BS EN 61131-6:2012

BSI Standards Publication

Programmable controllers

Part 6: Functional safety

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 61131-6:2012. It is identical to IEC 61131-6:2012.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/2, Elements of systems.

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

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

Published by BSI Standards Limited 2013

ISBN 978 0 580 76606 0

ICS 25.040.40; 35.240.50

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2013.

Amendments issued since publication

Amd. No.	Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61131-6

November 2012

ICS 25.040.40; 35.240.50

English version

Programmable controllers - Part 6: Functional safety

(IEC 61131-6:2012)

Automates programmables - Partie 6: Sécurité fonctionnelle (CEI 61131-6:2012)

Speicherprogrammierbare Steuerungen – Teil 6: Funktionale Sicherheit (IEC 61131-6:2012)

This European Standard was approved by CENELEC on 2012-11-06. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 61131-6:2012 E

Foreword

The text of document 65B/831/FDIS, future edition 1 of IEC 61131-6, prepared by SC 65B, "Devices & process analysis", of IEC TC 65, "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61131-6:2012.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2013-08-06
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2015-11-06

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

Endorsement notice

The text of the International Standard IEC 61131-6:2012 was approved by CENELEC as a European Standard without any modification.

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

IEC 60300-3-2:2004	NOTE Harmonized as EN 60300-3-2:2005 (not modified).
IEC 61000 series	NOTE Harmonized in EN 61000 series (not modified).
IEC 61025:2006	NOTE Harmonized as EN 61025:2007 (not modified).
IEC 61069-7:1999	NOTE Harmonized as EN 61069-7:1999 (not modified).
IEC 61078:2006	NOTE Harmonized as EN 61078:2006 (not modified).
IEC 61131-3:2003	NOTE Harmonized as EN 61131-3:2003 (not modified).
IEC 61165:2006	NOTE Harmonized as EN 61165:2006 (not modified).
IEC 61496-1:2004 + A1:2007	NOTE Harmonized as EN 61496-1:2004 (modified) + A1:2008 (not modified).
IEC 61496-3:2008	NOTE Harmonized as CLC/TS 61496-3:2008 (not modified).
IEC 61508 series	NOTE Harmonized in EN 61508 series (not modified).
IEC 61508-4:2010	NOTE Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE Harmonized as EN 61508-5:2010 (not modified).
IEC 61508-7:2010	NOTE Harmonized as EN 61508-7:2010 (not modified).
IEC 61511-1:2003	NOTE Harmonized as EN 61511-1:2004 (not modified).
IEC 61511-2:2003	NOTE Harmonized as EN 61511-2:2004 (not modified).
IEC 61511-3:2003	NOTE Harmonized as EN 61511-3:2004 (not modified).

IEC 62061:2005	NOTE Harmonized as EN 62061:2005 (not modified).
IEC 62079:2001	NOTE Harmonized as EN 62079:2001 (not modified).
CISPR 11:2009	NOTE Harmonized as EN 55011:2009 (modified).
ISO 8402:1994	NOTE Harmonized as EN ISO 8402:1995 (not modified).
ISO 9000-3:1997	NOTE Harmonized as EN ISO 9000-3:1997 (not modified).
ISO 9001:2008	NOTE Harmonized as EN ISO 9001:2008 (not modified).
ISO 13849-1:2006	NOTE Harmonized as EN ISO 13849-1:2008 (not modified).
ISO 13849-2:2003	NOTE Harmonized as EN ISO 13849-2:2003 (not modified).
ISO 14224:2006	NOTE Harmonized as EN ISO 14224:2006 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

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

Publication	Year	Title	EN/HD	Year
IEC 60947-5-1	2003	Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices	EN 60947-5-1 + corr. July	2004 2005
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	EN 61000-4-2	2009
IEC 61000-4-3	2006	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test	EN 61000-4-3	2006
IEC 61000-4-4	2012	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test	EN 61000-4-4	2012
IEC 61000-4-5 + corr. October	2005 2009	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test	EN 61000-4-5	2006
IEC 61000-4-6	2008	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields	EN 61000-4-6	2009
IEC 61000-4-8	2009	Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test	EN 61000-4-8	2010
IEC 61131-1	2003	Programmable controllers - Part 1: General information	EN 61131-1	2003
IEC 61131-2	2007	Programmable controllers - Part 2: Equipment requirements and tests	EN 61131-2	2007
IEC/TR 61131-4	2004	Programmable controllers - Part 4: User guidelines	-	-

Publication	Year	Title	EN/HD	Year
IEC 61326-3-1 + corr. August	2008 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	EN 61326-3-1	2008
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	EN 61326-3-2	2008
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2010
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
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	EN 61508-6	2010
IEC 61784-3	2010	Industrial communication networks - Profiles – Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	2010
IEC 62443	Series	Security for industrial process measurement and control - 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	-	-

CONTENTS

INTRODUCTION 8
1 Scope 10
2 Normative references 11
3 Terms and definitions 12
4 Conformance to this standard 25
5 FS-PLC safety lifecycle 25
5.1 General 25
5.2 FS-PLC functional safety SIL capability requirements 27
5.2.1 General 27
5.2.2 Data security 28
5.3 Quality management system 28
5.4 Management of FS-PLC safety lifecycle 29
5.4.1 Objectives 29
5.4.2 Requirements and procedures 29
5.4.3 Execution and monitoring 33
5.4.4 Management of functional safety 33
6 FS-PLC design requirements specification 33
6.1 General 33
6.2 Design requirements specification contents 34
6.3 Target failure rate 35
7 FS-PLC design, development and validation plan 36
7.1 General 36
7.2 Segmenting requirements 36
8 FS-PLC architecture 37
8.1 General 37
8.2 Architectures and subsystems 38
8.3 Data communication 38
9 HW design, development and validation planning 38
9.1 HW general requirements 38
9.2 HW functional safety requirements specification 38
9.3 HW safety validation planning 38
9.4 HW design and development 39
9.4.1 General 39
9.4.2 Requirements for FS-PLC behaviour on detection of a fault 39
9.4.3 HW safety integrity 40
9.4.4 Random HW failures 48
9.4.5 HW requirements for the avoidance of systematic failures 53
9.4.6 HW requirements for the control of systematic faults 53
9.4.7 HW classification of faults 54
9.4.8 HW implementation 55
9.4.9 De-rating of components 56
9.4.10 ASIC design and development 56
9.4.11 Techniques and measures to prevent the introduction of faults in ASICs 56

9.5 HW and embedded SW and FS-PLC integration 56
9.6 HW operation and maintenance procedures 57
9.6.1 Objective 57
9.6.2 Requirements 57
9.7 HW safety validation 58
9.7.1 General 58
9.7.2 Requirements 58
9.8 HW verification 59
9.8.1 Objective 59
9.8.2 Requirements 59
10 FS-PLC SW design and development 60
10.1 General 60
10.2 Requirements 61
10.3 Classification of engineering tools 61
10.4 SW safety validation planning 62
11 FS-PLC safety validation 62
12 FS-PLC type tests 62
12.1 General 62
12.2 Type test requirements 62
12.3 Climatic test requirements 65
12.4 Mechanical test requirements 65
12.5 EMC test requirements 65
12.5.1 General 65
12.5.2 General EMC environment 65
12.5.3 Specified EMC environment 67
13 FS-PLC verification 69
13.1 Verification plan 69
13.2 Fault insertion test requirements 70
13.3 As qualified versus as shipped 71
14 Functional safety assessment 71
14.1 Objective 71
14.2 Assessment requirements 72
14.2.1 Assessment evidence and documentation 72
14.2.2 Assessment method 72
14.3 FS-PLC assessment information 74
14.4 Independence 74
15 FS-PLC operation, maintenance and modification procedures 75
15.1 Objective 75
15.2 FS-PLC modification 75
16 Information to be provided by the FS-PLC manufacturer for the user 76
16.1 General 76
16.2 Information on conformance to this standard 76
16.3 Information on type and content of documentation 76
16.4 Information on catalogues and/or datasheets 76
16.5 Safety manual 76
16.5.1 General 76
16.5.2 Safety manual contents 76
Annex A (informative) Reliability calculations 79

