IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable controllers – Part 6: Functional safety

Automates programmables – Partie 6: Sécurité fonctionnelle

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XD
CODE PRIX

ICS 25.040.40; 35.240.50

ISBN 978-2-83220-402-3

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 6
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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PROGRAMMABLE CONTROLLERS –

Part 6: Functional safety

FOREWORD

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

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

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

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

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

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

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

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

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

INTRODUCTION

General

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

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

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

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

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

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

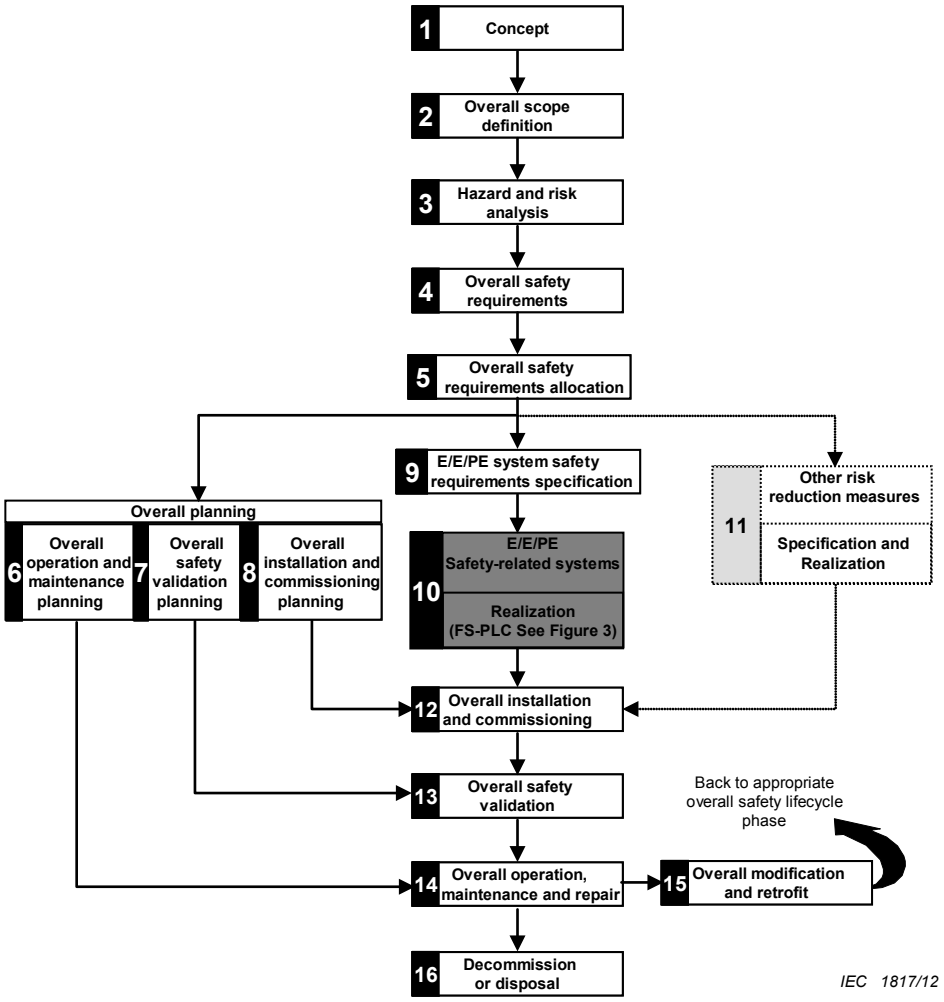
In keeping with 1.1 of IEC 61508-1:2010, this part encompasses the product specific requirements of IEC 61508-1, 61508-2 and 61508-3 as pertaining to programmable controllers and their associated peripherals.

