assurer que le fabricant du FS-PLC fournit des procédures de fonctionnement, de maintenance et de modification pour le système FS-PLC satisfaisant, en tous points, aux exigences de sécurité en termes d'intégrité de sécurité et de fonctions de sécurité exigées définies à l'Article 6.

Les informations concernant ces procédures de fonctionnement, de maintenance et de modification sont spécifiées à l'Article 16.

15.2 Modification du FS-PLC

Les fabricants qui déclarent être en conformité avec la présente Norme doivent disposer en permanence d'un système permettant de gérer les modifications (par exemple, consécutivement à la détection de défauts) afin d'améliorer le processus de conception ou de fabrication, ou encore d'améliorer des fonctionnalités. Ce système doit inclure la documentation des éléments suivants: détails de la modification, analyses de son impact (y compris la nécessité de nouvelle vérification et de revalidation), approbations pour la modification, résultats de revalidation/nouvelle vérification et les modifications associées au fonctionnement ou à la documentation d'un produit donné. Pour plus de détails, voir le 7.16 de la CEI 61508-1:2010 et le 7.8 de la CEI 61508-3:2010.

Toutes les modifications du FS-PLC doivent être analysées pour déterminer l'effet qu'une modification ou une amélioration apportée à un module du système FS-PLC aura sur les autres modules de ce système, de même que sur d'autres parties du système relatif à la sécurité.

Cette analyse doit être exécutée avant une modification ou une amélioration.

Une fois l'analyse effectuée, une décision doit être prise concernant la nécessité d'une nouvelle vérification du système FS-PLC. Cela dépend du nombre de modules affectés, de la

criticité des modules affectés et de la nature de la modification. Les décisions possibles sont les suivantes:

- seul le module modifié doit être revérifié;
- tous les modules affectés doivent être revérifiés; ou
- l'ensemble du système FS-PLC doit être revérifié.

Le fabricant du FS-PLC doit conserver un historique de cette analyse et la décision prise pour toutes les modifications qui affectent des parties pertinentes de la sécurité du FS-PLC.

16 Informations destinées à l'utilisateur devant être fournies par le fabricant du FS-PLC

16.1 Généralités

Le fabricant doit fournir aux utilisateurs les informations requises pour l'application, l'installation, la mise en service, le fonctionnement et la maintenance du FS-PLC. De plus, le fabricant peut dispenser une formation aux utilisateurs. Les informations à diffuser peuvent être disponibles sous une forme autre qu'un support imprimé.

16.2 Informations sur la conformité à la présente Norme

Le fabricant doit mettre à disposition, à la demande, des informations pour la vérification de la conformité.

16.3 Informations sur le type et le contenu de la documentation

Quatre types de documentation sont définis:

- catalogues et fiches techniques,
- manuels d'utilisation,
- manuels de sécurité et
- documentation technique.

NOTE Pour la préparation des instructions, voir la CEI 62079 et la CEI 61506.

16.4 Informations sur les catalogues et/ou fiches techniques

Ces documents doivent contenir la description et les spécifications du FS-PLC, de même que ses périphériques associés. En outre, ils doivent contenir toute autre information pertinente permettant de faciliter la compréhension de l'application et l'utilisation de ses produits, notamment caractéristiques fonctionnelles, règles de configuration d'équipement et conditions de service normales, en plus de dresser la liste des normes et certifications auxquelles ils sont conformes.

16.5 Manuel de sécurité

16.5.1 Généralités

L'objectif du manuel de sécurité consiste à documenter toutes les informations relatives à un FS-PLC donné requises pour permettre l'intégration du FS-PLC dans un système relatif à la sécurité, ce dernier étant conforme aux exigences de la série CEI 61508.

NOTE Ce texte est adapté du D.2.2 de la CEI 61508-2:2010 et du D.2.2 de la CEI 61508-3:2010.

16.5.2 Contenu du manuel de sécurité

16.5.2.1 Généralités

Chaque FS-PLC doit avoir un manuel de sécurité. En général, le manuel de sécurité doit contenir:

a) une spécification fonctionnelle des fonctions capables d'être exécutées;

b) une identification de la configuration matérielle et/ou logicielle du FS-PLC pour permettre la gestion de la configuration du système électrique/électronique/électronique programmable relatif à la sécurité, conformément à 6.2.1 de la CEI 61508-1:2010;

c) les contraintes concernant l'utilisation du FS-PLC et/ou hypothèses sur lesquelles les analyses du comportement ou des taux de défaillance du FS-PLC sont basées.

16.5.2.2 Contenu du manuel de sécurité

Le manuel de sécurité doit spécifier les fonctions de l'élément conforme. Celles-ci peuvent être utilisées pour prendre en charge la fonction de sécurité d'un système relatif à la sécurité ou les fonctions d'un sous-système ou d'un élément. Il est recommandé que la spécification décrive clairement les fonctions et les interfaces d'entrée et de sortie.

Pour chaque fonction, le manuel de sécurité doit contenir:

a) les modes de défaillance de l'élément conforme (en termes de comportement de ses sorties), du fait de défaillances aléatoires du matériel, donnant lieu à une défaillance de la fonction et n'étant pas détectés par les diagnostics internes au FS-PLC;

b) pour chaque mode de défaillance dans a), un taux de défaillance estimé;

c) les modes de défaillance de l'élément conforme (en termes de comportement de ses sorties), du fait de défaillances aléatoires du matériel, donnant lieu à une défaillance de la fonction et étant détectés par les diagnostics internes au FS-PLC;

d) les modes de défaillance des diagnostics internes au FS-PLC (en termes de comportement de leurs sorties), du fait de défaillances aléatoires du matériel, donnant lieu à une défaillance des diagnostics pour détecter des défaillances de la fonction;

e) pour chaque mode de défaillance dans c) et d), le taux de défaillance estimé;

f) pour chaque mode de défaillance dans c) détecté par les diagnostics internes au FS-PLC, l'intervalle d'essai de diagnostic;

g) pour chaque mode de défaillance dans c), les sorties de l'élément conforme initiées par les diagnostics internes;

NOTE 1 Les sorties des diagnostics internes comprennent le lancement de mesures supplémentaires (techniques/procédurales) sur le système, sous-système ou élément électrique/électronique/électronique programmable relatif à la sécurité afin d'atteindre ou de conserver un état de sécurité de l'équipement commandé.

h) exigences d'essai de sûreté et/ou de maintenance périodique;

i) pour ces modes de défaillance, par rapport à une fonction spécifiée, qui peuvent être détectés par des diagnostics externes, des informations suffisantes doivent être fournies pour faciliter le développement d'une capacité de diagnostics externes. Les informations doivent inclure des détails de modes de défaillance et, pour ces modes de défaillance, les taux de défaillance;

j) la tolérance aux pannes matérielles;

k) la classification en tant que type A ou type B de cette partie du FS-PLC fournissant la fonction;

NOTE 2 Les modes de défaillance sont classés comme étant sécurisés ou dangereux lorsque l'application du FS-PLC est connue relativement aux dangers de l'équipement commandé. Par exemple, si un capteur est appliqué de telle sorte qu'une sortie élevée soit utilisée pour signaler un danger de l'équipement commandé (par exemple, haute pression), un mode de défaillance empêchant le signalement correct du danger (par exemple, blocage de la sortie au niveau faible) est classé comme étant dangereux, alors qu'un mode de défaillance à l'origine du caractère élevé de la sortie du capteur est classé comme étant sécurisé. Cela

dépend de l'interprétation du signal du capteur par le FS-PLC et ne peut donc pas être spécifié sans appliquer de contraintes à l'application du capteur.