Annex B (informative) Typical FS-PLC Architectures 80
Annex C (informative) Energise to trip applications of FS-PLC 86
Annex D (informative) Available failure rate databases 88
Annex E (informative) Methodology for the estimation of common cause failure rates in a multiple channel FS-PLC 90
Bibliography 92

Figure 1 – FS-PLC in the overall E/E/PE safety-related system safety lifecycle phases 9
Figure 2 – Failure model 16
Figure 3 – FS-PLC safety lifecycle (in realization phase) 26
Figure 4 – Relevant parts of a safety function 35
Figure 5 – FS-PLC to engineering tools relationship 37
Figure 6 – HW subsystem decomposition 43
Figure 7 – Example: determination of the maximum SIL for specified architecture 45
Figure 8 – Example of limitation on hardware safety integrity for a multiple-channel safety function 47
Figure 9 – Fault classification and FS-PLC behaviour 54
Figure 10 – ASIC development lifecycle (V-Model) 56
Figure 11 – Model of FS-PLC and engineering tools layers 60
Figure B.1 – Single FS-PLC with single I/O and external watchdog (1oo1D) 81
Figure B.2 – Dual PE with single I/O and external watchdogs (1oo1D) 81
Figure B.3 – Dual PE with dual I/O, no inter-processor communication, and 1oo2 shutdown logic 82
Figure B.4 – Dual PE with dual I/O, inter-processor communication, and 1oo2D shutdown logic 83
Figure B.5 – Dual PE with dual I/O, no inter-processor communication, external watchdogs, and 2oo2 shutdown logic 83
Figure B.6 – Dual PE with dual I/O, inter-processor communication, external watchdogs, and 2oo2D shutdown logic 84
Figure B.7 – Triple PE with triple I/O, inter-processor communication, and 2oo3D shutdown logic 85

Table 1 – Safety integrity levels for low demand mode of operation 35
Table 2 – Safety integrity levels for high demand or continuous mode of operation 36
Table 3 – Faults to be detected and notified (alarmed) to the application program 40
Table 4 – Hardware safety integrity – low complexity (type A) subsystem 41
Table 5 – Hardware safety integrity – high complexity (type B) subsystem 41
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 50
Table 7 – Examples of tool classification 61
Table 8 – Performance criteria 64
Table 9 – Immunity test levels for enclosure port tests in general EMC environment 66
Table 10 – Immunity test levels in general EMC environment 67
Table 11 – Immunity test levels for enclosure port tests in specified EMC environment 68
Table 12 – Immunity test levels in specified EMC environment 69
Table 13 – Fault tolerance test, required effectiveness 71

Table 14 – Functional safety assessment Information 74
Table 15 – Minimum levels of independence of those carrying out functional safety assessment 75
Table E.1 – Criteria for estimation of common cause failure 90
Table E.2 – Estimation of common cause failure factor 91

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.

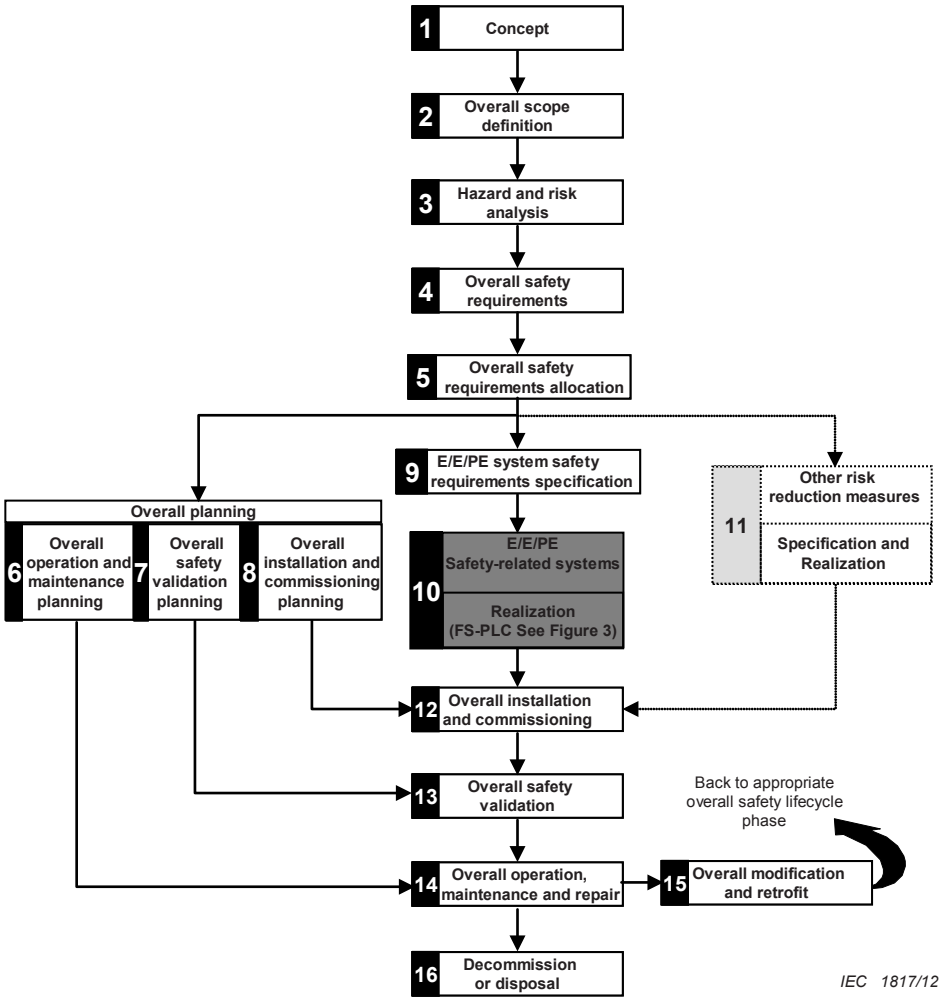
In keeping with 1.1 of IEC 61508-1:2010, this part encompasses the product specific requirements of IEC 61508-1, 61508-2 and 61508-3 as pertaining to programmable controllers and their associated peripherals.