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

Framework of this part

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

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



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

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

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

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

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

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

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

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

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

PROGRAMMABLE CONTROLLERS –

Part 6: Functional safety

1 Scope

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

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

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

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

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

The objective of this part is:

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SOMMAIRE

AVANT-PROPOS 98
INTRODUCTION 100
1 Domaine d'application 104
2 Références normatives 105
3 Termes et définitions 106
4 Conformité à la présente norme 121
5 Cycle de vie de sécurité du FS-PLC 121
5.1 Généralités 121
5.2 Exigences du niveau d'intégrité de sécurité fonctionnelle du FS-PLC 124
5.2.1 Généralités 124
5.2.2 Sécurité des données 125
5.3 Système de gestion de la qualité 126
5.4 Gestion du cycle de vie de sécurité du FS-PLC 126
5.4.1 Objectifs 126
5.4.2 Exigences et procédures 126
5.4.3 Exécution et surveillance 131
5.4.4 Gestion de la sécurité fonctionnelle 131
6 Spécification des exigences de conception du FS-PLC 131
6.1 Généralités 131
6.2 Contenu de la spécification des exigences de conception 131
6.3 Taux de défaillance ciblé 133
7 Planification de la conception, du développement et de la validation du FS-PLC 135
7.1 Généralités 135
7.2 Exigences de segmentation 135
8 Architecture du FS-PLC 135
8.1 Généralités 135
8.2 Architectures et sous-systèmes 137
8.3 Communication de données 137
9 Planification de la conception, du développement et de la validation du matériel 137
9.1 Exigences matérielles générales 137
9.2 Spécification des exigences de sécurité fonctionnelle du matériel 137
9.3 Planification de la validation de la sécurité matérielle 138
9.4 Conception et développement du matériel 138
9.4.1 Généralités 138
9.4.2 Exigences pour le comportement du FS-PLC en matière de détection d'une panne 138
9.4.3 Intégrité de sécurité du matériel 139
9.4.4 Défaillances aléatoires du matériel 149
9.4.5 Exigences matérielles permettant d'éviter les défaillances systématiques 154
9.4.6 Exigences matérielles pour le contrôle des pannes systématiques 154
9.4.7 Classification matérielle des pannes 155
9.4.8 Implémentation matérielle 157
9.4.9 Déclassement des composants 157
9.4.10 Conception et développement des circuits intégrés spécifiques 158

9.4.11 Techniques et mesures permettant d'empêcher l'introduction de pannes dans les circuits intégrés spécifiques 160
9.5 Matériel, logiciel intégré et intégration du FS-PLC 160
9.6 Procédures de fonctionnement et de maintenance du matériel 160
9.6.1 Objectif 160
9.6.2 Exigences 160
9.7 Validation de la sécurité du matériel 162
9.7.1 Généralités 162
9.7.2 Exigences 162
9.8 Vérification du matériel 163
9.8.1 Objectif 163
9.8.2 Exigences 163
10 Conception et développement du logiciel du FS-PLC 163
10.1 Généralités 163
10.2 Exigences 165
10.3 Classification des outils d'ingénierie 165
10.4 Planification de la validation de la sécurité logicielle 166
11 Validation de la sécurité du FS-PLC 166
12 Essais de type du FS-PLC 167
12.1 Généralités 167
12.2 Exigences d'essai de type 167
12.3 Exigences d'essai climatiques 170
12.4 Exigences d'essai mécanique 170
12.5 Exigences d'essai CEM 170
12.5.1 Généralités 170
12.5.2 Environnement CEM général 170
12.5.3 Environnement CEM spécifié 172
13 Vérification du FS-PLC 174
13.1 Plan de vérification 174
13.2 Exigences des essais de génération de panne 175
13.3 Comparaison des produits «tels que qualifiés» et «tels qu'expédiés» 176
14 Evaluation de la sécurité fonctionnelle 177
14.1 Objectif 177
14.2 Exigences d'évaluation 177
14.2.1 Preuves et documentation concernant l'évaluation 177
14.2.2 Méthode d'évaluation 178
14.3 Informations de l'évaluation du FS-PLC 179
14.4 Indépendance 180
15 Procédures de fonctionnement, de maintenance et de modification du FS-PLC 181
15.1 Objectif 181
15.2 Modification du FS-PLC 181
16 Informations destinées à l'utilisateur devant être fournies par le fabricant du FS-PLC 182
16.1 Généralités 182
16.2 Informations sur la conformité à la présente Norme 182
16.3 Informations sur le type et le contenu de la documentation 182
16.4 Informations sur les catalogues et/ou fiches techniques 182
16.5 Manuel de sécurité 182