De plus, le niveau de couverture de diagnostic déclarée pour un FS-PLC varie généralement d'une application à une autre, en fonction du degré des diagnostics du FS-PLC ou du traitement des signaux externes qui s'ajoutent éventuellement à des diagnostics internes du FS-PLC.

Il s'ensuit que les estimations de la tolérance aux pannes matérielles ou du taux de défaillances non dangereuses ne sont effectuées que si des contraintes pèsent sur l'application du FS-PLC. Ces contraintes se trouvent hors du contrôle du fournisseur du FS-PLC. Par conséquent, aucune déclaration ne doit être effectuée dans le manuel de sécurité, pour ce qui concerne la tolérance aux pannes matérielles ou au taux de pannes non dangereuses, ou encore à toute autre caractéristique de la sécurité fonctionnelle dépendant de la connaissance des modes de défaillance non dangereux et dangereux, à moins que les hypothèses sous-jacentes, quant à ce qui constitue les modes de défaillance non dangereux et dangereux, ne soient clairement spécifiées.

l) des indications concernant la façon d'intégrer la contribution du FS-PLC au temps de réponse de la fonction de sécurité ou au temps de sécurité du processus.

Pour chaque fonction du FS-PLC associée à la défaillance systématique, le manuel doit contenir:

1) la capacité systématique du FS-PLC ou la partie de l'élément qui fournit la fonction;
2) des instructions ou contraintes associées à l'application du FS-PLC, pertinentes pour la fonction, qu'il convient d'observer pour empêcher les défaillances systématiques du FS-PLC.

NOTE 3 L'intégrité de sécurité systématique indiquée par la capacité systématique ne peut être atteinte que lorsque les instructions et contraintes sont observées. En cas de violations, la déclaration de capacité systématique est partiellement ou intégralement non valide.

16.5.2.3 Contenu du manuel de sécurité des outils d'ingénierie

Les outils d'ingénierie doivent être identifiés et toutes les instructions nécessaires à leur utilisation doivent être mises à la disposition de l'intégrateur et de l'utilisateur.

NOTE Pour les outils d'ingénierie, cela est effectué en identifiant clairement l'élément et en démontrant que son contenu n'a pas été modifié.

Annexe A
(informative)

Calculs de fiabilité

A.1 Généralités

L'Annexe A fait référence à un certain nombre d'exemples de techniques de calcul des probabilités de défaillance pour un système instrumenté de sécurité conçu et installé conformément à la CEI 61511-1. Cette partie est de nature informative et il convient de l'interpréter comme les seules techniques d'évaluation à utiliser.

Les méthodologies référencées proviennent de l'Annexe B de la CEI 61508-6:2010, de la CEI 61078, de la CEI 61025, de la CEI 61165 et de la série ISA TR 84.00.02.

A.2 Technique de bloc-diagramme de fiabilité

La CEI 61078 et l'Annexe B de la CEI 61508-6:2010 illustrent la technique du bloc-diagramme de fiabilité, qui permet de calculer les probabilités de défaillance pour les fonctions instrumentées de sécurité conçues conformément à la présente norme.

A.3 Technique d'analyse par arbre de panne

La CEI 61025 et l'ISA TR 84.00.02-3 illustrent la technique d'analyse par arbre de panne, qui permet de calculer les probabilités de défaillance pour les fonctions instrumentées de sécurité conçues conformément à la présente norme.

A.4 Technique de modélisation de Markov

La CEI 61165 et l'ISA TR 84.00.02-4 illustrent la technique de modélisation de Markov, qui permet de calculer les probabilités de défaillance pour les fonctions instrumentées de sécurité conçues conformément à la présente norme.

Annexe B
(informative)

Architectures FS-PLC typiques

B.1 Exemples d'architectures de sous-systèmes FS-PLC

Les sous-systèmes du FS-PLC peuvent comprendre plusieurs architectures. Davantage d'informations sur les exemples d'architectures sont fournies dans le B.3.2.2 et le B.3.3.2 de la CEI 61508-6:2010.

Une architecture M pour N (MooN) est composée de N canaux, pouvant tous contribuer au traitement de la fonction de sécurité du FS-PLC. Au moins M canaux sont requis pour accomplir la fonction de sécurité du FS-PLC. Le système exécute la fonction de sécurité du FS-PLC si M canaux fonctionnent correctement. (N-M) définit la tolérance aux pannes du système, où les pannes du canal (N-M+1) entraînent la défaillance de la fonction de sécurité du FS-PLC.

Exemples:

1oo1: La tolérance aux pannes est de 0 et le nombre de canaux est de 1. Cette architecture comprend un canal unique, dans lequel toute défaillance dangereuse provoque une défaillance de la fonction de sécurité lorsqu'une sollicitation survient.

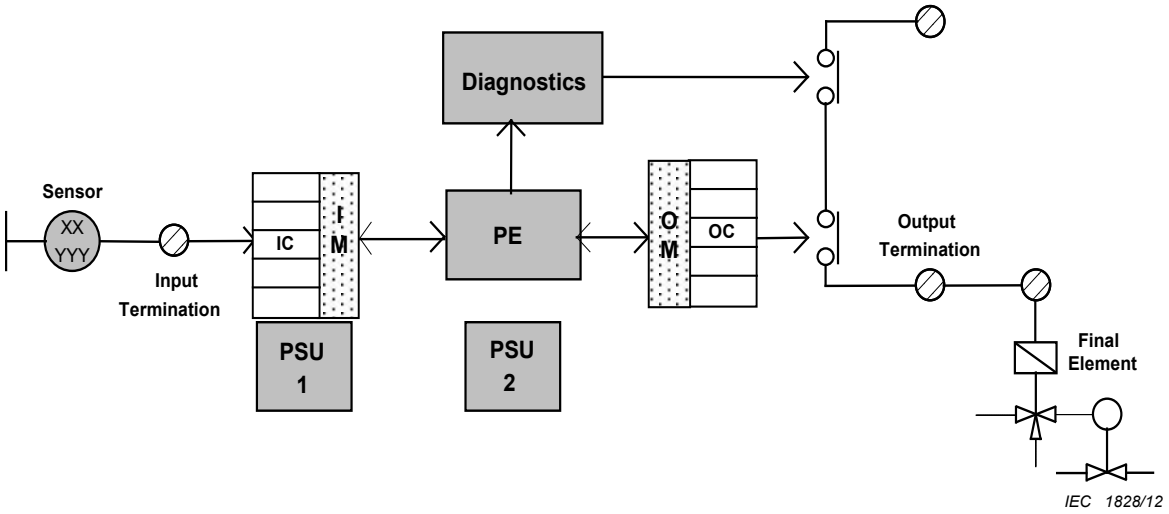
1oo2: La tolérance aux pannes est de 1 et le nombre de canaux est de 2. Cette architecture comprend deux canaux connectés en parallèle, de façon que chaque canal puisse traiter la fonction de sécurité. Il faudrait ainsi qu'une défaillance dangereuse survienne dans les deux canaux avant qu'une fonction de sécurité ne tombe en panne sur sollicitation. On suppose que tout essai de diagnostic signalerait seulement les pannes détectées, mais ne modifierait pas les états de sortie ni le vote des sorties.