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

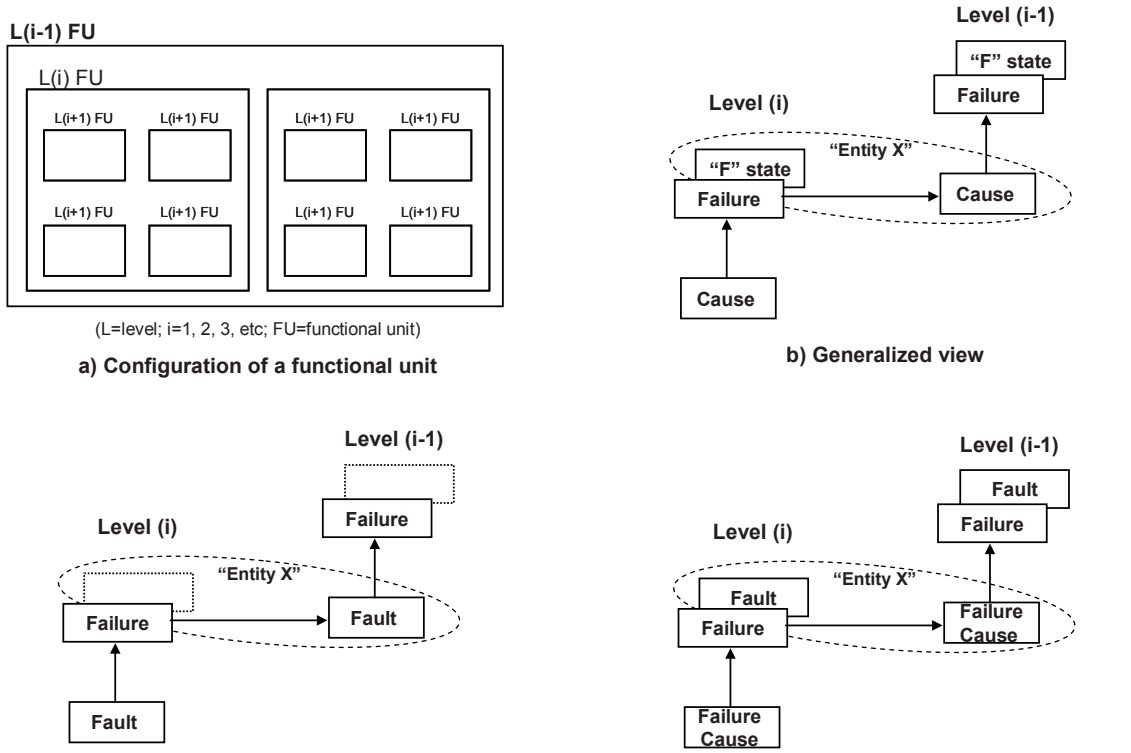
Note 1 to entry: This is based on IEC 60050-191:1990, 191-04-01 with changes to include systematic failures due to, for example, deficiencies in specification or software.

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 ($\lambda(t)$) of an entity (single components or systems) such that $\lambda(t).dt$ 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.

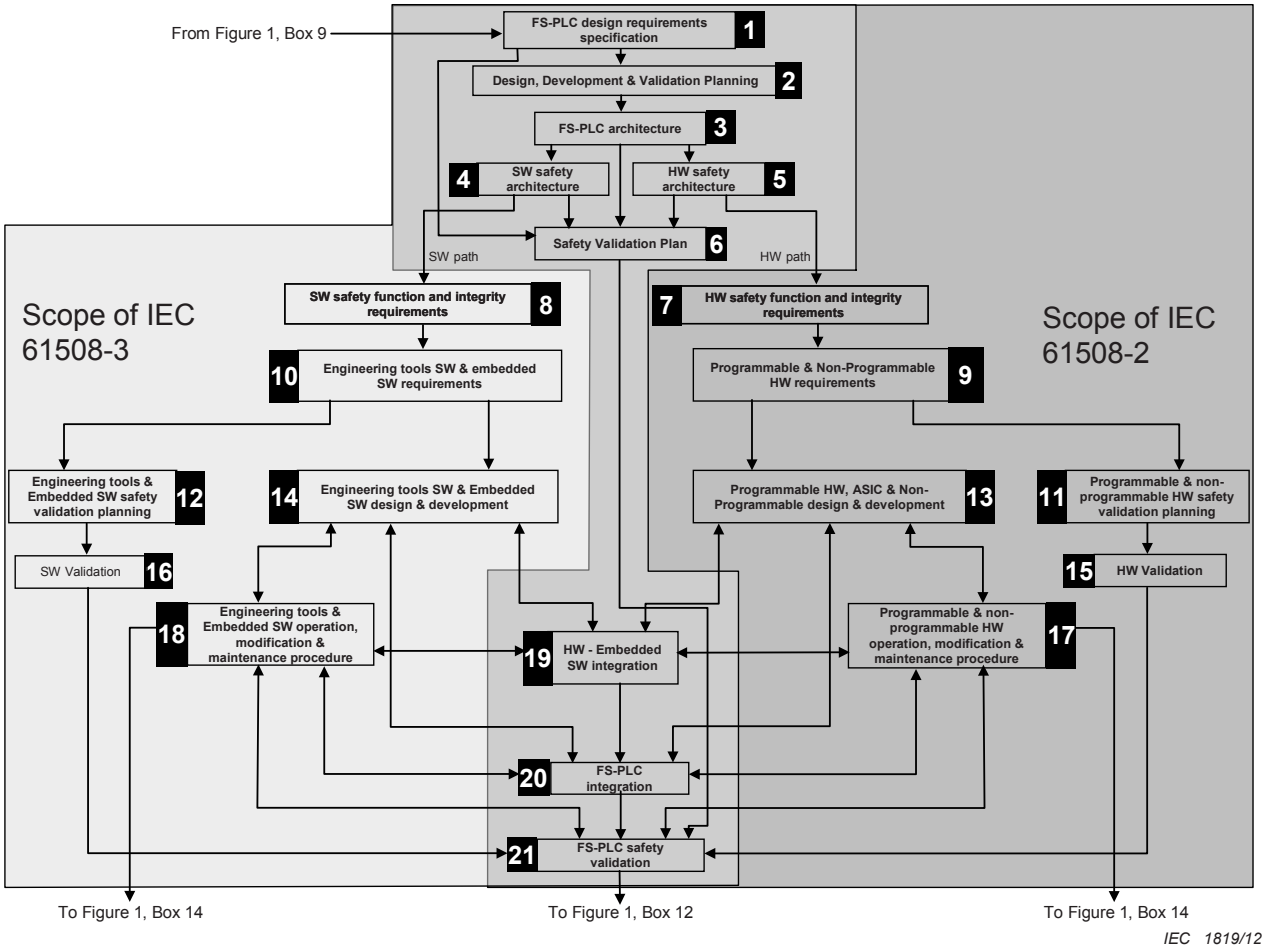
Conformance to these clauses and subclauses is the responsibility of the manufacturer of the FS-PLC.

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.