16.5.1 Généralités 182
16.5.2 Contenu du manuel de sécurité 183
Annexe A (informative) Calculs de fiabilité 185
Annexe B (informative) Architectures FS-PLC typiques 186
Annexe C (informative) Applications d'alimentation au déclenchement du FS-PLC 195
Annexe D (informative) Bases de données des taux de défaillance disponibles 197
Annexe E (informative) Méthodologie pour l'estimation des taux de défaillance de cause commune dans un FS-PLC à canaux multiples 199
Bibliographie 201

Figure 1 – FS-PLC dans l'ensemble des phases du cycle de vie de sécurité d'un système électrique/électronique/électronique programmable relatif à la sécurité 102
Figure 2 – Modèle de défaillance 112
Figure 3 – Cycle de vie de sécurité du FS-PLC (en phase de réalisation) 123
Figure 4 – Parties appropriées d'une fonction de sécurité 134
Figure 5 – Relation entre le FS-PLC et les outils d'ingénierie 136
Figure 6 – Décomposition du sous-système matériel 142
Figure 7 – Exemple: détermination du niveau d'intégrité de sécurité maximal pour l'architecture spécifiée 145
Figure 8 – Exemple de limitation sur l'intégrité de sécurité matérielle pour une fonction de sécurité à canaux multiples 148
Figure 9 – Classification des pannes et comportement du FS-PLC 156
Figure 10 – Cycle de développement des circuits intégrés spécifiques (modèle en V) 159
Figure 11 – Modèle du FS-PLC et couches pour les outils d'ingénierie 164
Figure B.1 – FS-PLC unique avec E/S unique et horloge de surveillance externe (1oo1D) 187
Figure B.2 – Processeur élémentaire double avec E/S unique et horloges de surveillance externes (1oo1D) 188
Figure B.3 – Processeur élémentaire double avec E/S double, aucune communication inter-processeurs et logique de fermeture 1oo2 189
Figure B.4 – Processeur élémentaire double avec E/S double, communication inter-processeurs et logique de fermeture 1oo2D 190
Figure B.5 – Processeur élémentaire double avec E/S double, aucune communication inter-processeurs, horloges de surveillance externes et logique de fermeture 2oo2 191
Figure B.6 – Processeur élémentaire double avec E/S double, communication inter-processeurs, horloges de surveillance externes et logique de fermeture 2oo2D 192
Figure B.7 – Processeur élémentaire triple avec E/S triple, communication inter-processeurs et logique de fermeture 2oo3D 193

Tableau 1 – Niveaux d'intégrité de sécurité pour un mode de fonctionnement à faible sollicitation 134
Tableau 2 – Niveaux d'intégrité de sécurité pour un mode de fonctionnement à sollicitation élevée/continue 134
Tableau 3 – Pannes à détecter et à notifier (alarme) au programme d'application 139
Tableau 4 – Intégrité de sécurité matérielle – sous-système peu complexe (type A) 140
Tableau 5 – Intégrité de sécurité matérielle – sous-système très complexe (type B) 140

Tableau 6 – Pannes ou défaillances à considérer lors de la quantification de l'effet des défaillances aléatoires du matériel ou à prendre en compte pour la détermination du taux de défaillances non dangereuses 151
Tableau 7 – Exemples de classifications d'outils 166
Tableau 8 – Critères de performances 169
Tableau 9 – Niveaux d'immunité des essais pour l'accès enveloppe dans un environnement CEM général 171
Tableau 10 – Niveaux d'immunité des essais dans un environnement CEM général 172
Tableau 11 – Niveaux d'essais d'immunité pour les essais enveloppe dans un environnement CEM spécifié 173
Tableau 12 – Niveaux d'essais d'immunité dans un environnement CEM spécifié 174
Tableau 13 – Essai de tolérance aux pannes, efficacité exigée 176
Tableau 14 – Informations de l'évaluation de la sécurité fonctionnelle 180
Tableau 15 – Niveaux d'indépendance minimum des personnes chargées de procéder à l'évaluation de la sécurité fonctionnelle 181
Tableau E.1 – Critères d'estimation de la défaillance de cause commune 199
Tableau E.2 – Estimation du facteur de défaillance de cause commune 200