2oo2: La tolérance aux pannes est de 0 et le nombre de canaux est de 2. Cette architecture comprend deux canaux connectés en parallèle, de façon que l'exécution de la fonction de sécurité nécessite une sollicitation des deux canaux à la fois. On suppose que tout essai de diagnostic signalerait seulement les pannes détectées, mais ne modifierait pas les états de sortie ni le vote des sorties.

2oo3: La tolérance aux pannes est de 1 et le nombre de canaux est de 3. Cette architecture comprend trois canaux connectés en parallèle présentant une disposition de vote majoritaire pour les signaux de sortie; de cette manière, l'état de sortie n'est pas modifié si un seul canal donne un résultat différent, en désaccord avec les deux autres canaux. On suppose que tout essai de diagnostic signalerait seulement les pannes détectées, mais ne modifierait pas les états de sortie ni le vote des sorties.

Les implémentations d'architectures suivantes sont typiques de ce qui peut être trouvé dans les FS-PLC.

B.2 FS-PLC unique avec E/S unique et horloge de surveillance externe (1oo1D)



Légende

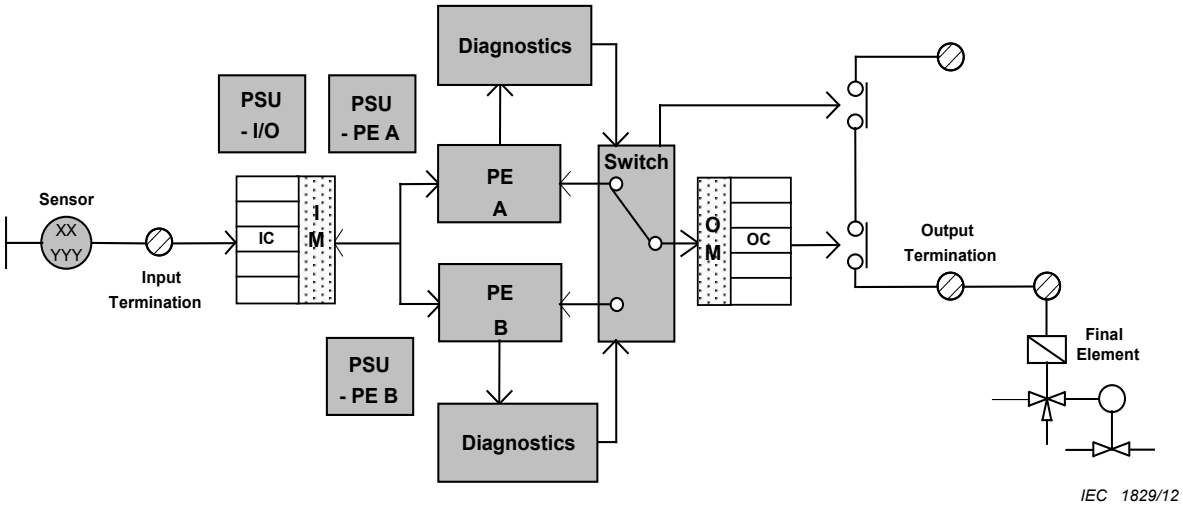
Anglais	Français
Diagnostics	Diagnostics
Sensor	Capteur
Input Termination	Terminal d'entrée
PE	PE
PSU 1	BA 1
PSU 2	BA 2
OM	MS
IC	CE
IM	ME
Output Termination	Terminal de sortie
Final Element	Elément final
OC	CS

Figure B.1 – FS-PLC unique avec E/S unique et horloge de surveillance externe (1oo1D)

Cette configuration n'a pas de redondance. Elle est constituée d'un canal unique: processeur élémentaire unique (PE), canal d'entrée (CE) sur un module d'entrée (ME), canal de sortie (CS) sur un module de sortie (MS). Cette configuration peut inclure des blocs d'alimentation (BA) redondants. La fonction d'horloge de surveillance (diagnostic) externe offre un deuxième moyen de désactiver les sorties et de mettre le processus commandé en état de sécurité. Cette fonction d'horloge de surveillance externe désactive la deuxième sortie de contact si une panne dangereuse est détectée dans le résolveur logique ou le module de sortie associé. Les sorties sont présentées comme des contacts mais elles peuvent être réalisées par des interrupteurs à semi-conducteurs ou autres.

Toutes les pannes sécurisées entraînent un mauvais déclenchement du processus commandé. Toutes les pannes dangereuses détectées entraînent également un mauvais déclenchement du processus commandé car le système doit être arrêté pour remplacer les modules.

B.3 Processeur élémentaire double avec E/S unique et horloges de surveillance externes (1oo1D)



Légende

Anglais	Français
Diagnostics	Diagnostics
Sensor	Capteur
Input Termination	Terminal d'entrée
PE A	PE A
PE B	PE B
PSU – PE B	BA – PE B
PSU – PE A	BA – PE A
PSU – I/O	BA – E/S
OM	MS
IC	CE
IM	ME
Switch	Interrupteur
Output Termination	Terminal de sortie
Final Element	Elément final
OC	CS