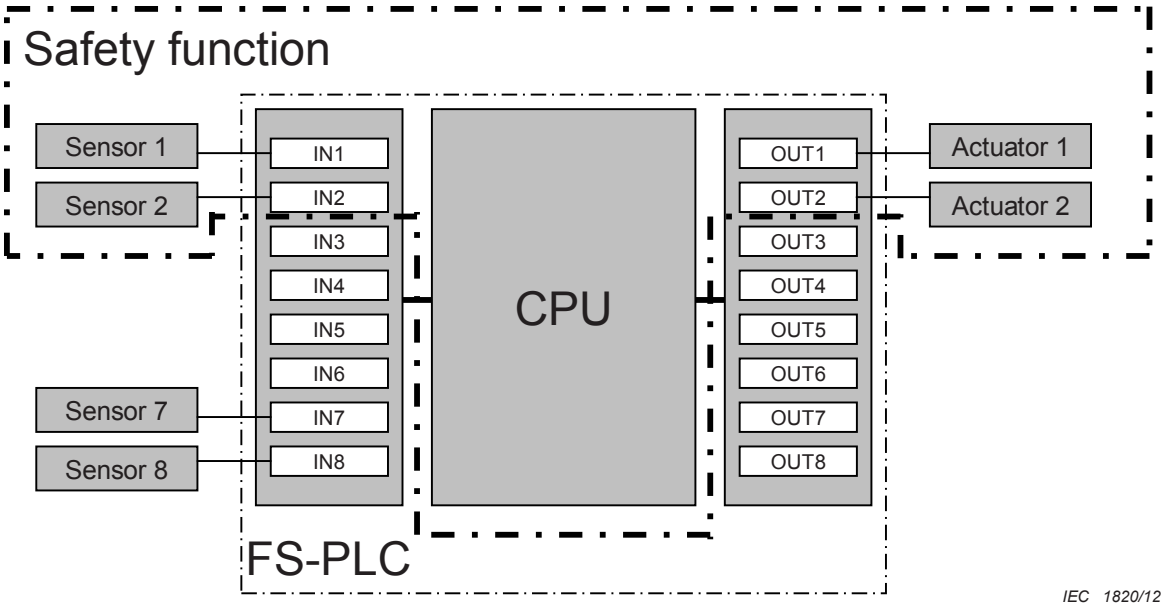


Figure 4 – Relevant parts of a safety function

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.

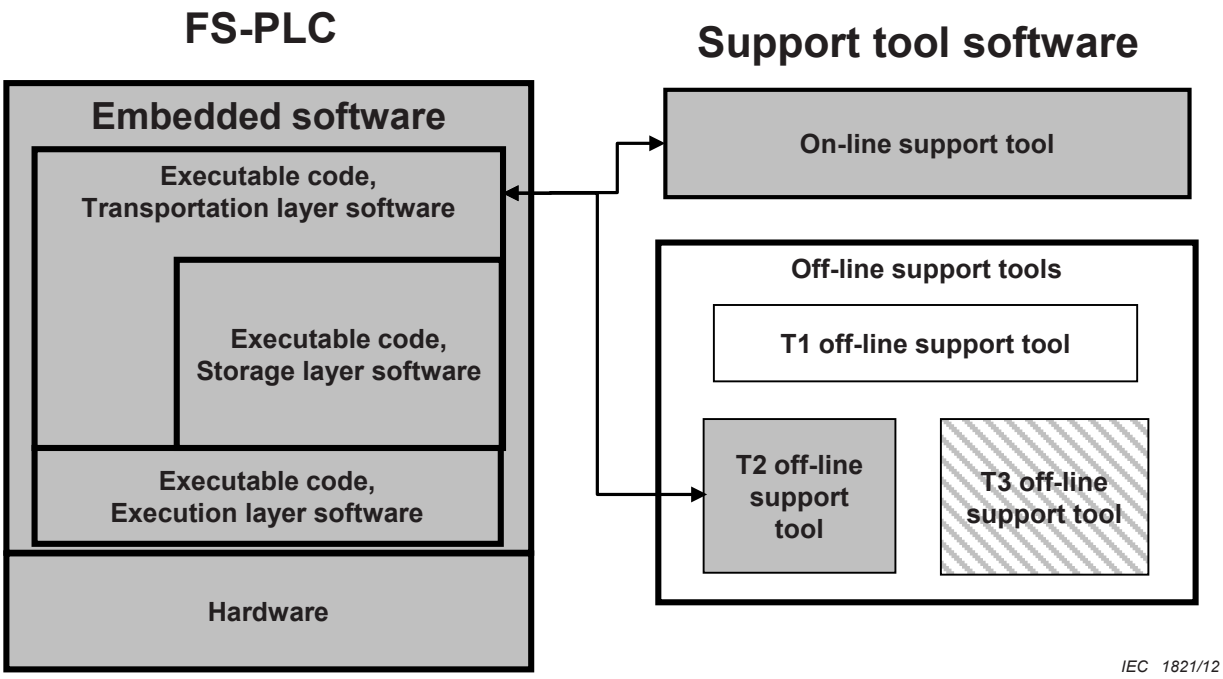


Figure 5 – FS-PLC to engineering tools relationship

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.

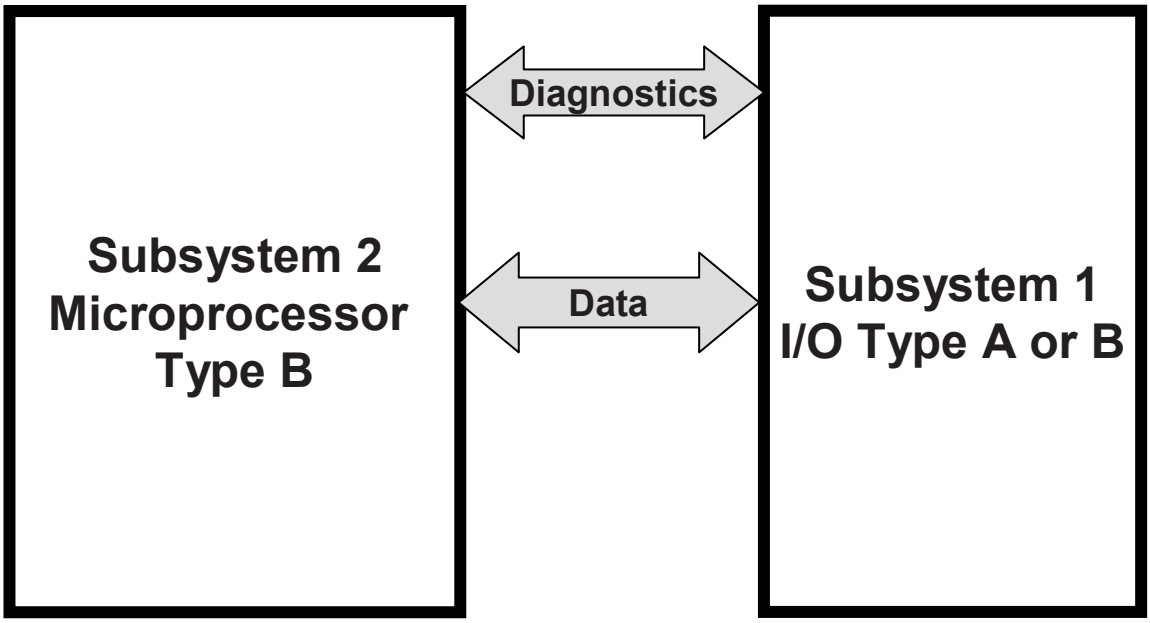


Figure 6 – HW subsystem decomposition

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.