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

AUTOMATES PROGRAMMABLES –

Partie 6: Sécurité fonctionnelle

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61131-6 a été établie par le sous-comité 65B: Equipements de mesure et de contrôle-commande, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65B/831/FDIS	65B/850/RVD

Le rapport de vote indiqué dans le tableau ci-dessus fournit toutes les informations sur le vote ayant abouti à l'approbation de la présente norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61131, présentées sous le titre général *Automates programmables,* peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

Généralités

La série CEI 61131 comprend les parties suivantes, regroupées sous le titre général *Automates programmables*:

Partie 1: Informations générales
Partie 2: Exigences et essais des équipements
Partie 3: Langages de programmation
Partie 4: Guide pour l'utilisateur
Partie 5: Communications
Partie 6: Sécurité fonctionnelle
Partie 7: Programmation en logique floue
Partie 8: Lignes directrices pour l'application et la mise en œuvre des langages de programmation

Cette partie de la série CEI 61131 constitue la Partie 6 d'une série de normes sur les automates programmables et leurs périphériques associés, et il convient de la lire conjointement avec les autres parties de la série.

Ce document étant la norme de produit FS-PLC, il convient de respecter les dispositions de cette partie dans le domaine des automates programmables et leurs périphériques associés.

Aucune conformité avec la Partie 6 de la CEI 61131 ne peut être déclarée à moins que les exigences de l'Article 4 de cette partie soient respectées.

Les termes d'utilisation générale sont définis dans la Partie 1 de la CEI 61131. Les termes spécifiques sont définis dans chaque partie.

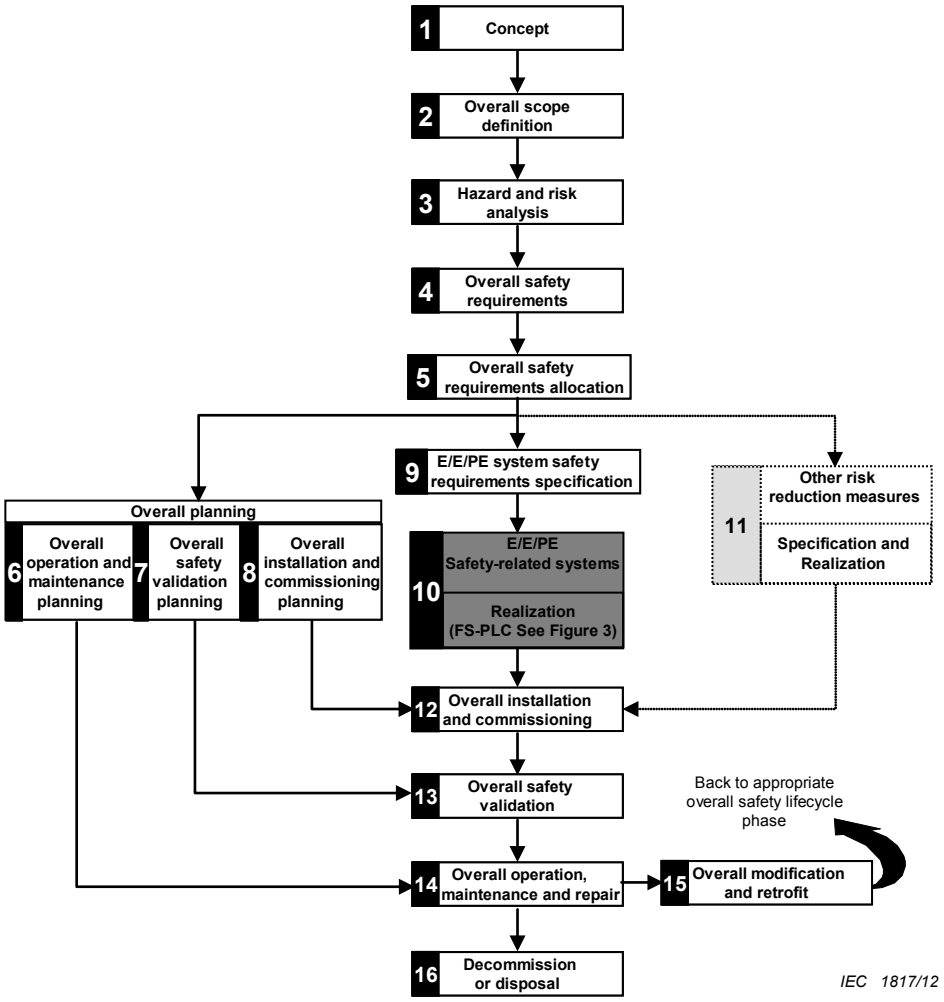
Conformément au 1.1 de la CEI 61508-1:2010, cette partie intègre les exigences spécifiques au produit des CEI 61508-1, 61508-2 et 61508-3 comme appartenant aux automates programmables et à leurs périphériques associés.