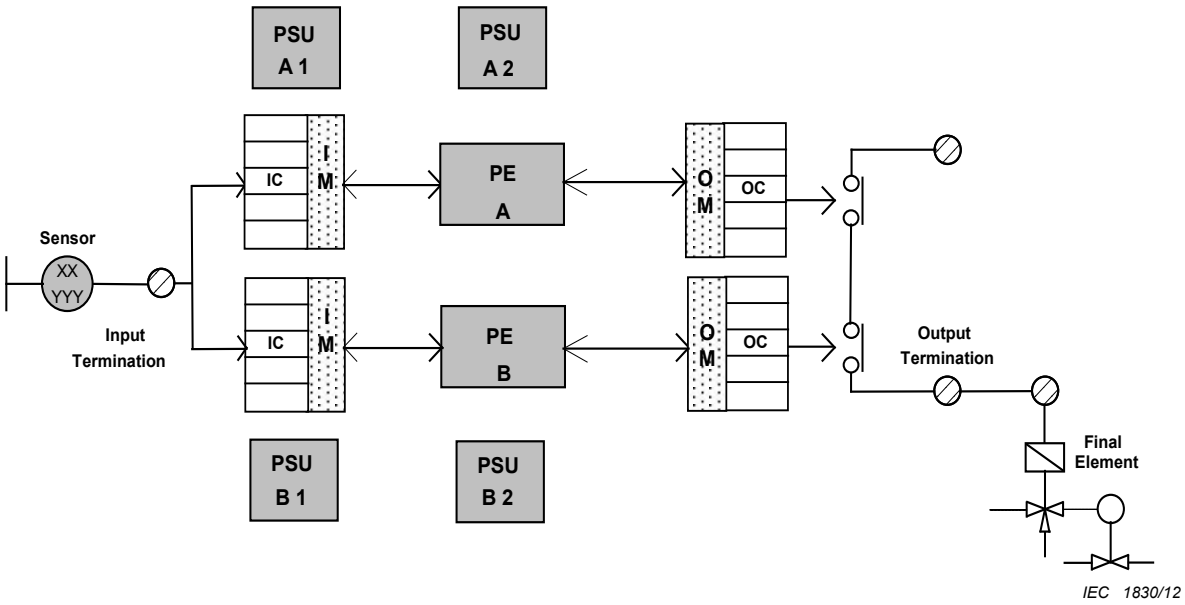
Figure B.2 – Processeur élémentaire double avec E/S unique et horloges de surveillance externes (1oo1D)

Cette configuration double est constituée de processeurs élémentaires redondants et d'horloges de surveillance externes. L'interrupteur est contrôlé par les fonctions d'horloge de surveillance, qui surveillent les résultats de diagnostics des processeurs élémentaires. La deuxième méthode pour désactiver les sorties sera utilisée si les deux entrées de diagnostic vers l'interrupteur sont désactivées. L'interrupteur passe régulièrement d'une position à l'autre afin que sa fonctionnalité, et la fonctionnalité et les diagnostics de chaque partie traitée puissent être vérifiés dans les deux états. Les deux processeurs élémentaires comparent les résultats et si une différence est détectée, les deux horloges de surveillance sont réglées de manière à désactiver les sorties. Toute différence entre les parties traitées entraîne la désactivation des sorties afin de mettre le processus commandé en état de sécurité. Les pannes détectées dans l'un des modules E/S uniques entraînent également la désactivation des sorties. Les pannes sécurisées non détectées par le résolveur logique, ainsi que les erreurs de comparaison mentionnées ci-dessus, entraînent un mauvais déclenchement du

processus commandé. Les autres pannes non dangereuses et dangereuses détectées d'un processeur élémentaire peuvent être réparées en ligne.

Si une panne dangereuse du processeur entraînant les sorties n'est pas détectée, le système de sécurité sera en incapacité de fonctionner.

B.4 Processeur élémentaire double avec E/S double, aucune communication inter-processeurs et logique de fermeture 1oo2



Légende

Anglais	Français
Sensor	Capteur
Input Termination	Terminal d'entrée
PE A	PE A
PE B	PE B
PSU A 1	BA A 1
PSU A 2	BA A 2
OM	MS
IC	CE
IM	ME
Output Termination	Terminal de sortie
Final Element	Elément final
PSU B 1	BA B 1
PSU B 2	BA B 2
OC	CS

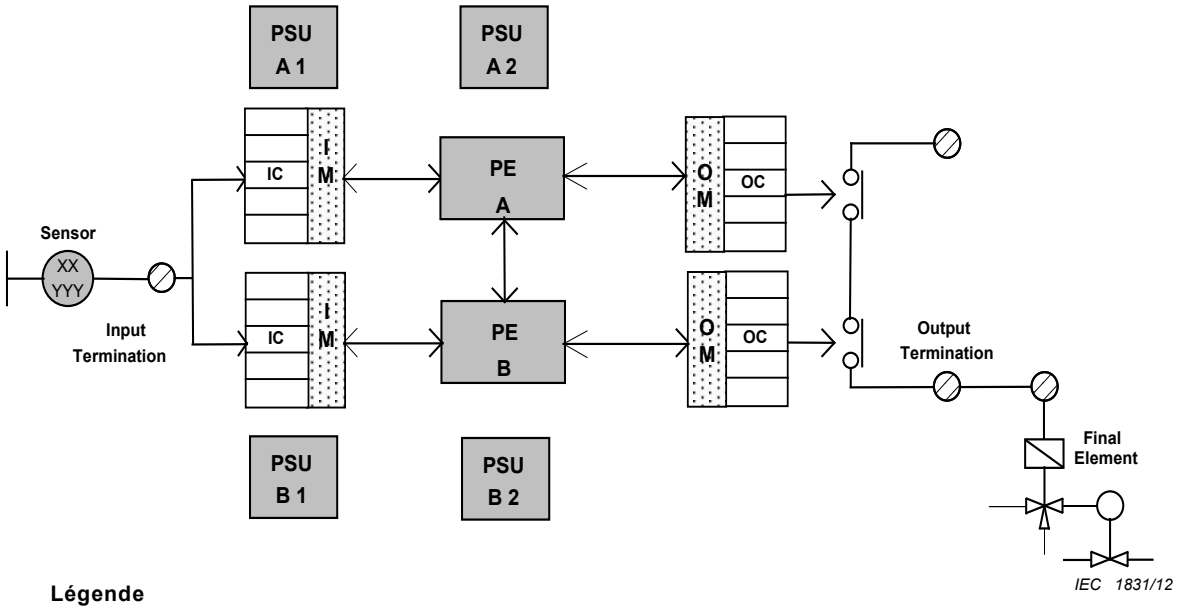
Figure B.3 – Processeur élémentaire double avec E/S double, aucune communication inter-processeurs et logique de fermeture 1oo2

Cette configuration double se présente comme deux canaux indépendants. Il n'existe aucune communication entre les processeurs élémentaires. La couverture de diagnostic est déterminée par la couverture de diagnostic réalisable dans un système à canal unique. Les sorties d'un canal vers chaque élément final sont câblées en série avec les sorties de l'autre canal, chaque canal peut donc ouvrir le circuit de sortie et mettre le processus commandé en état de sécurité. Chaque processeur élémentaire commande l'état de sécurité des sorties si

les entrées font une transition correspondant à un événement dangereux ou si une panne dangereuse est détectée dans l'un des modules du canal. Cette configuration ne possède pas d'horloge de surveillance externe, car les sorties de chaque canal sont câblées en série.

Toutes les pannes non dangereuses et dangereuses détectées dans le système entraînent un mauvais déclenchement du processus commandé.