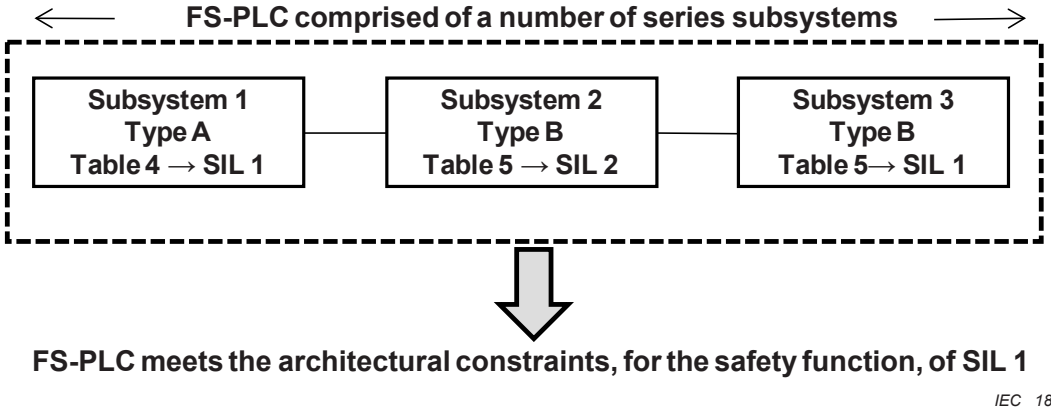


Figure 7 – Example: determination of the maximum SIL for specified architecture

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:

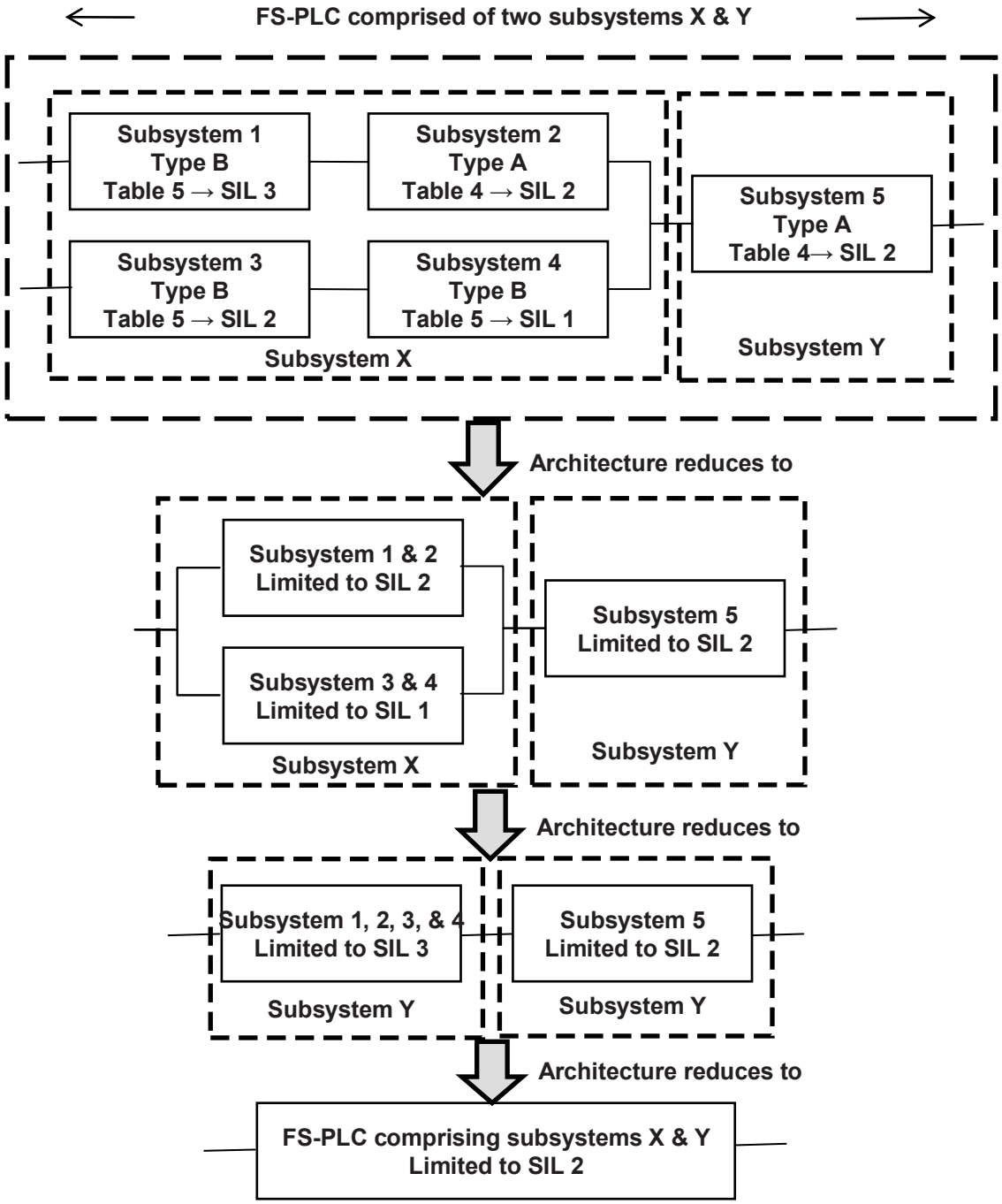
a) Combining subsystems 1 and 2: The hardware fault tolerance and safe failure fraction achieved by the combination of subsystems 1 and 2 (each separately meeting the requirements for SIL 3 and SIL 2 respectively) meet the requirements of SIL 2 (determined by subsystem 2; see 9.4.3.2.5);

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.

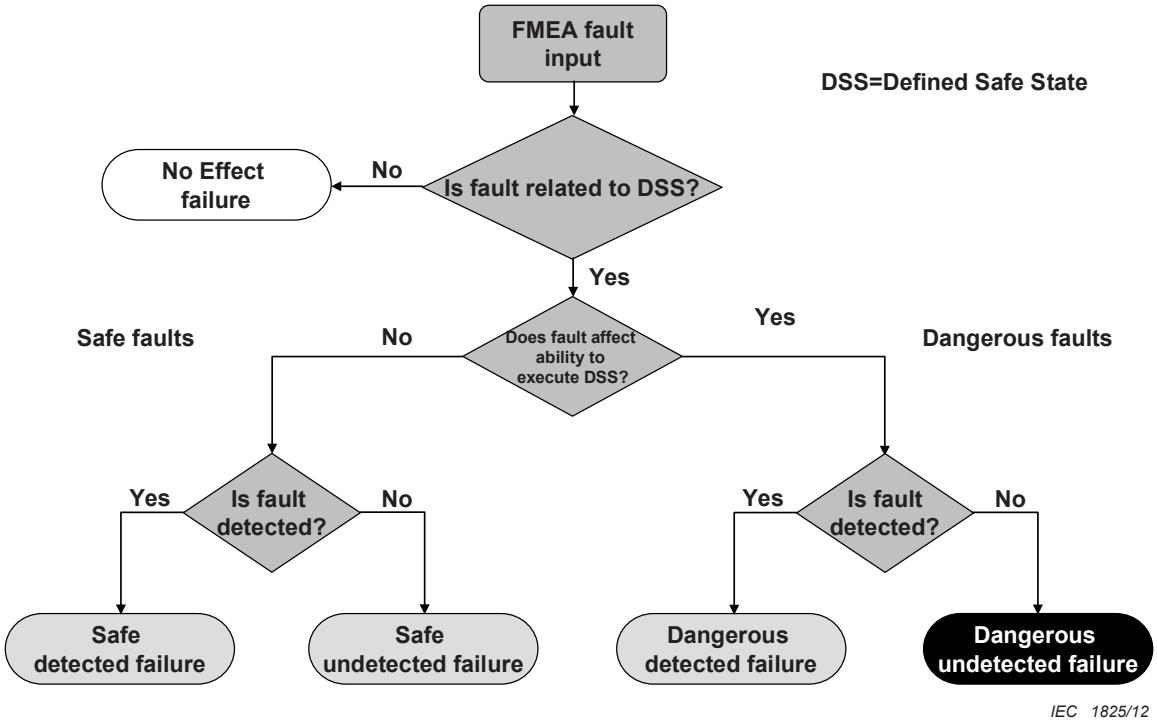


Figure 9 – Fault classification and FS-PLC behaviour

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).