L'objectif de ce document est de suivre dans le principe la structure de la série CEI 61508. Cependant, certains aspects n'ont pas de corrélation directe et il est donc nécessaire de les traiter différemment. Cela est dû en partie au fait que l'on aborde dans un seul document le matériel, les logiciels, les microprogrammes, etc.

Structure de cette partie

La Figure 2 de la CEI 61508-1:2010 est incluse ici, sous la dénomination Figure 1. Elle a été ajustée de manière à montrer comment un automate programmable de sécurité fonctionnelle (FS-PLC) s'adapte à l'ensemble du cycle de vie d'un système électrique/électronique/électronique programmable relatif à la sécurité. Bien que la case 10 de la Figure 1 inclue des capteurs, un sous-système logique et des éléments finaux (par exemple, des actionneurs), car c'est le point de vue de la CEI 61508-1, ici, l'accent est mis sur le FS-PLC comme cela est référencé à la Figure 3.

C'est pourquoi la phase Réalisation, Figure 1, case 10, incarne uniquement le sous-système logique, dans la perspective de cette partie.



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

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

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

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

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

Légende

Anglais	Français
Concept	Concept
Overall scope definition	Définition du domaine d'application général
Hazard and risk analysis	Analyse des risques et des dangers
Overall safety requirements	Exigences de sécurité générales
Overall safety requirements allocation	Allocation des exigences de sécurité générales
Overall planning	Planification générale
Overall operation and maintenance planning	Planification générale du fonctionnement et de la maintenance
Overall safety validation planning	Planification générale de la validation de la sécurité
Overall installation and commissioning planning	Planification générale de l'installation et de la mise en service
E/E/PE system safety requirements specification	Spécification des exigences de sécurité pour les systèmes électriques/électroniques/électroniques programmables

Anglais	Français
E/E/PE Safety-related systems	Systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
Realization (FS-PLC See Figure 3)	Réalisation (FS-PLC, voir Figure 3)
Other risk reduction measures	Autres mesures de réduction des risques
Specification and Realization	Spécification et réalisation
Overall installation and commissioning	Installation et mise en service générales
Overall safety validation	Validation générale de la sécurité
Overall operation, maintenance and repair	Fonctionnement, maintenance et réparation généraux
Decommission or disposal	Mise hors service ou destruction
Overall modification and retrofit	Modification et amélioration générales
Back to appropriate overall safety lifecycle phase	Retour à la phase appropriée du cycle de vie de sécurité générale
NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.	NOTE 1 Les activités relatives à la vérification, à la gestion de la sécurité fonctionnelle et à l'évaluation de la sécurité fonctionnelle ne sont pas affichées pour plus de clarté, mais elles sont relatives à toutes les phases du cycle de vie de sécurité global du logiciel et du système électrique/électronique/électronique programmable.
NOTE 2 The phases represented by box 11 is outside the scope of this standard.	NOTE 2 Les phases représentées dans la case 11 ne relèvent pas du domaine d'application de la présente norme.
NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 10 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.	NOTE 3 La CEI 61508-2 et la CEI 61508-3 concernent la case 10 (réalisation) mais également, le cas échéant, les aspects électroniques programmables (matériel et logiciel) des cases 13, 14 et 15.
NOTE 4 See IEC 61508-1, Table 1 for a description of the objectives and scope of the phases represented by each box.	NOTE 4 Pour obtenir une description des objectifs et du domaine d'application des phases représentées dans chaque case, voir la CEI 61508-1, Tableau 1.
NOTE 5 The technical requirements necessary for the overall operation, maintenance, repair Modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.	NOTE 5 Les exigences techniques relatives aux activités générales de fonctionnement, de maintenance, de réparation, de modification, d'amélioration, de mise hors service ou de destruction seront spécifiées dans la documentation du fournisseur du système électrique/électronique/électronique programmable relatif à la sécurité et de ses éléments et composants.