B.5 Processeur élémentaire double avec E/S double, communication inter-processeurs et logique de fermeture 1oo2D



Légende

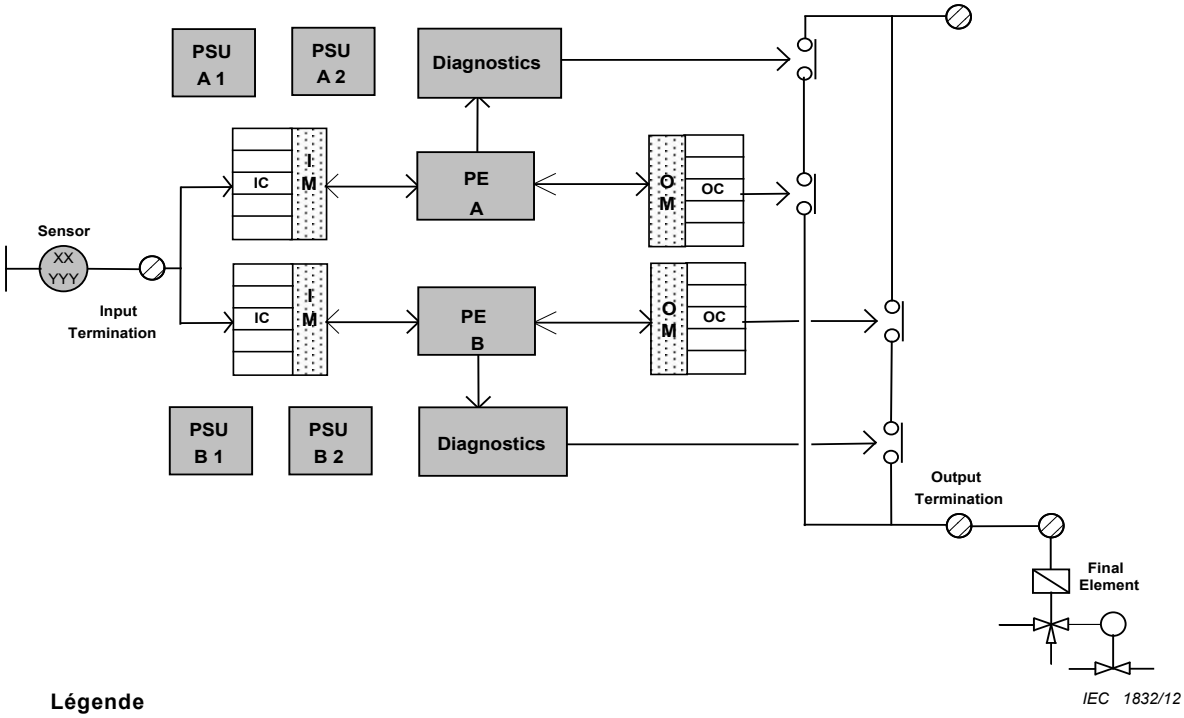
Anglais	Français
PSU A 1	BA A 1
PSU A 2	BA A 2
Sensor	Capteur
Input Termination	Terminal d'entrée
IC	CE
IM	ME
PE A	PE A
PE B	PE B
OM	MS
OC	CS
Output Termination	Terminal de sortie
Final Element	Elément final
PSU B 1	BA B 1
PSU B 2	BA B 2
OC	CS

Figure B.4 – Processeur élémentaire double avec E/S double, communication inter-processeurs et logique de fermeture 1oo2D

Cette configuration double se présente également comme deux canaux indépendants. Ce système intègre une communication entre les processeurs élémentaires. Cette communication augmente la couverture générale du diagnostic des processeurs élémentaires car des essais de comparaison peuvent être réalisés. La communication permet également aux processeurs de comparer les valeurs d'entrée et de continuer à fonctionner avec une entrée saine en cas

de détection d'une panne sur l'autre entrée. Toutes les autres pannes non dangereuses et dangereuses détectées dans le système entraînent un mauvais déclenchement du processus commandé.

B.6 Processeur élémentaire double avec E/S double, aucune communication inter-processeurs, horloges de surveillance externes et logique de fermeture 2oo2



Légende

Anglais	Français
PSU A 1	BA A 1
PSU A 2	BA A 2
Diagnostics	Diagnostics
Sensor	Capteur
Input Termination	Terminal d'entrée
IC	CE
IM	ME
PE A	PE A
PE B	PE B
OM	MS
OC	CS
Output Termination	Terminal de sortie
Final Element	Elément final
PSU B 1	BA B 1
PSU B 2	BA B 2

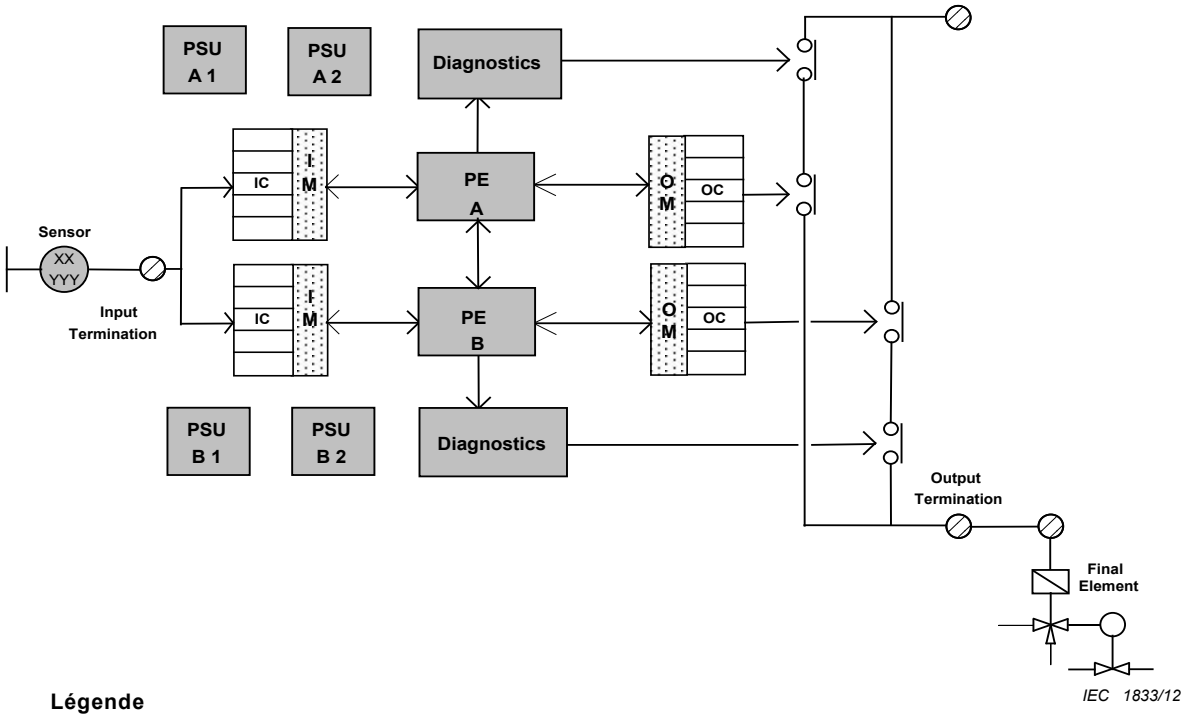
Figure B.5 – Processeur élémentaire double avec E/S double, aucune communication inter-processeurs, horloges de surveillance externes et logique de fermeture 2oo2

Cette configuration possède deux canaux indépendants 1oo1D. Il n'existe aucune communication entre les processeurs élémentaires dans ce système. Les sorties vers les éléments finaux de chaque canal sont câblées en parallèle afin de réduire le nombre de

mauvais déclenchements ou de déclenchements parasites. Les deux canaux doivent donc demander aux sorties de s'ouvrir avant l'ouverture d'une sortie. Ce câblage crée un vote 2oo2 des sorties de chaque canal. Le système possède des horloges de surveillance externes dans chaque canal pour améliorer la sécurité. Ces horloges de surveillance offrent une deuxième méthode pour désactiver la sortie d'un canal en cas de panne dangereuse d'un résolveur logique ou de détection d'un module de sortie.