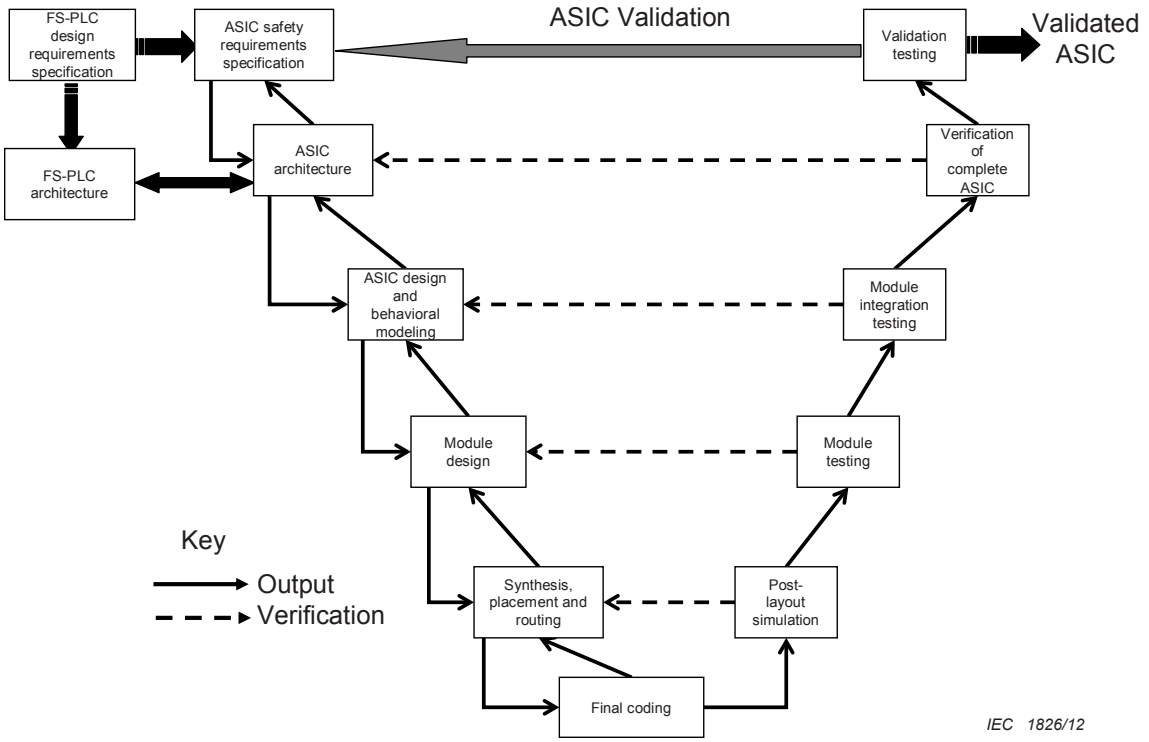


Figure 10 – ASIC development lifecycle (V-Model)

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.

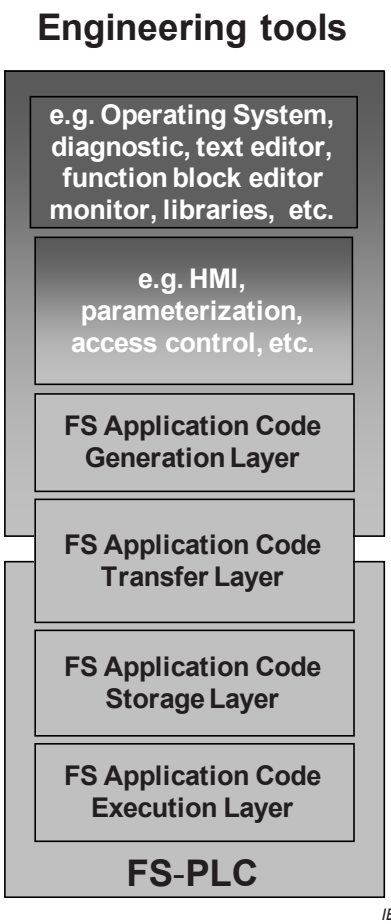


Figure 11 – Model of FS-PLC and engineering tools layers

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)

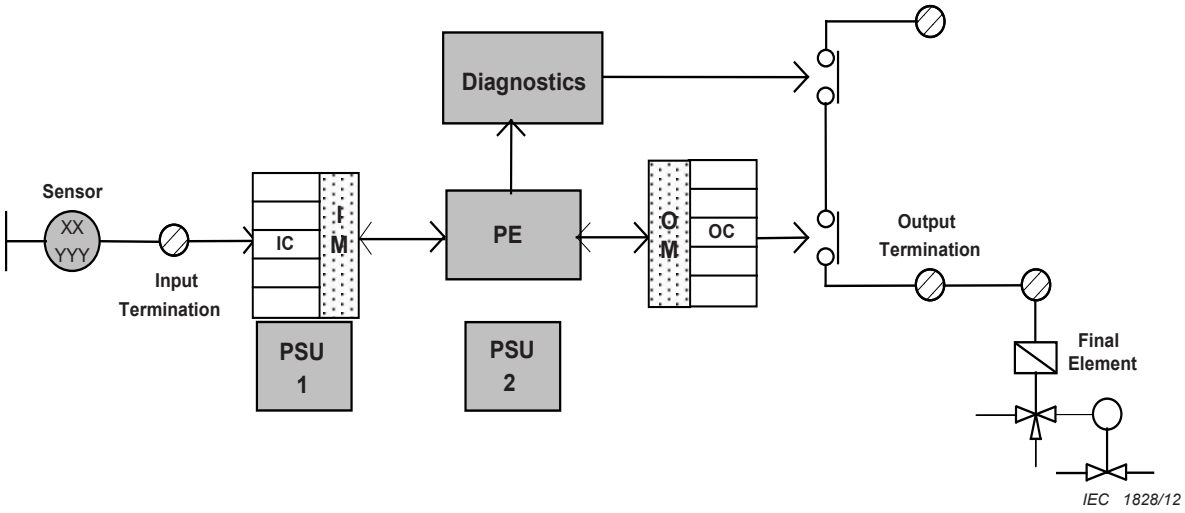


Figure B.1 – Single FS-PLC with single I/O and external watchdog (1oo1D)

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)