Figure 1 – FS-PLC dans l'ensemble des phases du cycle de vie de sécurité d'un système électrique/électronique/électronique programmable relatif à la sécurité

Les domaines inclus dans cette partie sont la gestion du cycle de vie de sécurité du FS-PLC, l'allocation des exigences de sécurité fonctionnelle et la planification du développement; avec un intérêt tout particulier pour la phase Réalisation (case 10) du cycle de vie de sécurité global, présenté dans la Figure 1. Cette partie suppose que le FS-PLC est utilisé en tant que sous-système logique pour l'ensemble du système électrique/électronique/électronique programmable.

La Figure 1, Réalisation (case 10), inclut:

- l'attribution des aspects sécuritaires du FS-PLC au matériel, au logiciel ou au microprogramme, ou toute autre combinaison du FS-PLC,
- les architectures matérielles du FS-PLC,
- les activités de vérification et de validation au niveau du FS-PLC,

- les exigences de modification du FS-PLC,
- les informations sur le fonctionnement et la maintenance pour l'utilisateur du FS-PLC,
- les informations fournies par le fabricant du FS-PLC pour l'utilisateur.

AUTOMATES PROGRAMMABLES –

Partie 6: Sécurité fonctionnelle

1 Domaine d'application

Cette partie de la série CEI 61131 spécifie les exigences pour les automates programmables (PLC) et leurs périphériques associés, comme défini dans la Partie 1, visant à être utilisés comme sous-système logique d'un système électrique/électronique/électronique programmable relatif à la sécurité. Un automate programmable et ses périphériques associés, conformes aux exigences de cette partie, sont considérés comme appropriés dans un système électrique/électronique/électronique programmable relatif à la sécurité et sont identifiés comme un automate programmable de sécurité fonctionnelle (FS-PLC). Un FS-PLC est généralement un sous-système matériel ou logiciel. Un FS-PLC peut également inclure des éléments logiciels, par exemple des blocs fonctionnels prédéfinis.

En général, un système électrique/électronique/électronique programmable relatif à la sécurité est constitué de capteurs, d'actionneurs, d'un logiciel et d'un sous-système logique. Cette partie est une implémentation spécifique pour les produits des exigences de la série CEI 61508 et la conformité à cette partie remplit toutes les exigences applicables de la série CEI 61508 relative aux FS-PLC. Bien que la série CEI 61508 soit une norme système, cette partie fournit des exigences spécifiques aux produits pour l'application des principes de la série CEI 61508 relative aux FS-PLC.

Cette partie de la série CEI 61131 traite uniquement de la sécurité fonctionnelle et des exigences d'intégrité de sécurité d'un FS-PLC lorsqu'il est utilisé comme partie d'un système électrique/électronique/électronique programmable relatif à la sécurité. La définition des exigences de sécurité fonctionnelle de l'ensemble du système électrique/électronique/électronique programmable relatif à la sécurité et la définition des exigences de sécurité fonctionnelle de l'utilisation finale dans une application du système électrique/électronique/électronique programmable relatif à la sécurité n'entre pas dans le cadre de cette partie, mais elles sont des données à prendre en compte pour cette partie. Pour les informations spécifiques aux applications, le lecteur est renvoyé à des références de normes telles que la série CEI 61511, la CEI 62061 et la série ISO 13849.