Si toutes les pannes dangereuses ne sont pas détectées dans les modules d'un canal du système, le système sera en incapacité de fonctionner.

B.7 Processeur élémentaire double avec E/S double, communication inter-processeurs, horloges de surveillance externes et logique de fermeture 2oo2D



Légende

Anglais	Français
PSU A 1	BA A 1
PSU A 2	BA A 2
Diagnostics	Diagnostics
Sensor	Capteur
Input Termination	Terminal d'entrée
IC	CE
IM	ME
PE A	PE A
PE B	PE B
OM	MS
OC	CS
Output Termination	Terminal de sortie
Final Element	Elément final
PSU B 1	BA B 1
PSU B 2	BA B 2

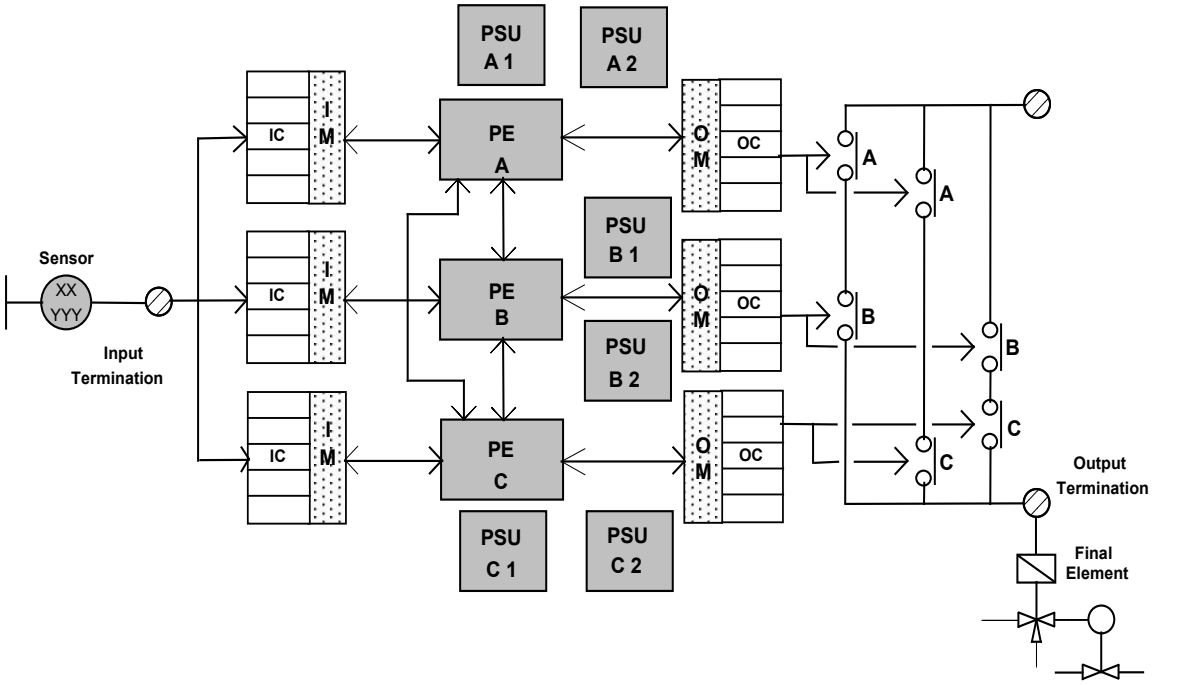
Figure B.6 – Processeur élémentaire double avec E/S double, communication inter-processeurs, horloges de surveillance externes et logique de fermeture 2oo2D

Cette configuration redondante se présente comme deux canaux indépendants. Ce système intègre une communication entre les processeurs élémentaires. Les sorties vers les éléments finaux de chaque canal sont câblées en parallèle afin de réduire le nombre de mauvais

déclenchements ou de déclenchements parasites. Les deux canaux doivent donc demander aux sorties de s'ouvrir avant l'ouverture d'une sortie. Le système possède des horloges de surveillance externes dans chaque canal ou branche pour améliorer la sécurité. Ces horloges de surveillance offrent une deuxième méthode pour désactiver la sortie d'une branche en cas de détection d'une panne dangereuse sur un processeur. La communication inter-processeurs améliore la capacité de diagnostic car des comparaisons peuvent être effectuées entre les états de sortie des deux canaux.

Toutes les pannes détectées dans le système pouvant être localisées dans un canal peuvent être réparées en ligne.

B.8 Processeur élémentaire triple avec E/S triple, communication inter-processeurs et logique de fermeture 2oo3D



Légende

Anglais	Français
PSU A 1	BA A 1
PSU A 2	BA A 2
Sensor	Capteur
Input Termination	Terminal d'entrée
IC	CE
IM	ME
OM	MS
OC	CS
Output Termination	Terminal de sortie
Final Element	Elément final
PSU B 1	BA B 1
PSU B 2	BA B 2
PE C	PE C
PE A	PE A
PE B	PE B
A	A
B	B
C	C
PSU C 1	BA C 1
PSU C 2	BA C 2

Figure B.7 – Processeur élémentaire triple avec E/S triple, communication inter-processeurs et logique de fermeture 2oo3D

Cette configuration redondante contient trois canaux avec une communication inter-processeurs. Chaque sortie vers l'élément final utilise un dispositif de décision de sorties

hexadécimales tolérant aux pannes qui effectue un vote 2oo3 sur les trois entrées dans le dispositif de décision. A l'aide de la communication inter-processeurs, les processeurs peuvent effectuer un vote 2oo3 sur la valeur du capteur lue par le système. Le vote 2oo3 permet également à une panne survenant dans l'une des trois branches d'être surpassée. Les pannes non dangereuses ou dangereuses détectées dans le système triple peuvent être réparées en ligne sans arrêter le processus commandé.

Annexe C
(informative)

Applications d'alimentation au déclenchement du FS-PLC

C.1 Généralités

La majorité des fonctions de sécurité lors d'une sollicitation se désactivent au déclenchement. En d'autres termes, les sorties sont désactivées lorsque la fonction de sécurité est sollicitée.

Au contraire, certaines fonctions de sécurité sont alimentées au déclenchement. En d'autres termes, les sorties sont activées lorsque la fonction de sécurité est sollicitée.

Les applications d'alimentation au déclenchement concernent plus souvent la diminution des conséquences d'un événement dangereux, plutôt que la prévention. Les applications typiques sont la protection contre l'incendie et la sécurité en matière de gaz, par exemple, la sonnerie d'une alarme d'évacuation ou le fonctionnement d'une soupape de décharge de produit extincteur.