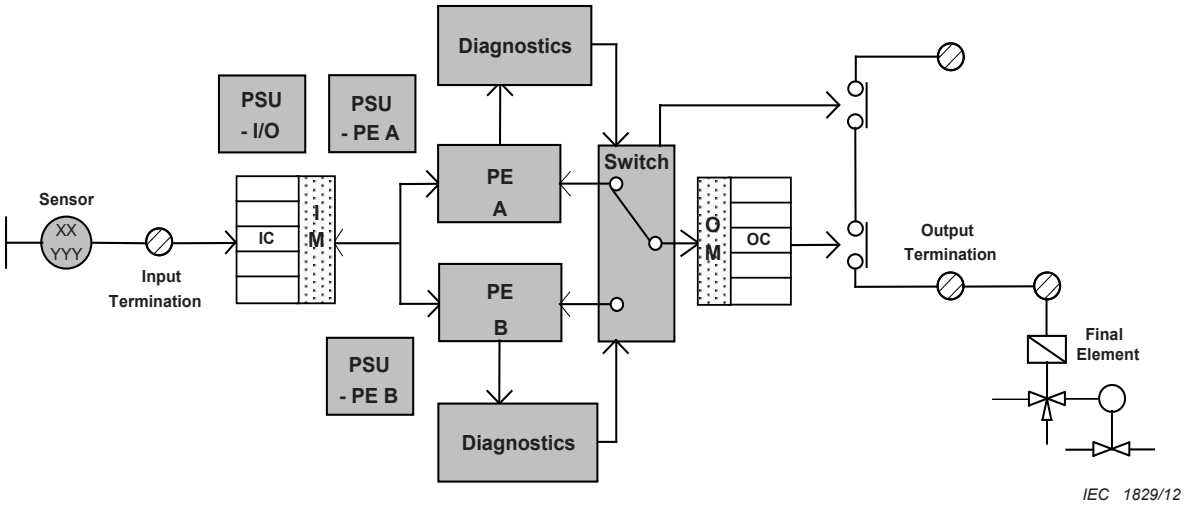


Figure B.2 – Dual PE with single I/O and external watchdogs (1oo1D)

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

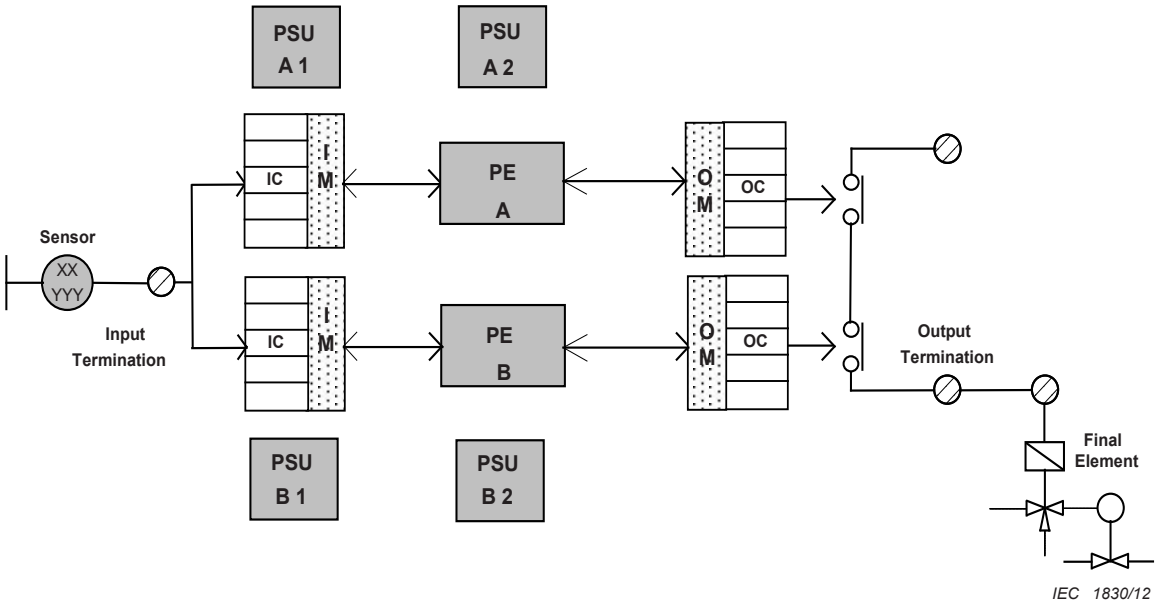


Figure B.3 – Dual PE with dual I/O, no inter-processor communication, and 1oo2 shutdown logic

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

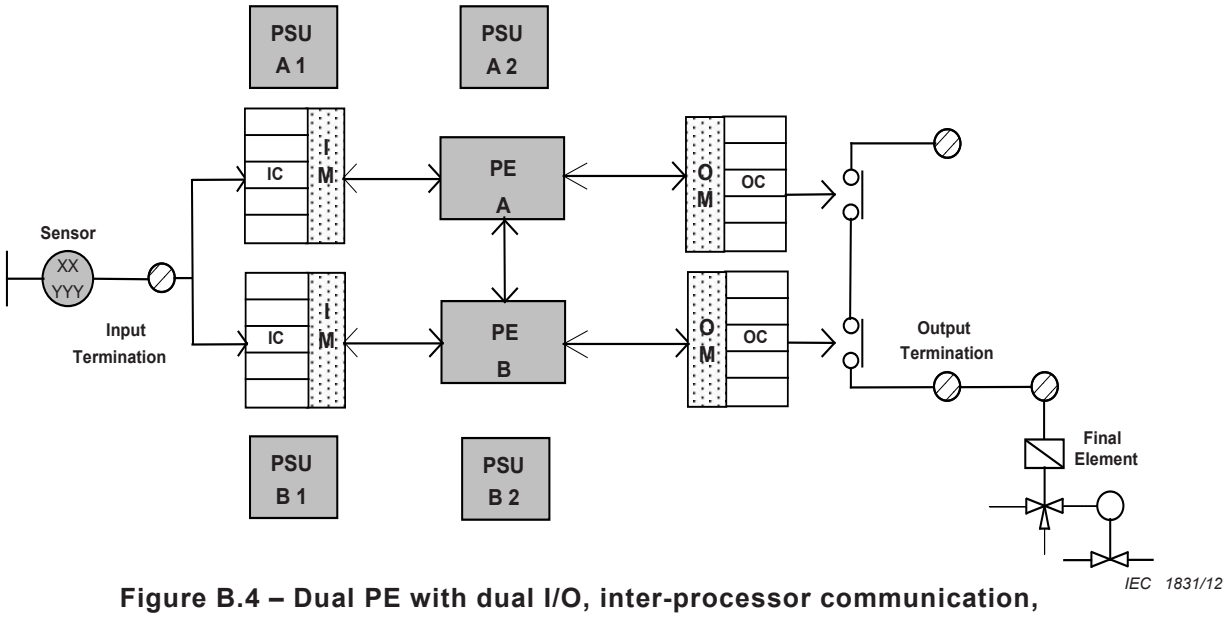


Figure B.4 – Dual PE with dual I/O, inter-processor communication, and 1oo2D shutdown logic

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

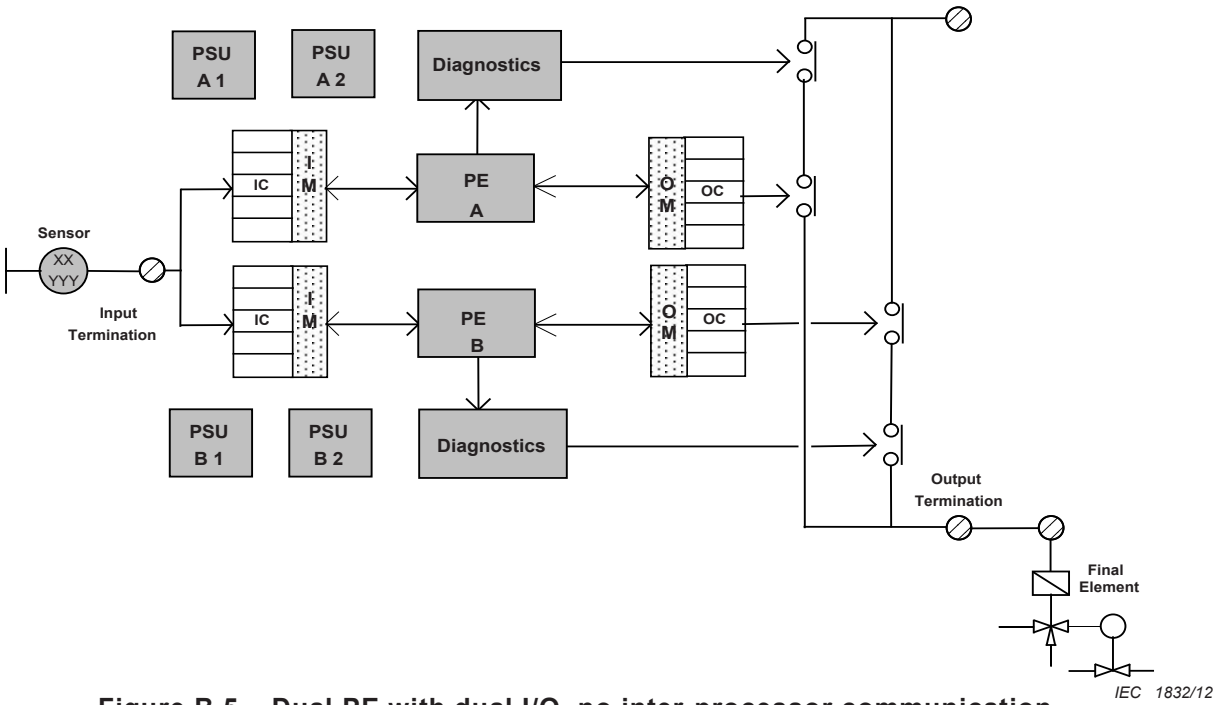


Figure B.5 – Dual PE with dual I/O, no inter-processor communication, external watchdogs, and 2oo2 shutdown logic

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

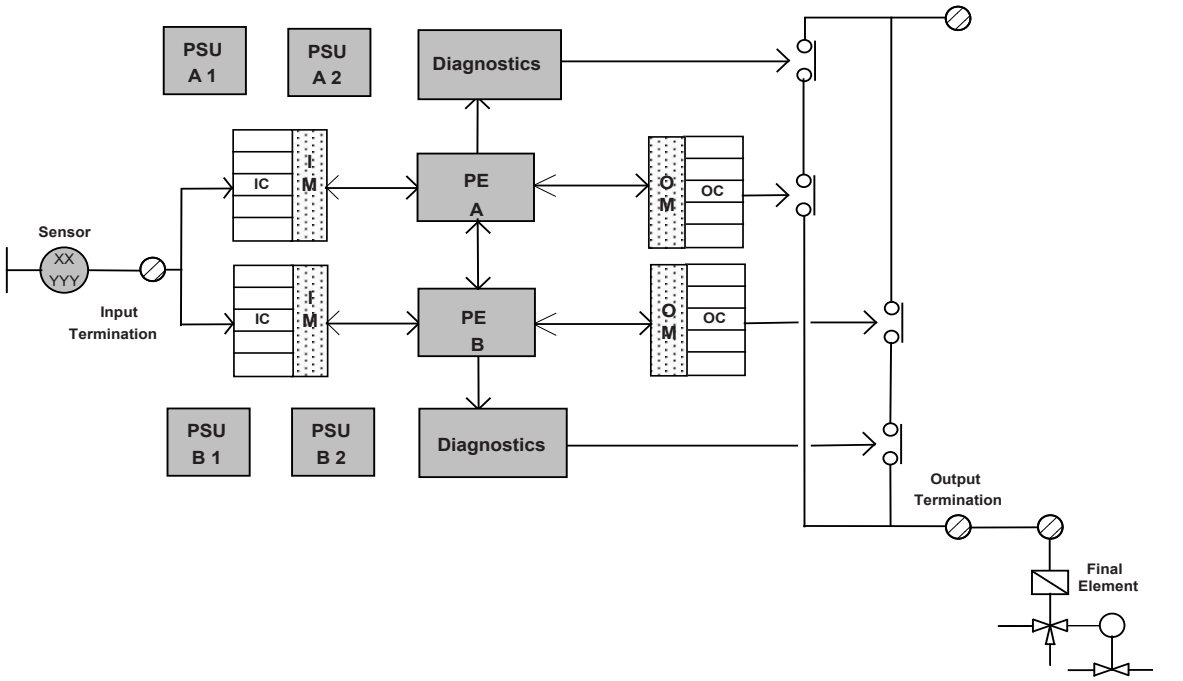


Figure B.6 – Dual PE with dual I/O, inter-processor communication, external watchdogs, and 2oo2D shutdown logic

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

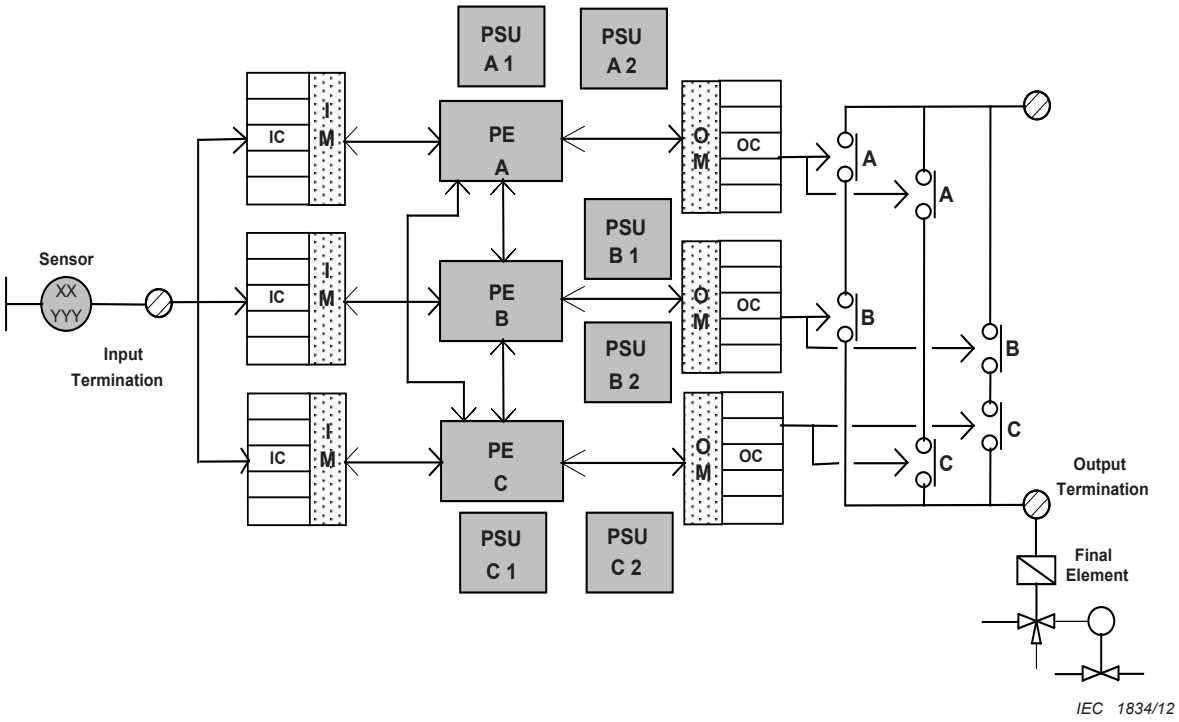


Figure B.7 – Triple PE with triple I/O, inter-processor communication, and 2oo3D shutdown logic

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*

_____

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™