Cette partie ne couvre pas les exigences de sécurité générale pour un FS-PLC telles que les exigences relatives aux chocs électriques et aux dangers liés aux incendies spécifiés dans la CEI 61131-2.

Cette partie s'applique à un FS-PLC ayant un niveau d'intégrité de sécurité (SIL) inférieur ou égal à SIL 3.

L'objectif de cette partie est:

- d'établir et de décrire les éléments du cycle de vie de sécurité d'un FS-PLC, conformément au cycle de vie général de sécurité identifié dans les CEI 61508-1, -2 et -3;
- d'établir et de décrire les exigences pour le matériel et les logiciels des FS-PLC relatifs à la sécurité fonctionnelle et aux exigences d'intégrité de sécurité d'un système électrique/électronique/électronique programmable relatif à la sécurité;
- d'établir des méthodes d'évaluation pour un FS-PLC dans cette partie pour les paramètres/critères suivants:
  - une déclaration de niveau d'intégrité de sécurité (SIL) pour laquelle le FS-PLC est compétent,
  - une valeur de probabilité de défaillance à la demande (PFD),

  - une valeur de fréquence moyenne de défaillance dangereuse par heure (PFH),
  - une valeur pour la fraction de défaillance en sécurité (SFF),
  - une valeur pour la tolérance aux pannes matérielles (HFT),
  - une valeur de couverture de diagnostic (DC),
  - la vérification que les processus de cycle de vie de sécurité spécifiés par le fabricant de FS-PLC sont en place,
  - l'état de sécurité défini,
  - les mesures et techniques pour la prévention et le contrôle des pannes systématiques, et
  - pour chaque mode de défaillance traité dans cette partie, le comportement fonctionnel de l'état de panne;
- d'établir les définitions et d'identifier les principales caractéristiques pour la sélection et l'application des FS-PLC et leurs périphériques associés.

Cette partie est principalement destinée aux fabricants de FS-PLC. Elle inclut également le rôle essentiel des utilisateurs de FS-PLC via les exigences de la documentation utilisateur. Certaines instructions utilisateur concernant les FS-PLC peuvent se trouver dans la CEI 61131-4.

Les exigences du Guide ISO/CEI 51 et du Guide CEI 104 relatives à cette partie sont intégrées ci-dessous.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60947-5-1:2003, *Appareillage à basse tension – Partie 5-1: Appareils et éléments de commutation pour circuits de commande – Appareils électromécaniques pour circuits de commande*

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

CEI 61000-4-2:2008, *Compatibilité électromagnétique (CEM) – Partie 4-2: Techniques d'essai et de mesure – Essai d'immunité aux décharges électrostatiques*

CEI 61000-4-3:2006, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques*

CEI 61000-4-4:2012, *Compatibilité électromagnétique (CEM) – Partie 4-4: Techniques d'essai et de mesure – Essai d'immunité aux transitoires électriques rapides en salves*

CEI 61000-4-5:2005, *Compatibilité électromagnétique (CEM) – Partie 4-5: Techniques d'essai et de mesure – Essai d'immunité aux ondes de choc*

CEI 61000-4-6:2008, *Compatibilité électromagnétique (CEM) – Partie 4-6: Techniques d'essai et de mesure – Immunité aux perturbations conduites, induites par les champs radioélectriques*

CEI 61000-4-8:2009, *Compatibilité électromagnétique (CEM) – Partie 4-8: Techniques d'essai et de mesure – Essai d'immunité au champ magnétique à la fréquence du réseau*

CEI 61131-1:2003, *Automates programmables – Partie 1: Informations générales*

CEI 61131-2:2007, *Automates programmables – Partie 2: Exigences et essais des équipements*

CEI 61131-4:2004, *Programmable controllers – Part 4: User guidelines* (disponible en anglais seulement)

CEI 61326-3-1:2008, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

CEI 61326-3-2:2008, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

CEI 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

CEI 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61784-3:2010, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

CEI 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

Guide CEI 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications* (disponible en anglais seulement)

Guide ISO/CEI 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

EN 50205:2002, *Relais de tout ou rien à contacts guidés (liés)*