Les demandes de FS-PLC utilisées dans les applications d'alimentation au déclenchement sont un peu différentes, et plus exigentes. Si un FS-PLC peut éventuellement être utilisé pour alimenter le déclenchement d'applications, il est recommandé au fabricant de prendre cela en considération et de fournir des données de défaillance spécifiques et des instructions d'utilisation pour de telles applications.

C.2 Etat sécurisé et état de sollicitation

Pour supprimer l'alimentation afin de lancer les applications, l'état de sollicitation de la fonction de sécurité est généralement le même que l'état de sécurité défini, c'est-à-dire que les sorties sont hors tension. Pour fournir l'énergie pour le déclenchement d'applications, l'état de sollicitation correspond à des sorties alimentées, mais l'état de sécurité défini correspond généralement toujours à des sorties hors tension. L'action entreprise en cas de détection d'une panne est donc différente de celle entreprise lorsque la fonction de sécurité est sollicitée.

Dans certaines applications, cela est nécessaire. Par exemple, la décharge non commandée de produit extincteur due à une panne interne pourrait constituer un grave danger.

C.3 Informations supplémentaires exigées lors d'une utilisation dans des applications d'alimentation au déclenchement

Il convient de fournir les informations supplémentaires suivantes à l'utilisateur:

- taux de défaillance aléatoire du matériel pour l'alimentation de l'opération de déclenchement. Le modèle de fiabilité du FS-PLC (voir 9.4.3) peut être différent pour l'alimentation au déclenchement et il peut s'avérer nécessaire d'effectuer une analyse distincte des effets et des modes de défaillance pour déterminer les taux de défaillance. Notez que les taux de défaillance de déclenchement peuvent être beaucoup plus élevés pour produire l'énergie pour le déclenchement;
- différences avec l'intégrité de sécurité systématique du FS-PLC lors du fonctionnement en mode de production d'énergie pour le déclenchement;
- conditions de fonctionnement spéciales ou mesures de diminution des pannes recommandées qu'il convient d'observer lors de la production d'énergie pour le déclenchement;

- il convient de mettre en évidence la distinction entre l'action sur sollicitation du FS-PLC et l'action en cas de détection d'une panne.

C.4 Considérations spécifiques

Il convient que le fabricant et l'utilisateur du FS-PLC prêtent une attention toute particulière aux éléments suivants:

- le FS-PLC est particulièrement dépendant de l'intégrité de la source d'alimentation dans les applications de production d'énergie pour le déclenchement. La défaillance de la source d'alimentation entraîne une incapacité du FS-PLC à répondre à une sollicitation. De plus, le FS-PLC peut être incapable d'indiquer qu'il est en état de panne;
- l'utilisation de sources d'alimentation indépendantes et redondantes est recommandée. Il convient d'être très attentif aux défaillances de cause commune dans les sources d'alimentation ou le système d'alimentation;
- il convient de prendre en compte la conformité avec les autres codes et normes spécifiques à un secteur, par exemple EN54 et NFPA72 pour la protection contre l'incendie et la sécurité en matière de gaz;
- les pannes survenant dans les lignes de champ et les dispositifs de champ du circuit de sortie peuvent empêcher une sortie alimentée au déclenchement de fonctionner sur sollicitation. Une surveillance du circuit de champ des sorties alimentées au déclenchement est recommandée pour détecter ce type de défaillances.

Annexe D
(informative)

Bases de données des taux de défaillance disponibles

D.1 Bases de données

La bibliographie suivante est une liste non exhaustive, sans ordre spécifique déterminé, de sources de données de taux de défaillance pour les composants électroniques et non électroniques. Il convient de noter que ces sources ne concordent pas toujours entre elles, et par conséquent, il convient d'être très vigilant quant à l'application des données.

- CEI/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment* (disponible en anglais seulement), Union Technique de l'Electricité et de la Communication (www.ute-fr.com). identique au RDF 2000/Reliability Data Handbook, UTE C 80-810
- Norme Siemens SN 29500, *Failure rates of components, (parts 1 to 14)*; Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.
- Telcordia SR-332, Issue 01: May 2001, *Reliability Prediction Procedure for Electronic Equipment*, (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06).
- EPRD (RAC-STD-6100) – *Electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.
- NNPRD-95 (RAC-STD-6200) – *Non-electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).
- HRD5, *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom
- Norme commerciale/militaire chinoise GJB/z 299B, *Electronic Reliability Prediction*, (http://www.itemuk.com/china299b.html)
- ISBN:0442318480, *AT&T reliability manual – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors*, AT&T Reliability Manual, Van Nostrand Reinhold, 1990,.
- FIDES:janvier 2004, *Manuel de données de fiabilité développé par un consortium d'entreprises françaises, sous la supervision du Ministère français de la Défense*. FIDES est disponible sur demande à l'adresse suivante: fides@innovation.net.
- Livre d'or de l'IEEE – *Les pratiques recommandées du livre d'or de l'IEEE sur la conception de réseaux électriques industriels et commerciaux fiables fournissent des données sur la fiabilité de l'équipement utilisé dans les réseaux de distribution électrique industriels et commerciaux*. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Téléphone: +1 800 678 IEEE (aux Etats-Unis et au Canada) +1 732 981 0060 (hors des Etats-Unis et du Canada), Fax: +1 732 981 9667 e-mail: customer.service@ieee.org.
- IRPH ITALTEL, *Reliability Prediction Handbook* – Le manuel Italtel IRPH est disponible sur demande auprès de: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy. Il s'agit de la version italienne du CNET RDF des entreprises de télécommunication. Les normes sont basées sur les mêmes ensembles de données, seuls quelques procédures et facteurs ont été modifiés.
- PRISM (RAC / EPRD) – Le logiciel PRISM est disponible sur demande à l'adresse ci-dessous, ou est intégré dans plusieurs packages logiciels relatifs à la fiabilité disponibles dans le commerce: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

D.2 Normes utiles relatives aux défaillances de composants

Les normes suivantes incluent des informations relatives à la défaillance de composants.

- CEI 60300-3-2, *Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*
- CEI 60300-3-5, *Gestion de la sûreté de fonctionnement – Partie 3-5: Guide d'application – Conditions des essais de fiabilité et principes des essais statistiques*
- CEI 60319, *Présentation et spécification des données de fiabilité pour les composants électroniques*
- CEI 60706-3, *Maintenabilité de matériel – Partie 3: Vérification et recueil, analyse et présentation de données*
- CEI 60721-1, *Classification des conditions d'environnement – Partie 1: Agents d'environnement et leurs sévérités*
- CEI 61709, *Composants électriques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*
- CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

NOTE Voir l'Annexe D de cette norme pour plus d'informations sur les modes de défaillance des composants électriques/électroniques.

Annexe E
(informative)

Méthodologie pour l'estimation des taux de défaillance de cause commune dans un FS-PLC à canaux multiples

E.1 Généralités

Cette Annexe informative fournit une approche qualitative simple pour l'estimation des taux de défaillance de cause commune pouvant s'appliquer à la conception du FS-PLC.

Voir également l'estimation des défaillances de cause commune dans l'Annexe D de la CEI 61508-6:2010.

E.2 Méthodologie

Il convient d'évaluer la conception de la ou des parties à canaux multiples du FS-PLC pour établir l'efficacité des mesures utilisées pour lutter contre les défaillances de cause commune. Il convient d'identifier les éléments applicables du Tableau E.1 et d'établir un score global, utilisé pour déterminer le facteur de défaillance de cause commune, en pourcentage, dans le Tableau E.2.

Tableau E.1 – Critères d'estimation de la défaillance de cause commune

Elément	Score
Séparation/répartition	
Tous les éléments du canal sont-ils séparés physiquement, par exemple sur des cartes de circuits imprimés physiquement distinctes?	5
Tous les éléments du canal sont-ils enfermés dans des boîtiers blindés séparés?	5
Les entrées dans les canaux sont-elles entièrement séparées, par exemple il n'existe aucune résistance de mode commun?	5
Des bus de données E/S séparés et indépendants sont-ils utilisés pour chaque canal?	5
La connexion transversale ou la transmission de données entre les canaux est-elle évitée, autres que les informations de diagnostic?	5
Diversité/redondance	
Les essais de diagnostic d'un canal sont-ils indépendants du fonctionnement d'un autre canal?	5
Les canaux utilisent-ils des différences temporelles délibérées pour les opérations fonctionnelles (diversité temporelle) afin de réduire le risque de défaillances coïncidentes?	10
Des logiciels embarqués différents développés séparément sont-ils utilisés dans plusieurs canaux?	10
L'intervalle d'essai de diagnostic de chaque canal est-il inférieur à 1 min?	10
Au moins un canal utilise-t-il substantiellement la technologie des autres canaux, par exemple un relais électromagnétique dans un canal et un relais électronique dans les autres?	10
Conception	
Les bus de données E/S ont-ils une bonne détection des erreurs?	5
Les concepteurs de FS-PLC ont-ils une expérience préalable sur l'élimination des défaillances de cause commune?	5
Evaluation/analyse	
L'analyse des effets et des modes de défaillance du matériel a-t-elle été utilisée lors du processus de conception pour identifier et éliminer les sources de défaillances de cause commune?	10

Elément	Score
La conception à canaux multiples a-t-elle été parfaitement examinée par le personnel compétent, indépendamment de l'équipe de conception?	10
Contrôle de l'environnement	
Existe-t-il des mesures pour détecter et réagir au dépassement de température?	5
La sensibilité de la compatibilité électromagnétique a-t-elle été soumise à essais à des niveaux industriels élevés plutôt que standard?	10
Existe-t-il des protections environnementales supplémentaires significatives?	5

A l'aide du Tableau E.1, il convient d'ajouter les éléments considérés comme affectant la conception à canaux multiples afin de fournir un score global pour la conception du FS-PLC. Lorsque des méthodes équivalentes visant à éviter les défaillances de cause commune ont été utilisées dans la conception du FS-PLC, le score approprié peut être déclaré à condition que l'équivalence soit justifiée.

Ce score global peut être utilisé pour déterminer un facteur de défaillance de cause commune (β) à l'aide du Tableau E.2.

Tableau E.2 – Estimation du facteur de défaillance de cause commune

Score global	Facteur de défaillance de cause commune β
<45	5 % (0,05)
45 – 70	2 % (0,02)
>70	1 % (0,01)

Le taux de défaillance de cause commune pour les défaillances dangereuses non détectées est déterminé en multipliant le taux de défaillances aléatoires dangereuses non détectées du matériel pour un canal par le facteur de défaillance de cause commune (β).

Bibliographie

CEI 60050-191:1990, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-2:2004, *Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

CEI 61000 (toutes les parties), *Compatibilité électromagnétique (CEM)*

CEI 61025:2006, *Analyse par arbre de panne (AAP)*

CEI 61069-7:1999, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 7: Evaluation de la sécurité d'un système*

CEI 61078:2006, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

CEI 61131-3:2003, *Programmable controllers – Part 3: Programming languages* (disponible en anglais seulement)

CEI 61165:2006, *Application des techniques de Markov*

CEI 61496-1:2008, *Sécurité des machines – Equipements de protection électro-sensibles – Partie 1: Prescriptions générales et essais*

CEI 61496-3:2008, *Sécurité des machines – Equipements de protection électro-sensibles – Partie 3: Exigences particulières pour les équipements utilisant des dispositifs protecteurs optoélectroniques actifs sensibles aux réflexions diffuses (AOPDDR)*

CEI 61506:1997, *Mesure et commande dans les processus industriels – Documentation des logiciels d'application*

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

CEI 61508-7:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

CEI 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

CEI 61511-1:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel*

CEI 61511-2:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de la CEI 61511-1*

CEI 61511-3:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

CEI 62061:2005, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

CEI 62079:2001, *Etablissement des instructions – Structure, contenu et présentation*

CEI/TR 62380:2004, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment* (disponible en anglais seulement)

Guide CEI 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications* (disponible en anglais seulement)

CISPR 11:2009, *Appareils industriels, scientifiques et médicaux – Caractéristiques de perturbations radioélectriques – Limites et méthodes de mesure*

ISO/CEI 2382 (toutes les parties), *Technologies de l'information – Vocabulaire*

ISO/CEI 2382-1, *Technologies de l'information – Vocabulaire – Partie 1:Termes fondamentaux*

ISO/CEI 2382-14, *Technologies de l'information – Vocabulaire – Partie 14:Fiabilite, maintenabilite et disponibilite*

ISO/CEI 12207:2008, *Ingénierie des systèmes et du logiciel – Processus du cycle de vie du logiciel*

ISO 8402:1994, *Management de la qualité et assurance de la qualité – Vocabulaire*

ISO 9000-3:1997, *Normes pour le management de la qualité et l'assurance de la qualité – Partie 3: Lignes directrices pour l'application de l'ISO 9001:1994 au développement, à la mise à disposition, à l'installation et à la maintenance du logiciel*

ISO 9001:2008, *Systèmes de management de la qualité – Exigences*

ISO 13849-1:2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2:2003, *Sécurité des machines – Parties des systèmes de commande relatifs à la sécurité – Partie 2: Validation*

ISO 14224:2006, *Industries du pétrole, de la pétrochimie et du gaz naturel – Recueil et échange de données de fiabilité et de maintenance des équipements*

IEEE 352-1987, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems* (disponible en anglais seulement)

IEEE 828-2005, *IEEE Standard for Software Configuration Management Plans* (disponible en anglais seulement)

IEEE 1042-1987, *IEEE Guide to Software Configuration Management* (disponible en anglais seulement)

ISA TR 84.00.02:2002, *Part-1, Safety Instrumented Function (SIF) – Safety Integrity Level* (disponible en anglais seulement)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch