IEC 61557-15

Edition 1.0 2014-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Electrical safety in low voltage distribution systems up to 1 000 V a.c. and 1 500 V d.c. – Equipment for testing, measuring or monitoring of protective measures –
Part 15: Functional safety requirements for insulation monitoring devices in IT systems and equipment for insulation fault location in IT systems

Sécurité électrique dans les réseaux de distribution basse tension de 1 000 V c.a. et 1 500 V c.c. – Dispositifs de contrôle, de mesure ou de surveillance de mesures de protection –
Partie 15: Exigences de sécurité fonctionnelle pour les contrôleurs d'isolement de réseaux IT et les dispositifs de localisation de défauts d'isolement pour réseaux IT

IEC 61557-15:2014-02(EN-FR)

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

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

IEC 61557-15

Edition 1.0 2014-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Electrical safety in low voltage distribution systems up to 1 000 V a.c. and 1 500 V d.c. – Equipment for testing, measuring or monitoring of protective measures –
Part 15: Functional safety requirements for insulation monitoring devices in IT systems and equipment for insulation fault location in IT systems

Sécurité électrique dans les réseaux de distribution basse tension de 1 000 V c.a. et 1 500 V c.c. – Dispositifs de contrôle, de mesure ou de surveillance de mesures de protection –
Partie 15: Exigences de sécurité fonctionnelle pour les contrôleurs d'isolement de réseaux IT et les dispositifs de localisation de défauts d'isolement pour réseaux IT

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XC

ICS 17.220.20, 29.080.01, 29.240.01

ISBN 978-2-8322-1406-0

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 10
2 Normative references 10
3 Terms, definitions and abbreviations 11
3.1 Terms and definitions 11
3.2 Abbreviations 22
4 Definition of safety functions embedded in IMDs and IFLSs 23
4.1 General 23
4.2 Definition of safety functions 23
4.2.1 Local insulation warning (LIW) 23
4.2.2 Remote insulation warning (RIW) 24
4.2.3 Local location warning (LLW) 24
4.2.4 Remote location warning (RLW) 24
4.2.5 Remote enabling / disabling command (REDC) 25
4.2.6 Local transformer monitoring warning (LTMW) 25
5 Requirements on products implementing safety-related functions 25
5.1 Requirement on non-safety-related functions 25
5.2 Additional performance requirements for products implementing safety functions 26
5.2.1 General 26
5.2.2 Additional performance requirements for IMDs complying with SIL 1 or SIL 2 26
5.2.3 Additional performance requirements for IFLSs complying with SIL 1 or SIL 2 26
6 Management of functional safety during the development lifecycle 26
6.1 Management of functional safety for the IT system 26
6.2 Use of IMDs and IFLSs in IT systems 27
6.3 Safety lifecycle of IMDs and IFLSs in the realisation phase 27
7 Management of functional safety during the realisation lifecycle of IMDs and IFLSs 28
7.1 General 28
7.2 IMD and IFL design requirement specification (phase 10.1) 29
7.2.1 Specification of functional safety requirements 29
7.2.2 Provisions for the development of safety functions 29
7.2.3 Verification plan for the development of safety functions 30
7.2.4 Validation plan for the development of safety functions 30
7.2.5 Planning of commissioning, installation and setting into operation 30
7.2.6 Planning of user documentation 31
7.3 IMD and IFLS safety validation planning (phase 10.2) 31
7.3.1 General 31
7.3.2 Functional safety plan 31
7.4 IMD and IFLS design and development (phase 10.3) 32
7.4.1 General 32
7.4.2 Design standards 32
7.4.3 Realization 32

7.4.4 Safety integrity and fault detection 32
7.4.5 Safety integrity level (SIL) assignment 33
7.4.6 Hardware requirements 33
7.4.7 Software requirements 33
7.4.8 Review of requirements 33
7.4.9 Requirements for the probability of dangerous failure on demand (PFD) 34
7.4.10 Failure rate data 35
7.4.11 Diagnostic test interval 35
7.4.12 Architectural constraints 35
7.4.13 Estimation of safe failure fraction (SFF) 37
7.4.14 Requirements for systematic safety integrity 37
7.5 IMD and IFLS integration (phase 10.4) 40
7.5.1 Hardware integration 40
7.5.2 Software integration 40
7.5.3 Modifications during integration 40
7.5.4 Integration tests 40
7.6 IMD and IFLS documentation related to installation, commissioning, operation and maintenance procedures (phase 10.5) 41
7.6.1 General 41
7.6.2 Functional specification 41
7.6.3 Compliance information 41
7.6.4 Information for commissioning, installation, setting into operation, operation and maintenance 41
7.7 IMD and IFLS safety validation (phase 10.6) 42
7.7.1 General 42
7.7.2 Test 42
7.7.3 Verification 42
7.7.4 Validation 43
7.7.5 EMC requirements 43
8 Requirements for modifications 44
8.1 General 44
8.2 Modification request 44
8.3 Impact analysis 44
8.4 Authorization 44
9 Proven in use approach 44
Annex A (informative) Risk analysis and SIL assignment for IMDs and IFLSs 45
A.1 General 45
A.2 SIL assignment for IMDs and IFLSs 47
A.3 Example of risk graph 48
A.4 Alternative method of SIL assignment – quantitative method 49
Annex B (informative) Examples for the determination of PFD, DC and SFF 50
B.1 General 50
B.2 Examples of IMD and IFLS architectures 51
Annex C (informative) Failure rate databases 52
C.1 General 52
C.2 Failure rate references in current standards 52
Annex D (informative) Guide to embedded software design and development 53
D.1 General 53

D.2 Software element guidelines 53
D.2.1 General 53
D.2.2 Interface with system architecture 53
D.2.3 Software specifications 53
D.2.4 Pre-existent software 54
D.2.5 Software design 55
D.2.6 Coding 55
D.3 Software development process guidelines 55
D.3.1 Development process: software lifecycle 55
D.3.2 Documentation: documentation management 55
D.3.3 Configuration and software modification management 56
D.3.4 Configuration and archiving management 56
D.3.5 Software modifications management 57
D.4 Development tools 57
D.5 Reproduction of executable code production 57
D.6 Software verification and validation 57
D.7 General verification and validation guidelines 57
D.8 Verification and validation review 58
D.9 Software testing 58
D.9.1 General validation 58
D.9.2 Software specification verification: validation tests 59
D.9.3 Software design verification: software integration tests 59
D.9.4 Detailed design verification: module tests 60
Annex E (informative) Information for the assessment of safety functions 61
E.1 General 61
E.2 Documentation management 61
E.3 Documentation provided for conformity assessment 61
E.4 Documentation of the development lifecycle 63
E.5 Design documentation 63
E.6 Documentation of verification and validation 63
E.7 Test documentation 63
E.8 Documentation of modifications 63
E.9 Information for use 63
Annex F (informative) Example of applications 64
F.1 Overview 64
F.2 Limitation in applications 64
F.3 Typical applications covered by IEC 61557-15 64
F.3.1 General 64
F.3.2 Local alarming 64
F.3.3 Local transformer monitoring warning 65
F.3.4 Alarming and processing of remote insulation warning and/or remote location warning 66
F.3.5 Automatic disconnection of the complete IT system in case of a first insulation fault 67
F.3.6 Automatic disconnection of an IT system sub-network 69
F.3.7 Management of multiple source system (two incomers or of incomer plus generator) 71
F.3.8 Management of multiple source systems (two incomers or of incomer plus generator – with a load shedder) 72
Bibliography 74

Figure 1 – Relationship between IEC 61557-15 and related standards 8
Figure 2 – Overall safety lifecycle applicable to an IT system 27
Figure 3 – IMD and IFLS safety lifecycle (in realisation phase) 28
Figure A.1 – Functional elements of an IT system and their relationship to the definitions and abbreviations of the IEC 61508 series 45
Figure A.2 – SIL assignment for IMDs and IFLSs 47
Figure A.2 – Example of risk graph 48
Figure B.1 – Flowchart for PFD, DC, SFF determination 51
Figure F.1 – Local alarming, based on the systematic presence of one person and based on a well-defined alarming management process 65
Figure F.2 – Local transformer monitoring warning, based on the systematic presence of a skilled person, and based on a well-defined alarming management process 66
Figure F.3 – Alarming and processing of the remote insulation warning and/or the remote location warning in a supervisory control system 67
Figure F.4 – Disconnection of the complete IT system in case of insulation fault detection 68
Figure F.5 – Threshold 1 warning information and threshold 2 disconnection of the complete IT system in case of an insulation fault detection 69
Figure F.6 – Automatic disconnection of a faulty feeder via direct signal from the IFLS 70
Figure F.7 – Automatic disconnection of a faulty feeder via a PLC 71
Figure F.8 – Management of multiple source systems (two incomers or of one incomer plus generator) 72
Figure F.9 – Management of multiple source system (two incomers or of one incomer plus generator, with a load shedder) 73

Table 1 – Abbreviations with reference 22
Table 2 – Safety integrity levels (SIL) and probability of a dangerous failure on demand (PFD) of IMDs and IFLSs 29
Table 3 – Hardware safety integrity: architectural constraints on type A and type B safety-related subsystems 37
Table A.1 – IT system risk analysis 46
Table A.3 – Link between minimum risk reduction and SIL 48
Table A.4 – Example of classifications according to risk graph Figure A.1 49
Table E.1 – Documentation to be provided 62

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ELECTRICAL SAFETY IN LOW VOLTAGE DISTRIBUTION SYSTEMS UP TO 1 000 V AC AND 1 500 V DC – EQUIPMENT FOR TESTING, MEASURING OR MONITORING OF PROTECTIVE MEASURES –

Part 15: Functional safety requirements for insulation monitoring devices in IT systems and equipment for insulation fault location in IT systems

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 61557-15 has been prepared by IEC technical committee 85: Measuring equipment for electrical and electromagnetic quantities.

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

FDIS	Report on voting
85/465/FDIS	85/470/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.

This part of IEC 61557 is to be used in conjunction with Part 8 and Part 9.

A list of all parts of the IEC 61557 series, published under the general title *Electrical safety in low voltage distribution systems up to 1 000 V a.c. and 1 500 V d.c. – Equipment for testing, measuring or monitoring of protective measures*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC 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

IEC 61508 deals with functional safety, this topic being of upmost importance for safety related systems. Functional safety may be applicable to IT systems where safety is based on insulation monitoring devices (IMD) and insulation fault location systems (IFLS), and also on additional safety related measures (e.g. circuit-breakers).

Insulation monitoring devices and insulation fault location systems comprise electrical and electronic components and can comprise embedded software.

Product requirements for these devices are defined in IEC 61557-8 and IEC 61557-9. These standards include elementary requirements which need to be taken into account for the functional safety approach according to IEC 61557-15, but do not cover the whole range of requirements which shall be fulfilled for the assignment of a defined level of functional safety and for the respective validation.

IEC 61508 series covers basic aspects to be considered when electrical and electronic systems are used to carry out safety functions. One of the major objectives of this series of standards is to facilitate the development of international application or equipment standards by the responsible technical committee. This will allow the technical committee to take the special requirements of their application fully into account.

It is recognized that there is a great variety of applications of insulation monitoring devices and of insulation fault location systems in IT systems. This part of IEC 61557 defines basic safety functions as well as their related levels of functional safety (SIL) and defines feasible measures and principles to develop and validate these devices and systems under functional safety aspects.

Figure 1 shows the link between IEC 61557-15 and the relevant product, safety and EMC standards as well as the link to the IEC 61508 series.

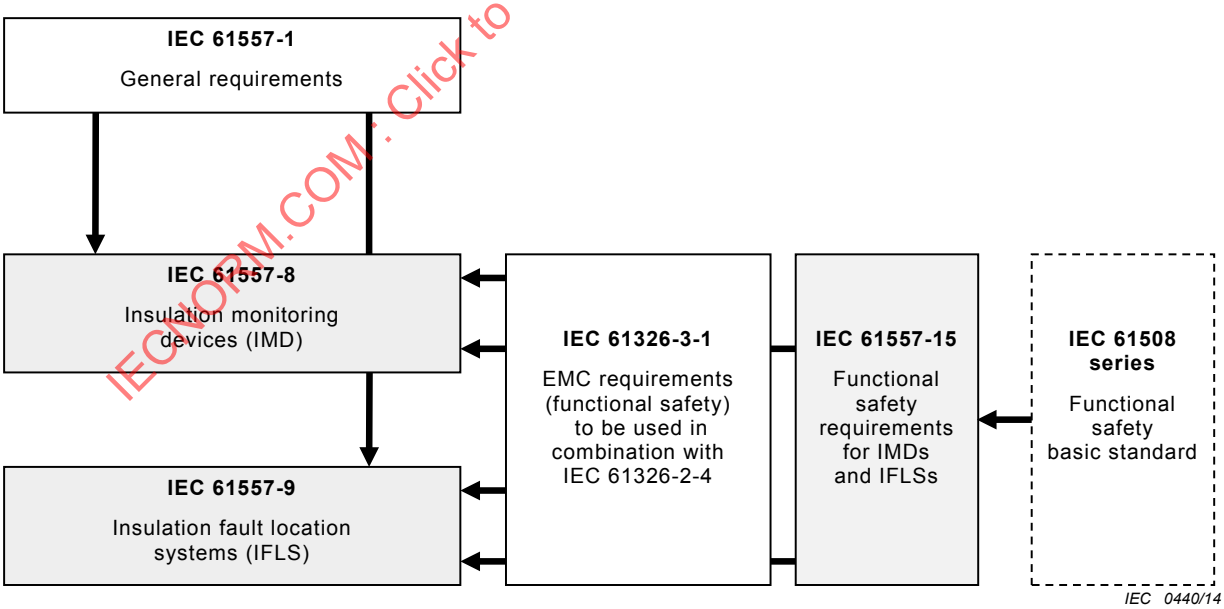


Figure 1 – Relationship between IEC 61557-15 and related standards

This part of IEC 61557 does not cover phases 1 to 9 and 11 to 16 of IEC 61508-1 for the complete IT systems. In particular, this standard does not cover the use of IMDs and IFLSs in customer application.

NOTE 1 An insulation fault location system (IFLS) can consist of several devices according to IEC 61557-9: insulation fault locator (IFL), locating current injector (LCI), locating current sensor (LCS), insulation monitoring device (IMD) according to IEC 61557-8.

IMDs and IFLSs are not protective devices in general, but they are part of the protective measures in IT systems. IMDs and IFLSs function as permanent monitoring of the insulation resistance of the unearthed IT system and the localization of insulation faults in any part of the system can be seen as safety functions which are part of the protective measures in an IT system.

This part of IEC 61557 only applies to IMDs and IFLSs implementing SIL 1 and SIL 2 related safety functions. Higher SIL levels are not specified in this standard because those levels are generally not required for IMDs and IFLSs in IT systems.

Conformance to this standard may be required for IMDs or IFLSs when functional safety is requested in the respective application within IT systems. However, it does not generally dictate that for these devices, a defined level of functional safety according to this standard is required.

NOTE 2 Examples of applications where functional safety can be requested depending on the risk analysis are:

– chemistry,
– mines,
– marine,
– hospital,
– photovoltaic farms,
– railway signalling systems,
– control systems (e.g. in nuclear power plants),
– etc.

Examples of typical applications are provided in Annex F.

ELECTRICAL SAFETY IN LOW VOLTAGE DISTRIBUTION SYSTEMS UP TO 1 000 V AC AND 1 500 V DC – EQUIPMENT FOR TESTING, MEASURING OR MONITORING OF PROTECTIVE MEASURES –

Part 15: Functional safety requirements for insulation monitoring devices in IT systems and equipment for insulation fault location in IT systems

1 Scope

This part of IEC 61557 specifies requirements related to functional safety and is based on the IEC 61508 standard series for the realization of insulation monitoring devices (IMD) as specified in IEC 61557-8 and for insulation fault location systems (IFLS) according to IEC 61557-9, according to phase 10 of the IEC 61508-1 lifecycle. These devices provide safety related functions for IT systems.

This part of IEC 61557 is:

– concerned only with functional safety requirements intended to reduce the functional risk during the use of IMDs and IFLSs;

– restricted to risks arising directly from the device itself or from several IMDs or IFLSs working together in a system;

– intended to define the basic safety functions provided by the devices.

This part of IEC 61557 does not:

– deal with electrical safety according to IEC 61010-1 and the requirements of IEC 61557-8 and IEC 61557-9;

– cover the hazard and risk analysis of a particular use of the IMD or IFLS;

– identify all the safety functions for the application in which the IMD or IFLS is used;

– cover the IMD or IFLS manufacturing process.

Functional safety requirements depend on the application and should be considered as part of the overall risk assessment of the specific application. The supplier of IMDs and IFLSs is not responsible for the application. The application designer is responsible for the risk assessment and for specifying the overall functional safety requirements of the complete IT system and he should select the functional safety level (SIL) of the IMD and/or IFLS when their safety function is part of the functional safety assessment in the IT system.

2 Normative references

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

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

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

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

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 61508-6:2010, *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 61557-1, *Electrical safety in low voltage distribution systems up to 1 000 V a.c. and 1 500 V d.c. – Equipment for testing, measuring or monitoring of protective measures – Part 1: General requirements*

IEC 61557-8, *Electrical safety in low voltage distribution systems up to 1 000 V a.c. and 1 500 V d.c. – Equipment for testing, measuring or monitoring of protective measures – Part 8: Insulation monitoring devices for IT systems*

IEC 61557-9:2009, *Electrical safety in low voltage distribution systems up to 1 000 V a.c. and 1 500 V d.c. – Equipment for testing, measuring or monitoring of protective measures – Part 9: Equipment for insulation fault location in IT systems*

IEC 61326-2-4:2012, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 2-4: Particular requirements – Test configurations, operational conditions and performance criteria for insulation monitoring devices according to IEC 61557-8 and for equipment for insulation fault location according to IEC 61557-9*

IEC 61326-3-1:2008, *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*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the definitions given in IEC 61557-1, IEC 61557-8 and IEC 61557-9 and the following apply.

3.1.1
hazard
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: ISO/IEC Guide 51:1999, 3.5, modified – The note has been adapted.]

3.1.2
electrical hazard
potential source of harm when electric energy is present in an electrical installation or equipment

[SOURCE: IEC 60050-651:1999, 651-01-30, modified – The note has been deleted.]

3.1.3
hazardous situation
circumstance in which people, property or the environment are exposed to one or more hazards

[SOURCE: IEC 61508-4:2010, 3.1.3]

3.1.4
hazardous event
event that may result in harm

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the consequence of the hazardous event and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

[SOURCE: IEC 61508-4:2010, 3.1.4]

3.1.5
harmful event
occurrence in which a hazardous situation or hazardous event results in harm

Note 1 to entry: Adapted from ISO/IEC Guide 51:1999, 3.4, to allow for a hazardous event.

[SOURCE: IEC 61508-4:2010, 3.1.5]

3.1.6
risk
combination of the probability of occurrence of harm and the severity of that harm

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

3.1.7
tolerable risk
risk which is accepted in a given context based on the current values of society

Note 1 to entry: Tolerable risk is achieved by the iterative process of risk assessment (risk analysis and risk evaluation) and risk reduction.

[SOURCE: ISO/IEC Guide 51:1999, 3.7, modified – Note 1 to entry has been added.]

3.1.8
residual risk
risk remaining after protective measures have been taken

[SOURCE: ISO/IEC Guide 51:1999, 3.9]

3.1.9
safety
freedom from unacceptable risk

[SOURCE: ISO/IEC Guide 51:1999, 3.1, modified – The note has been deleted.]

3.1.10
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 system and other risk reduction measures

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

3.1.11
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]

3.1.12
reasonable foreseeable misuse
use of a product, process or service in a way not intended by the supplier, but which may result from readily predictable human behaviour

[SOURCE: ISO/IEC Guide 51:1999, 3.14]

3.1.13
environment
all relevant parameters that can affect the achievement of functional safety in the specific application under consideration and in any safety lifecycle phase

Note 1 to entry: This would include, for example, physical environment, operating environment, legal environment and maintenance environment.

[SOURCE: IEC 61508-4:2010, 3.2.2]

3.1.14
fault
abnormal condition that may cause a reduction in, or a loss of, the capability of a functional unit to perform a required function

[SOURCE: IEC 61508-4:2010, 3.6.1; based on ISO/IEC 2382-14:1997, 14-01-10]

3.1.15
fault avoidance
use of techniques and procedures that aim to avoid the introduction of faults during any phase of the safety lifecycle of the safety related system

[SOURCE: IEC 61508-4:2010, 3.6.2]

3.1.16
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

Note 1 to entry: The definition in IEC 60050-191-15-05 refers only to sub-item faults (the attribute of an item that makes it able to perform a required function in the presence of certain given sub-item faults).

[SOURCE: IEC 61508-4:2010, 3.6.3, modified – The note has been adapted; based ISO/IEC 2382-14:1997, 14-01-10]

3.1.17
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 60050-191-04-01 with changes to include systematic failures due to, for example, deficiencies in specification or software.

Note 2 to entry: See Figure 4 of IEC 61508-4:2010 for the relationship between faults and failures, both in the IEC 61508 series and IEC 60050-191.

Note 3 to entry: Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

Note 4 to entry: Failures are either random (in hardware) or systematic (in hardware or software).

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – Figure 4 has been deleted.]

3.1.18
safety lifecycle
necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety related system are no longer available for use

[SOURCE: IEC 61508-4:2010, 3.7.1, modified – Notes 1 and 2 have been deleted.]

3.1.19
proven in use
demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required safety integrity level

[SOURCE: IEC 61508-4:2010, 3.8.18]

3.1.20
safety integrity level
SIL
discrete level (one out of a possible two), corresponding to a range of safety integrity values, for specifying the safety integrity requirements of a safety function allocated (in whole or in part) to an IMD or IFLS

Note 1 to entry: SIL 2 has the highest level of safety integrity and SIL 1 has the lowest according to this standard.

Note 2 to entry: SIL 3 and SIL 4 are not considered in this standard as it is not relevant to the risk reduction requirements normally associated with IMDs and IFLSs. For applicable requirements to SIL 3 and SIL 4 see IEC 61508.

[SOURCE: IEC 61508-4:2010, 3.5.8, modified – Note 3 has been deleted.]

3.1.21
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

EXAMPLE: Examples of safety functions include:

– functions that are required to be carried out as positive actions to avoid hazardous situations (for example switching off a motor); and

– functions that prevent actions being taken (for example preventing a motor starting).

[SOURCE: IEC 61508-4:2010, 3.5.1]

3.1.22
dangerous failure
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]

3.1.23
safe failure
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]

3.1.24
diagnostic coverage
DC
fraction of dangerous failures detected by automatic on-line diagnostic tests

Note 1 to entry: The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures.

Note 2 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 $\lambda_{D\ total}$ is the total dangerous failure rate:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{D\ total}}$$

Note 3 to entry: This definition is applicable providing the individual components have constant failure rates.

[SOURCE: IEC 61508-4:2010, 3.8.6, modified – Part of the definition has been moved into Note 1 to entry and the other notes have been renumbered accordingly.]

3.1.25
diagnostic test(s)
test(s) intended to detect faults or failures and to produce a specified output information or activity when a fault or failure is detected

Note 1 to entry: Diagnostic tests can be carried out by manual activation of the tests or by automatic self-test of the devices.

[SOURCE: IEC 61800-5-2:2007, 3.4, modified – Note 1 to entry has been added.]

3.1.26
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: In this standard there are three validation phases:

– overall safety validation (see Figure 2 of IEC 61508-1:2010);

– E/E/PE system validation (see Figure 3 of IEC 61508-1:2010);

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

Note 2 to entry: Validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the 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 safety requirements specification.

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

3.1.27
verification
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: In the context of this standard, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall E/E/PE system and software)), 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]

3.1.28
insulation monitoring device
IMD
device which permanently monitors the insulation resistance to earth of unearthed IT a.c. systems, IT a.c. systems with galvanically connected d.c. circuits having nominal voltages up to 1 000 V a.c., as well as monitoring the insulation resistance of unearthed IT d.c. systems with voltages up to 1 500 V d.c., independent from the method of measuring

[SOURCE: IEC 61557-8:2007, Clause 1, modified – The scope has been adapted to form of a definition.]

3.1.29
insulation fault location system
IFLS
device or combination of devices used for insulation fault location in IT systems

Note 1 to entry: The insulation fault location system is used in addition to an insulation monitoring device. It injects a locating current between the electrical system and earth and locates insulation faults

[SOURCE: IEC 61557-9:2009, 3.1, modified – Part of the definition has been moved into Note 1 to entry.]

3.1.30
equipment under control
EUC
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities;, whose power supply system is an IT system such as described in IEC 60364-4-41

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

Note 2 to entry: In IEC 61557-15 EUC is the IT system in which the IMD or IFLS is installed.

[SOURCE: IEC 61508-4:2010, 3.2.1 modified – Notes 1 and 2 to entry have been added.]

3.1.31
safety-related system
SRS
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 detection of a condition which may lead to a hazardous event. 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 be designed to:

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

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

c) achieve a combination of a) and b).

Note 5 to entry: A person can be part of a safety-related system. 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]

3.1.32
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 a 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/PE 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]

3.1.33
safety integrity
probability of an IMD or IFLS 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: In IEC 61508 there are four levels of safety integrity (SIL). For IMDs and IFLSs only SIL 1 and SIL 2 are specified.

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 and systematic safety integrity.

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

[SOURCE: IEC 61508-4:2010, 3.5.4, modified – Replaced "E/E/PE safety-related system" by "IMD or IFLS".]

3.1.34
development lifecycle
way in which the following safety-related activities of IMD and IFLS development are included:

– the definition of safety functions
– planning of functional safety
– design and development
– integration and testing
– documentation
– organization of modifications
– verification
– validation

3.1.35
mode of operation
way in which a safety function operates

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – Low demand mode, high demand mode and continuous mode have been separated into new definitions.]

3.1.35.1

low demand mode
mode of operation which 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

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).

3.1.35.2

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

3.1.35.3

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

3.1.36
systematic faults
faults which can appear in the different phases of the lifecycle, including:

– specification errors,
– design and development errors,
– integration errors,
– errors at verification or validation,
– errors in the documentation and
– errors at installation and use

3.1.37
additional functions
functions in a safety related IMD or IFLS which are not designated as safety function

3.1.38
systematic safety integrity
part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure

Note 1 to entry: Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

[SOURCE: IEC 61508-4:2010, 3.5.6]

3.1.39
common cause failure
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]

3.1.40
diagnostic test interval
interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage

[SOURCE: IEC 61508-4:2010, 3.8.7]

3.1.41
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:

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

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

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

[SOURCE: IEC 61508-4:2010, 3.6.15, modified – Part of the definition has been moved into Note 1 to entry.]

3.1.42
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]

3.1.43
MooN architecture
architecture made up of a number (M) of independent channels, any of which (N) are sufficient to perform the correct safety function

3.1.44
MooND architecture
architecture made up of a number (M) of independent channels, any of which (N) are sufficient to perform the correct safety function plus diagnostics (D)

3.1.45
dangerous failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

– 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
– decreases the probability that the safety function operates correctly when required.

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

3.1.46
safe failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

– 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
– 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]

3.1.47
dependent failure
failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events that caused it

Note 1 to entry: Two events A and B are dependent, only if: P (A and B) > P (A) × P (B).

[SOURCE: IEC 61508-4:2010, 3.6.9]

3.1.48
end of life
EOL
life cycle stage of a product starting when it is finally removed from its intended use-phase

[SOURCE: IEC Guide 109:2012, 3.1]

3.1.49
mean time to failure
MTTF
expectation of the time to failure

[SOURCE: IEC 60050-191:1990, 191-12-07]

3.1.50
insulation fault
defect in the insulation of an electric installation or equipment that can result either in an abnormal current through this insulation or in a disruptive discharge

[SOURCE: IEC 60050-604:1987, 604-02-02, modified – Added "electric installation".]

3.1.50.1
symmetrical insulation fault
defect in the insulation of an electric installation or equipment creating a resistive path to earth having approximately the same resistance from all phase conductors to earth

3.1.50.2
asymmetrical insulation fault
defect in the insulation of an electric installation or equipment creating a resistive path to earth having different resistances from the phase conductors to earth

3.1.51
insulation resistance
R_F
resistance in the system being monitored, including the resistance of all the connected appliances to earth

[SOURCE: IEC 61557-8:2007, 3.2]

3.1.52
proof 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

[SOURCE: IEC 61508-4:2010, 3.8.5, modified – The notes have been deleted.]

3.1.53
process safety time
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]

3.1.54
system leakage capacitance
C_e
maximum permissible value of the total capacitance to earth of the system to be monitored, including any connected appliances, up to which value the insulation monitoring device can work as specified

[SOURCE: IEC 61557-8:2007, 3.6]

3.1.55
electrical/electronic/programmable electronic
E/E/PE
based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

Note 1 to entry: In IEC 61557-15, IMDs and/or IFLSs are the safety related devices which are designated as E/E/PE in the IEC 61508 series.

[SOURCE: IEC 61508-4:2010, 3.2.13, modified – The note and example have been replaced by Note 1 to entry.]

3.1.56
response sensitivity
value of the evaluating current or insulation resistance at which the evaluator responds under specified conditions

[SOURCE: IEC 61557-9:2009, 3.4, modified – The note has been deleted.]

3.2 Abbreviations

For the purposes of this document, the abbreviations given in IEC 61557-1, IEC 61557-8 and IEC 61557-9 and the following as outlined in Table 1 apply.

Table 1 – Abbreviations with reference

Abbreviation	Terms	Reference
DC	Diagnostic coverage	IEC 61508-4, 3.8.6
E/E/PE	Electric, electronic, programmable electronic	IEC 61508-4, 3.2.13
EMC	Electromagnetic compatibility	IEC 61000-1-1
EOL	End of life	IEC Guide 109:2012, 3.1
EUC	Equipment under control	IEC 61508-4
FMEA	Failure mode and effect analysis	IEC 60812
IFL	Insulation fault locator	IEC 61557-9
IFLS	Insulation fault location system	3.1.29
IMD	Insulation monitoring device	3.1.28
IT (system)	I: all live parts isolated from earth (power system to earth) T: direct connection of exposed-conductive parts to earth (ground) independently of the earthing of any point of the power system	IEC 60364-1:2005, 312.2
LCI	Locating current injector	IEC 61557-9:2009, 3.7
LIW	Local Insulation warning	4.2.1
LLW	Local location warning	4.2.3
LTMW	Local transformer monitoring warning	4.2.6
MooN	Number (M) out of (N) independent channels	IEC 61508-4:2010, Table 1
MooND	Number (M) out of (N) independent channels with diagnostics (D)	IEC 61508-4:2010, Table 1

Abbreviation	Terms	Reference
MTTF	Mean time to failure	IEC 60050,191-12-07
MTTR	Mean time to restoration	IEC 61508-4:2010, 3.6.21
PFD	Probability of dangerous failure on demand	IEC 61508-4:2010, 3.6.17
PFH	Probability of dangerous failure per hour	IEC 61508-4:2010, 3.6.19
REDC	Remote enabling / disabling command	4.2.5
RIW	Remote insulation warning	4.2.2
RLW	Remote Location warning	4.2.4
SFF	Safe failure fraction	IEC 61508-4:2010, 3.6.15
SIL	Safety integrity level	IEC 61508-4:2010, 3.5.8
SRS	Safety related system	IEC 61508-4:2010, 3.2.1

4 Definition of safety functions embedded in IMDs and IFLSs

4.1 General

Clause 4 describes functions of an IMD or IFLS that can be designated as safety function according to this standard. The safety functions in Clause 4 are considered to form an exhaustive list. Any other specific safety function, if any, shall comply with IEC 61508.

It is not mandatory to provide all these functions in an IMD or IFLS. It is generally not mandatory to assign an SIL level to these functions. However, if an SIL level is assigned to one of these functions, this function shall comply with the requirements specified in this standard.

An SIL level is assigned to a function, not to a product. As a consequence, different safety functions in an IMD or in an IFLS may have different SIL levels.

Where a safety function relies on limit values for parameters, the maximum tolerances of the limit values shall be defined.

The safety integrity level of the application depends on the correct integration of the safety function provided by the IMD or IFLS within the IT system (see user documentation in 7.2.6).

4.2 Definition of safety functions

4.2.1 Local insulation warning (LIW)

This function aims at issuing a warning signal when the insulation resistance between the system and earth falls below a predetermined level.

This function includes the measurement of the insulation resistance R_f of an IT system including symmetrical and asymmetrical insulation faults, an assessment of this resistance and a local safe warning.

The safe position shall be the warning position.

A local safe warning should be made by visual indicators and/or audible signals generated by the product implementing the function.

NOTE Usually this function is provided by the IMD.

Products claiming an SIL level with such a function shall comply with IEC 61557-8, additionally with IEC 61557-15 and, in particular with additional performance requirements defined in 5.2.

4.2.2 Remote insulation warning (RIW)

This function aims at issuing a warning output signal when the insulation resistance between the system and earth falls below a predetermined level.

This function includes the measurement of the insulation resistance of an IT system including symmetrical and asymmetrical insulation faults, an assessment of this resistance and a warning output.

The warning output shall be reported remotely with a safe output.

The safe position shall be the warning position.

NOTE 1 A relay contact output or an electronic switching output or a safe data communication can be used to report the safe warning remotely.

NOTE 2 The warning output could also be used in some applications for switching.

Products claiming an SIL level with such a function shall comply with IEC 61557-8, additionally with IEC 61557-15 and, in particular with additional performance requirements defined in 5.2.

4.2.3 Local location warning (LLW)

This functions aims at issuing a warning signal when the insulation resistance between the system and earth falls below the response sensitivity.

This function includes the localization of an insulation fault in an IT system including symmetrical and asymmetrical insulation faults, an assessment of this fault and a local safe warning.

The safe position shall be the warning position.

A local safe warning should be made by visual indicators or audible signals generated by the product implementing the function.

NOTE Usually this function is provided by the IFLS.

Products claiming an SIL level with such a function shall comply with IEC 61557-9, additionally with IEC 61557-15 and, in particular, with additional performance requirements defined in 5.2.

4.2.4 Remote location warning (RLW)

This functions aims at issuing a warning signal if the insulation resistance between the system and earth falls below the response sensitivity.

This function includes the localization of an insulation fault in an IT system including symmetrical and asymmetrical insulation faults, an assessment of this fault and a remote safe warning.

The warning output shall be reported remotely with a safe output.

The safe position shall be the warning position.

NOTE 1 A relay contact output or an electronic switching output or a safe data communication can be used to report the safe warning remotely.

NOTE 2 The warning output could also be used in some applications for switching.

Products claiming an SIL level with such a function shall comply with IEC 61557-9, additionally with IEC 61557-15 and, in particular with additional performance requirements defined in 5.2.

4.2.5 Remote enabling / disabling command (REDC)

These functions are taking into account a remote command, either to enable the measurement of the insulation resistance of an IT system or to disable this measurement.

The safe position shall be to enable the measurement of the insulation resistance of an IT system.

NOTE A relay contact output, an electronic switching output or a safe data communication can be used to provide the remote command.

Products claiming an SIL level with such a function shall comply with IEC 61557-8 or IEC 61557-9, additionally with IEC 61557-15 and, in particular with additional performance requirements defined in 5.2.

4.2.6 Local transformer monitoring warning (LTMW)

This function aims at issuing a local warning signal when the isolating transformer for IT systems is working in abnormal conditions; either the current at the secondary side of the transformer is too high or the temperature of the transformer is too high.

This function includes monitoring of the rated output current, monitoring of the temperature of the transformer, an assessment of these measurements and a local safe warning.

The safe position shall be the warning position.

A local safe warning should be made by visual indicators and/or audible signals generated by the product implementing the function.

NOTE Usually this function is provided by the IMD.

Products claiming an SIL level with such a function shall comply with IEC 61557-8 and additionally, with IEC 61557-15, in particular with the additional performance requirements defined in 5.2.

5 Requirements on products implementing safety-related functions

5.1 Requirement on non-safety-related functions

Where the IMD and IFLS include additional functions which are not designated as safety function then all of the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety functions and additional functions are sufficiently independent (i.e. that the failure of any additional function does not cause a dangerous failure of the safety functions).

NOTE 1 Sufficient independence can be established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the probability of a dangerous failure for the highest safety integrity level associated with the safety functions involved.

NOTE 2 Additional functions of the IMD and IFLS can be for example, a facility for indicating the measured insulation resistance R_f.

5.2 Additional performance requirements for products implementing safety functions

5.2.1 General

IMDs and IFLSs complying with SIL 1 or SIL 2 according to this standard shall implement the following additional performance requirements in addition to the requirements of the product standards IEC 61557-8 or IEC 61557-9.

NOTE Further specification and test of the requirements are included in IEC 61557-8 and IEC 61557-9.

5.2.2 Additional performance requirements for IMDs complying with SIL 1 or SIL 2

5.2.2.1 Performance of the IMD in case of the interruption of the connection to the system to be monitored

IMDs complying with SIL 1 or SIL 2 shall comprise an indication if the connection to the system to be monitored is lost in a manner that the monitoring function is not ensured. This function includes monitoring of the connection to the line conductors of the system to be monitored and to earth.

5.2.2.2 EMC

The safety functions of the IMD shall comply with IEC 61326-3-1 and with IEC 61326-2-4 according to 7.7.5.

5.2.3 Additional performance requirements for IFLSs complying with SIL 1 or SIL 2

5.2.3.1 Performance of the IFLS in case of the interruption of the connection to the locating current sensor

IFLSs complying with SIL 1 or SIL 2 shall comprise an indication if the connection to one or more locating current sensors is lost.

5.2.3.2 EMC

The safety functions of the IFLS shall comply with IEC 61326-3-1 and with IEC 61326-2-4 according to 7.7.5.

6 Management of functional safety during the development lifecycle

6.1 Management of functional safety for the IT system

The system integrator and the end-user are responsible for the application of IEC 61508 in the related IT system where the development life cycle defined in Figure 2 applies.

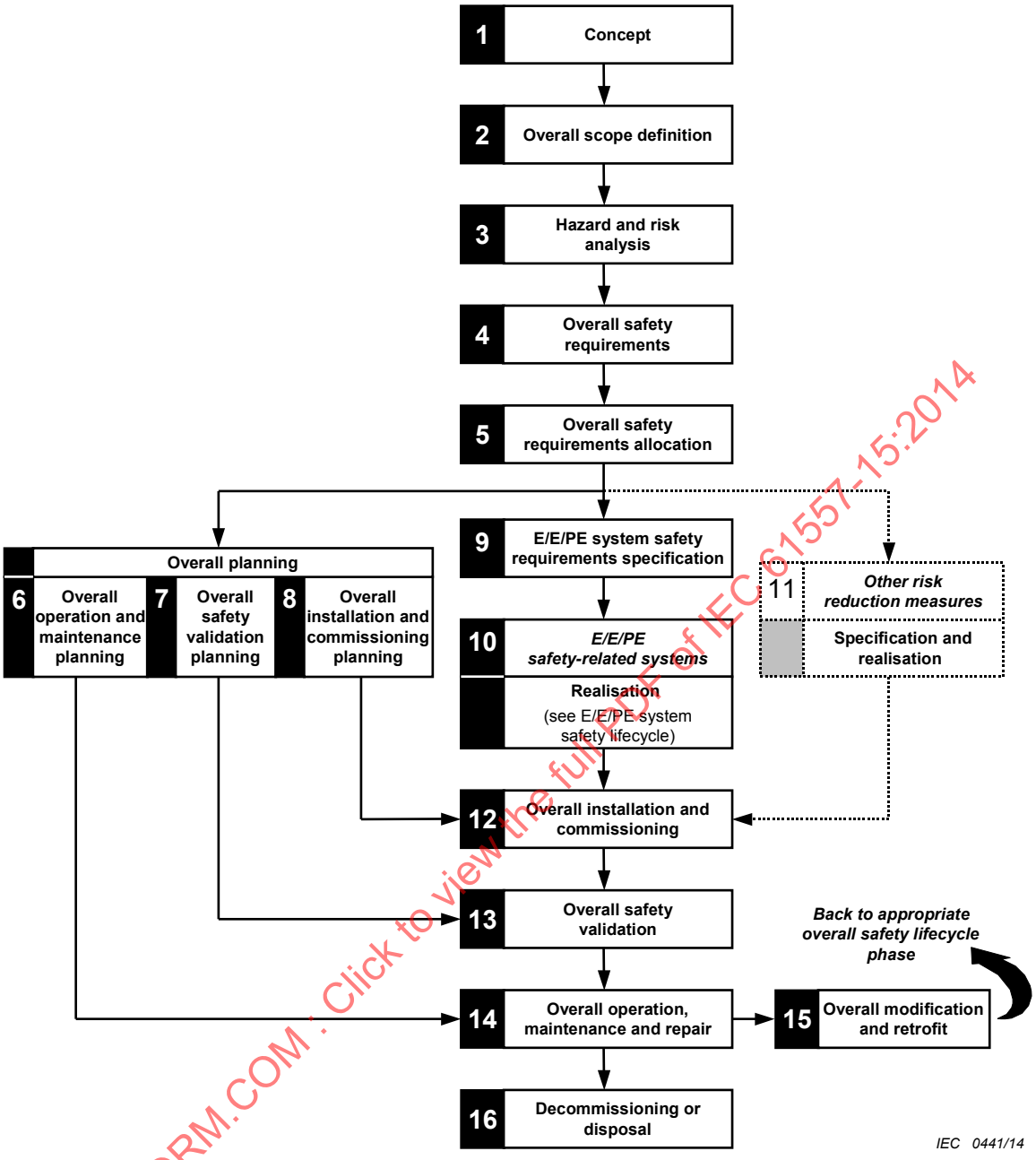


Figure 2 – Overall safety lifecycle applicable to an IT system

6.2 Use of IMDs and IFLSs in IT systems

Functional safety management objectives for IMDs and IFLSs are part of the functional safety management for the IT system where they are installed.

This standard covers, for IMDs and IFLSs only, phase 10 of the overall safety lifecycle applicable to an IT system. This standard does not cover phase 10 of the IT system realisation.

6.3 Safety lifecycle of IMDs and IFLSs in the realisation phase

IMDs and IFLSs are part of the protective measures in IT systems. This standard defines functional safety requirements for the realisation of IMDs and IFLSs according to Figure 3.

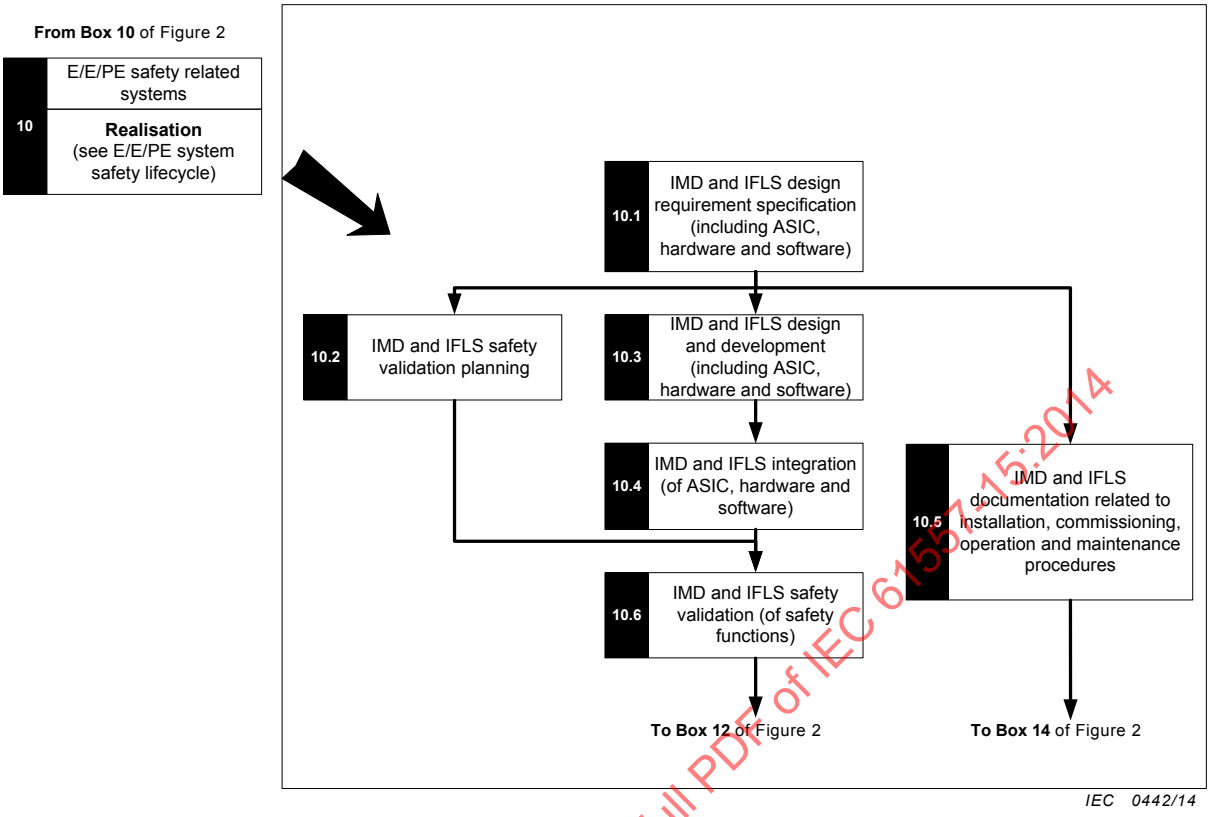


Figure 3 – IMD and IFLS safety lifecycle (in realisation phase)

7 Management of functional safety during the realisation lifecycle of IMDs and IFLSs

7.1 General

Clause 7 identifies the activities necessary for the overall realisation process of IMDs and IFLSs in order to ensure that the functional safety objectives are met. Management of functional safety is conducted during all stages of the safety lifecycle of IMDs and IFLSs. The development lifecycle is one important part of it. A functional safety plan shall be drawn up and documented for each IMD and IFLS design project.

The following general activities are included in the development lifecycle:

– planning, organizing, controlling and communicating the functional safety development process,
– ensuring competency of people for the functional safety activities,
– establishing, documenting and controlling the safety lifecycle process,
– defining and controlling the functional safety technical requirements,
– development of IMDs and IFLSs under functional safety premises,
– monitoring, reviewing and validation of the functional safety development process.

NOTE If conformity assessment according to ISO 9001 is provided, the functional safety development process can reference the appropriate quality procedures.

7.2 IMD and IFL design requirement specification (phase 10.1)

7.2.1 Specification of functional safety requirements

7.2.1.1 Specification of safety functionality requirements

Comprehensive and detailed safety functionality requirements including the safety functions shall be included in the development specification or in a separate document.

Safety functionality requirements will be determined by the risk reduction strategy as outlined in Annex A.

Specification of safety functionality requirements shall include:

– functional requirements specification:
  - the operating conditions of IMDs and IFLSs
  - a functional description of the IMDs and IFLSs
  - the required response characteristics
  - the description of the safety functions and their constraints
  - the description of fault reactions and their constraints
  - the description of the operating environment
  - tests and test conditions
– EMC requirements
– safety integrity requirements specification.

7.2.1.2 Specification of safety integrity requirements

The safety integrity requirements shall be expressed as a target value for the probability of dangerous failure on demand (PFD) of each IMD and IFLS.

IMDs and IFLSs are considered to operate in the low demand mode according to IEC 61508-2.

The safety integrity requirements shall be specified in terms of SIL in accordance with Table 2. A method of SIL assignment is given in Annex A.

Table 2 – Safety integrity levels (SIL) and probability of a dangerous failure on demand (PFD) of IMDs and IFLSs

Safety integrity level (SIL)	Probability of a dangerous failure on demand (PFD)	Risk reduction factor
1	$\geq 10^{-2}$ to 10^{-1}	>10 to ≤ 100
2	$\geq 10^{-3}$ to 10^{-2}	>100 to ≤ 1 000
For IMDs and IFLSs only safety integrity levels of 1 and 2 are assumed in this standard.		

7.2.2 Provisions for the development of safety functions

IMDs and IFLSs shall be developed to meet the requirements of the functional safety plan according to 7.3.2 and the specification of functional safety requirements according to 7.2.1 and shall meet the following requirements:

– design and development (see 7.4);
– design standards;
– requirements for safety integrity and fault detection;

– architectural constraints on hardware safety integrity;
– the probability of dangerous random hardware failures;
– systematic safety integrity;
– the avoidance of failures;
– the control of systematic faults;
– the behaviour on detection of faults;
– the design and development of safety related software.

The design of IMDs and IFLSs shall take into account human capabilities and limitations including reasonably foreseeable misuse.

The design includes its diagnostic and failure reaction functions shall be documented and verified at appropriate stages according to the functional safety plan.

7.2.3 Verification plan for the development of safety functions

The verification plan shall be developed and shall contain at least the following items:

– description of verification strategies,
– organizational structure for verification,
– selection and utilization of test equipment,
– description of verification activities,
– plan for the review of specifications:
  - functional safety plan,
  - specification of functional safety requirements,
  - specification of safety functionality requirements,
  - specification of safety integrity requirements,
  - specification for commissioning, installation and setting into operation.

The plan shall be reviewed and updated during the development lifecycle, if necessary.

7.2.4 Validation plan for the development of safety functions

The validation plan shall be developed and shall contain at least the following items:

– description of validation strategies
– organizational structure for validation,
– acceptance criteria for validation,
– actions at failure to meet the acceptance criteria.

The plan shall be reviewed and updated during the development lifecycle, if necessary.

7.2.5 Planning of commissioning, installation and setting into operation

The plan for commissioning, installation and putting into operation shall be developed and shall contain at least the following items:

– description of special actions,
– requirements on the organization and persons,
– documentation on the process of putting into operation,
– documentation on testing the putting into operation process.

The plan shall be reviewed and updated during the development lifecycle, if necessary.

7.2.6 Planning of user documentation

The plan for user documentation shall be developed and shall contain at least the following items:

– information on the safety functions,
– information on safety integrity,
– information on user activities for commissioning, installation, the process of putting into operation, operation, modification and decommissioning,
– end of life information, if applicable.

The plan shall be reviewed and updated during the development lifecycle, if necessary.

7.3 IMD and IFLS safety validation planning (phase 10.2)

7.3.1 General

A functional safety plan shall be established for the entire development lifecycle of IMDs and IFLSs. The plan shall define the activities during the lifecycle according to the requirements of Clauses 5 to 9 and shall be updated if necessary during the development process. The plan shall also identify the organizational details for the activities. It shall be incorporated as a section “functional safety plan” in the quality management plan or it may be a separate document.

7.3.2 Functional safety plan

The functional safety plan shall include the following items as a minimum:

– identify the relevant activities specified in Clauses 6, 7 and 8;
– identify the organization (persons, departments or other units or resources) that is responsible for carrying out and reviewing each of the activities specified in Clauses 6, 7 and 8;
– identify or establish the procedures and resources to record and maintain information relevant to the functional safety of the IMD and IFLS:
  - results of the hazard identification and risk assessment;
  - safety functions together with their safety requirements;
  - organization responsible for maintaining functional safety;
  - procedures necessary to achieve and maintain functional safety for the IMD and IFLS.
– describe the strategy for configuration management taking into account relevant organization issues, such as authorized persons and internal structures of the organization.
– establish a verification plan that shall include:
  - integration of the verification in the quality management;
  - details of persons, departments or units who shall carry out the verification;
  - selection of verification strategies and techniques;
  - selection of verification activities;
  - acceptance criteria;
  - means to be used for the evaluation of verification results.
– establish a validation plan including:
  - requirements for the validation;

- identification of the relevant modes of operation of the IMD and IFLS;
- the technical strategy for validation, for example analytical methods or statistical tests;
- acceptance criteria;
- actions to be taken in the event of failure to meet the acceptance criteria.

The validation plan should indicate whether IMDs and IFLSs are to be subjected to routine production, testing, type testing and/ or sample testing and which special tests are necessary for functional safety purposes.

7.4 IMD and IFLS design and development (phase 10.3)

7.4.1 General

The design and development of IMDs and IFLSs shall, with regard to functional safety, be in accordance with the specification of the functional safety requirements. Where IMDs and IFLSs include safety and additional functions, then all the hardware and software that can negatively affect any safety function under normal and fault conditions shall be treated as a safety function and shall comply with the respective SIL. This consideration is not necessary when safety functions and additional functions are adequate independent from each other.

Wherever practicable, the safety functions should be separated from the additional functions in hard and software and the links or interfaces between them should be clearly defined.

NOTE Adequate independent means that the failure of any additional function in hard or software is not capable of causing a dangerous failure of any safety function.

The design of IMDs and IFLSs shall take into account human capabilities and limitations and shall be suitable for the operators and maintenance staff of the devices.

7.4.2 Design standards

IMDs and IFLSs shall be designed in accordance with IEC 61557-8 and IEC 61557-9 respectively.

7.4.3 Realization

IMDs and IFLSs shall be realized in accordance with their functional safety plan and the specifications of functional safety requirements (see 7.3.2 and 7.2.1).

7.4.4 Safety integrity and fault detection

IMDs and IFLSs shall comply with the requirements for:

– hardware safety integrity, comprising of:
  - hardware requirements (see 7.4.6);
  - architectural constraints on hardware safety integrity (see 7.4.12);
  - the requirements for the probability of dangerous failure on demand (PFD) (see 7.4.9);
– software requirements (see 7.4.7)
– systematic safety integrity comprising of:
  - requirements for the safety integrity level (SIL) (see 7.4.5);
  - EMC requirements (see 7.7.5);
  - requirements for data communication when applicable (see 7.4.14.3.4);
  - requirements for the avoidance of failures (see 7.4.14.1)
  - requirements for the control of systematic faults (see 7.4.14.2)

- proven in use approach (see Clause 9), evidence that the components fulfil the relevant requirements

– behaviour on the detection of a fault (see 7.4.14.3)

7.4.5 Safety integrity level (SIL) assignment

The SIL level of the safety function shall apply both to the related software and hardware.

If different SIL levels are assigned to different safety functions of a single device, the highest SIL shall be used unless it can be proven that the different safety functions are sufficiently independent in hardware and software.

Sufficient independence shall be established by showing that the probability of a dependent failure between the parts implementing safety functions of different integrity levels is sufficiently low in comparison with the probability of a dangerous failure for the highest safety integrity level associated with the safety functions involved.

7.4.6 Hardware requirements

IMDs and IFLSs shall be designed to meet the requirements of the functional safety requirements specification.

The hardware designed and the documentation written during the design and documentation lifecycle phase of IMDs and IFLSs shall meet all of the following:

– the requirements for HW safety integrity comprising the architectural constraints on HW safety integrity of 7.4.12, and the requirements for the probability of random HW failures (PFD) of 7.4.9;

– the requirements for systematic safety integrity comprising, the requirements for the avoidance of failures of 7.4.14.1, and the requirements for the control of systematic faults of 7.4.14.2;

– the requirements on the IMD and IFLS with regard to fault detection behaviour according to 7.4.14.3;

– independence of safety functions and additional functions unless all will be treated as safety related. The independence shall be such that failures in the additional 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.

7.4.7 Software requirements

Software for the safety functions shall be in accordance with the requirements defined in IEC 61508-3 for the specific SIL.

NOTE Some guidance about the use of IEC 61508-3 can be found in Annex D.

7.4.8 Review of requirements

The requirements for safety-related hardware and software shall be reviewed to ensure that they are adequately specified. In particular, the following shall be considered:

– safety functions;

– safety integrity requirements;

– equipment and operator interfaces.

7.4.9 Requirements for the probability of dangerous failure on demand (PFD)

7.4.9.1 General

The PFD of each safety function (or group of simultaneously used safety functions) to be performed by IMDs and IFLSs, estimated according to 7.4.9 and Annex B, shall be equal to or less than the target failure data (see Table 2) as specified in the safety integrity requirements specification (see 7.2.1.2).

The PFD value as defined by the SIL refers to a complete safety function.

The PFD of each safety function (or group of simultaneously used safety functions) of the IMD or IFLS shall be estimated separately.

NOTE 1 A number of modelling methods are available and the most appropriate method is a matter for the analyst and will depend on the circumstances. Available methods include:

– fault tree analysis (see IEC 61025);
– Markov models (see IEC 61165);
– reliability block diagrams (see IEC 61078).
– see also IEC 60300-3-1.

NOTE 2 The mean time to restoration (MTTR) that is considered in the reliability model will need to take into account the diagnostic and proof test intervals, the repair time and any other delays prior to restoration, and the mission time.

NOTE 3 Failures due to common cause effects and data communication processes can result from effects other than actual failures of hardware components (for example decoding errors). However, such failures are considered, for the purposes of this standard, as random hardware failures (see Annex D of IEC 61508-6:2010).

NOTE 4 IEC 61508-6:2010, Annex B describes a simplified approach which can be used to estimate the probability of dangerous failure of a safety function due to random hardware failures in order to determine that architecture meets the required target failure measure.

7.4.9.2 Estimation of PFD

The PFD of each safety function to be performed by the IMD or IFLS, due to random hardware failures shall be estimated by applying Annex A of IEC 61508-2:2010, taking into account:

– the architecture of the IMD and IFLS as it relates to each safety function under consideration;
– the estimated failure rate of each subsystem of the IMD and IFLS in any modes which would cause a dangerous failure of the IMD and IFLS but which are detected by diagnostic tests;
– the estimated failure rate of each subsystem of the IMD and IFLS in any modes which would cause a dangerous failure of the IMD and IFLS which are undetected by the diagnostic tests;
– the susceptibility of the IMD and IFLS to common cause failures (see Annex D of IEC 61508-6:2010);
– the diagnostic coverage (DC) of the diagnostic tests (determined according to Annex A and Annex C of IEC 61508-2:2010) and the associated diagnostic test interval;

NOTE 1 When establishing the diagnostic test interval, the intervals between all of the tests which contribute to the diagnostic coverage will need to be considered.

– the intervals at which proof tests are undertaken to reveal dangerous faults which are undetected by diagnostic tests;

In practice, proof testing may be difficult to implement for certain parts of the IMD and IFLS. In such cases, the proof test interval may be assumed to be the mission time of those parts or of the IMD and IFLS itself.

– the repair times for detected failures;

NOTE 2 The repair time will constitute one part of the mean time to restoration (MTTR) which will also include the time taken to detect a failure and any time period during which repair is not possible (see Annex B of IEC 61508-6:2010 as an example of how the mean time to restoration can be used to calculate the probability of failure). For situations where repair can only be carried out during a specific period of time, for example while the IT system is shut down and in a safe state, it is particularly important that full account is taken of the time period when no repair can be carried out, especially when this is relatively large.

– the probability of dangerous failure of any data communication process (see 7.4.14.3.4), if applicable.

7.4.10 Failure rate data

Component failure rate data shall be obtained from:

– a recognized source; or
– estimates based upon those components that are considered to be proven in use (see Clause 9).

The expected average operating temperature for a component should be used when estimating its failure rate.

Any failure rate data used should have a confidence level of at least 60 % when taken from a reliability handbook, at least 70 % when taken from other kinds of assessment (e.g. self-assessment or manufacturer-assessment).

NOTE Data can be derived from that, published in a number of standards (see Annex C) and industry sources.

If component specific failure data are available, then this is preferred. If this is not the case, then generic data should be used.

Although a constant failure rate is assumed by most probabilistic estimation methods, this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time), the results of most probabilistic calculation methods are therefore meaningless. Thus, any probabilistic estimation should include a specification of the components' useful lifetimes. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolytic capacitors can be very sensitive).

7.4.11 Diagnostic test interval

The diagnostic test interval of an IMD and IFLS shall be such as to enable the IMD and IFLS to meet the requirement for the PFD (see 7.4.9.2).

Where a dangerous fault can lead to the loss of the safety function, detection of this fault within the DC limits and initiation of a fault reaction is required in order to prevent a hazard.

Diagnostic and failure reaction functions shall be performed within the specified maximum fault reaction time. The maximum fault reaction time shall be less than 8 h for IMDs and IFLSs.

The diagnostic test interval of any subsystem of the IMD and IFLS having a hardware fault tolerance of zero, on which a safety function is entirely dependent, shall be such that the sum of the diagnostic test interval and the time to perform the specified action (failure reaction function) to achieve or maintain a safe state is less than the specified maximum fault reaction time.

7.4.12 Architectural constraints

7.4.12.1 Limitations of SIL

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 of IMD or IFLS that carry out that safety function. A hardware fault tolerance of *N* means that *N*+1 faults could cause a loss of the safety function.

Table 3 in this standard is a combination of Table 1 and Table 2 specified in IEC 61508-1:2010. It specifies the highest safety integrity level that can be claimed for a safety function which uses a subsystem taking into account the hardware fault tolerance and safe failure fraction of that subsystem (see Annex C of IEC 61508-2:2010). The requirements of Table 3, shall be applied to each subsystem carrying out a safety function and hence every part of the IMD or IFLS in those subsystems.

With respect to these requirements:

– in determining the hardware fault tolerance, no account shall be taken of other measures (such as diagnostics) that may control the effects of faults;

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

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

7.4.12.2 Type A and type B subsystems

7.4.12.2.1 Type A subsystem

A subsystem can be regarded as a type A subsystem, if for the components required to achieve the safety function:

– the failure modes of all constituent components are well defined; and

– the behaviour of the subsystem under fault conditions can be completely determined; and

– there is sufficient dependable failure data from field experience to show that the claimed failure rates for detected and undetected dangerous failures are met.

7.4.12.2.2 Type B subsystem

A subsystem shall be regarded as a type B subsystem if, for the components required to achieve the safety function, one or more of the criteria of a type A subsystem is not satisfied.

This means that if at least one of the components of a subsystem satisfies the conditions for a type B subsystem then the entire subsystem should be regarded as type B subsystem rather than a type A subsystem.

NOTE For example, the control section consisting of micro controllers, etc. is considered as a type B subsystem.

7.4.12.3 Architectural constraints with regard to hardware fault tolerances and safe failure fraction (SFF)

The architectural constraints of Table 3 apply for every type A subsystem or for every type B subsystem forming part of the IMD or IFLS.

Table 3 – Hardware safety integrity: architectural constraints on type A and type B safety-related subsystems

Safe failure fraction[a]		Hardware fault tolerance *N* (see 7.4.12)		
Type A	Type B	0	1	2
–	< 0 % to 60 %	No SIL	SIL 1	SIL 2
< 0 % to < 60 %	60 % to < 90 %	SIL 1	SIL 2	–[b]
60 % to < 90 %	90 % to < 99 %	SIL 2	–[b]	–[b]
[a] See 7.4.13 for details of the estimation of safe failure fraction (SFF). [b] This standard applies only to IMDs and IFLSs with a safety integrity level not greater than SIL 2.				
NOTE See Annex B.2 for examples of IMD and IFLS architectures.				

7.4.13 Estimation of safe failure fraction (SFF)

7.4.13.1 Methods of analysis

To estimate the SFF of a subsystem, analysis (for example fault tree analysis or failure mode and effects analysis (FMEA)) shall be performed to determine all the relevant faults and their corresponding failure modes. The probability of each failure mode of the subsystem shall be determined based on the probability of the associated fault(s).

7.4.13.2 Basis of data

The estimation of SFF shall be based upon either:

– statistically significant failure rate data collected from field experience; or
– component failure data from a recognized source.

See also 7.4.13.

7.4.13.3 Calculation of SFF

The safe failure fraction of a subsystem shall be calculated using Annex A and Annex C of IEC 61508-2:2010.

7.4.14 Requirements for systematic safety integrity

7.4.14.1 Requirements for the avoidance of failures

7.4.14.1.1 General

Techniques and measures shall be used which minimize the introduction of faults during the design and development of the hardware of IMDs and IFLSs.

Tests as planned according to 7.4.14.1.4 shall be performed. See also 7.7.2.

7.4.14.1.2 Selection of design methods

In accordance with the required safety integrity level, the design method chosen shall ensure:

– transparency, modularity and other features which minimize complexity and enhance comprehensibility of the design;
– clear and precise specification of
  - functionality,
  - subsystem interfaces,

- sequencing and time-related information,
- concurrency and synchronization;

– clear and precise documentation and communication of information;

– verification and validation.

7.4.14.1.3 Design measures

The following design measures shall be applied:

– proper design of the IMD or IFLS and/or subsystems including:
  - the use of components within manufacturer specifications, for example temperature, loading, power supply, power rating, and timing parameters;
  - the derating of design parameters to improve reliability where necessary to achieve target failure rates;
  - the proper combination and assembly of subsystems, for example cabling, wiring and any interconnections;
  - the use of reviews and inspections for early detection of design defects.

– compatibility:
  - using subsystems with compatible operating characteristics.

– withstanding specified environmental conditions:
  - designing the IMD or IFLS so that it is capable of safe operation in all specified environments, for example temperature, humidity, vibration, EM phenomena, pollution degree, overvoltage category, altitude.

7.4.14.1.4 Test planning

During the design, the following different types of testing shall be planned as necessary:

– subsystem testing;

– integration testing;

– validation testing;

– configuration testing.

Documentation of the test planning shall include:

– types of tests to be performed and procedures to be followed;

– test environment, tools, configuration and programs;

– pass/fail criteria.

Automatic testing tools and integrated development tools shall be used, where applicable.

NOTE The integrity of such tools can be demonstrated by specific testing, by an extensive history of satisfactory use or by independent verification of their output for the particular IMD or IFLS that is being designed.

7.4.14.1.5 Design maintenance requirements

A process for design maintenance and retesting, to ensure the safety integrity of the IMD or IFLS remains at the required level during subsequent design revisions, shall be defined at the design stage.

7.4.14.2 Requirements for the control of systematic faults

7.4.14.2.1 Design features

For controlling systematic faults, the design shall include features that make the IMD or IFLS and its subsystems tolerant against:

– residual design faults in the hardware, unless the possibility of hardware design faults can be excluded by applying Table A.15 of IEC 61508-2:2010;
– environmental stresses, including electromagnetic disturbances, by applying Table A.16 of IEC 61508-2:2010;
– mistakes made by the operator of the IMD or IFLS (see Table A.17 of IEC 61508-2:2010);
– residual design faults in the software (see 7.4.3 of IEC 61508-3:2010 and Table A.2);
– errors and other effects arising from any data communication process, if applicable (see 7.4.14.3.4).

7.4.14.2.2 Testability and maintainability

Testability and maintainability shall be considered during the design and development activities in order to facilitate implementation of these properties in the final IMD or IFLS.

7.4.14.2.3 Human constraints

The design of the IMD or IFLS shall take into account human capabilities and limitations and be suitable for the actions assigned to operators and maintenance staff. The design of operator interfaces shall follow good human-factor practice and shall accommodate the likely level of training or awareness of operators.

7.4.14.2.4 Protection against unintentional modification

The IMD or IFLS shall incorporate measures to protect (or facilitate protection) against unintentional modifications to safety-related software, hardware, parameterization and configuration.

NOTE See IEC 61508-7:2010, B.4.8.

7.4.14.2.5 Loss of electrical supply

The IMD or IFLS shall be specified and designed taking into account the effects of the loss and return of electrical supply.

7.4.14.3 Behaviour on fault detection

7.4.14.3.1 Fault detection

When a dangerous failure is detected that can lead to the loss of the safety function the system shall go into the safe position within the maximum process safety time.

For IMDs and IFLSs, the process safety time shall be less than 8 h.

7.4.14.3.2 Fault tolerance greater than zero

The detection of a dangerous fault (by automatic self-tests or by any other means) in any subsystem which has a hardware fault tolerance greater than zero shall result in either:

– a failure reaction function, or
– the isolation of the faulty IMD or IFLS to allow continued safe operation of the system whilst the faulty part is repaired. If the repair is not completed within the mean time to restoration (MTTR) assumed in the calculation of the probability of dangerous failure (see 7.4.9), then a failure reaction function shall be initiated.

7.4.14.3.3 Fault tolerance zero

The detection of a dangerous fault (by automatic self-tests or by any other means) in any subsystem having a hardware fault tolerance of zero and on which a safety function is entirely dependent shall result in a failure reaction function.

7.4.14.3.4 Requirements for data communication

When data communication is used in the implementation of a safety function then the probability of undetected failure of the communication process shall be estimated taking into account transmission errors, repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade. This probability shall be taken into account when estimating the PFD of the safety function due to random hardware failures (see 7.4.9.2).

The measures necessary to ensure the required failure measure of the communication process shall be implemented according to the requirements of IEC 61508-2 and of IEC 61508-3.

Where the data communication is used to exchange safety related data with subsystems external to the IMD or IFLS the above requirements apply to the IMD or IFLS together with the related subsystems.

7.5 IMD and IFLS integration (phase 10.4)

7.5.1 Hardware integration

The IMD or IFLS shall be integrated according to its specified design.

As part of the integration of all subsystems and components into the IMD or IFLS the IMD or IFLS shall be tested according to the specified integration tests. These tests are specified on the verification plan and shall show that all modules interact correctly to perform their intended function and not perform unintended functions.

Alternatively, the requirements for hardware integration are covered when the type testing of the IMD or IFLS according to IEC 61557-8 or IEC 61557-9 and 7.7 is successfully passed.

7.5.2 Software integration

The integration of safety-related software parts/modules into the IMD or IFLS shall be carried out according to IEC 61508-3. It shall include tests that are specified on the software verification plan to ensure the compatibility of the software with the hardware such that the functional and safety performance requirements are satisfied.

NOTE This does not imply testing of all input combinations. Testing can be performed according to IEC 61508-3, Annex B.

7.5.3 Modifications during integration

During the integration, any modification or change to the IMD or IFLS shall be subject to an impact analysis, which shall identify all components affected, and additional verification.

7.5.4 Integration tests

The integration test(s) shall be specified in a verification plan. A functional test shall be applied, in which input data or set values, which adequately characterize the normally expected operation, are given to the IMD or IFLS. The safety function is requested (for example by simulation of an insulation fault) and its resulting operation is observed and compared with that given by the specification.

7.6 IMD and IFLS documentation related to installation, commissioning, operation and maintenance procedures (phase 10.5)

7.6.1 General

Operating instructions shall be provided as required by IEC 61557-8 for IMDs and IEC 61557-9 for IFLSs. The additional information for the user as outlined in 7.6 shall be provided to the user as an annex to the operating instructions or in separate documents.

User instructions contain essential information on how to use and how to maintain the safety-related devices. All instructions should be easily understood. Figures and schematics should be used to describe complex procedures and dependencies.

7.6.2 Functional specification

The functional specification shall describe the safety functions including their operating conditions and limitations.

7.6.3 Compliance information

Information for compliance with functional safety according to this standard shall be provided on request to the user.

The compliance information shall include the following mandatory items:

– Safety integrity level (SIL) with conditions,
– Probability of failure on demand (PFD).

7.6.4 Information for commissioning, installation, setting into operation, operation and maintenance

7.6.4.1 General

The information in 7.6.4.2 to 7.6.4.6 shall be provided to realize and maintain the defined level of functional safety of the IMD and IFLS in the application.

7.6.4.2 Information for commissioning

This information shall include all conditions and constraints in the application of IMDs and IFLSs which are required to observe the correct function of the safety functions.

7.6.4.3 Information for installation

This information shall include all conditions and constraints for the installation of IMDs and IFLSs that are required to observe the correct function of the safety functions and information on the identification of the hard and software versions.

7.6.4.4 Information for setting into operation

This information shall include all requirements for observing the correct safety functions of IMDs and IFLSs for setting them into operation.

It shall include:

– settings for the safety functions and for the additional functions,
– measures to prevent the settings from unauthorized modifications,
– tests to be performed on the IMD or IFLS itself and in the IT system,
– documentation of the tests with identification of the tests, the results and the testing person.

7.6.4.5 Information for operation

This information shall include all requirements and constraints for observing the correct safety functions of IMDs and IFLSs for their operation.

They shall include:

– test intervals which are necessary to maintain the safety functions and the diagnostic coverage (DC);
– necessary reactions on the failure during the tests and on possible fault indications on the devices;
– documentation and/or supervision of the tests and operation.

7.6.4.6 Information for maintenance

This information shall include all requirements for observing the correct safety functions of IMDs and IFLSs for their maintenance over the lifetime of the devices.

This information shall include:

– routine actions for the maintenance of the devices to observe the safety functions if necessary;
– maintenance actions after failed tests or fault indications on the devices;
– measures after repair and reinstallation of the devices;
– measures for software updates and the following tests, if applicable;
– end of life information for the replacement of devices, if necessary.

7.7 IMD and IFLS safety validation (phase 10.6)

7.7.1 General

Tests, verification and validation shall be performed to ensure the compliance with the functional safety plan (see 7.3.2).

7.7.2 Test

Testing of the safety functions of the IMD or IFLS shall be carried out concurrently with each phase of the development process.

The test shall be documented, and shall include a detailed description of:

– the functional testing of each safety function,
– the functional testing of each diagnostics function for each safety function,
– the acceptance criteria.

Tests may be either “black-box” where no account is taken of the internal implementation of the safety function, or “white-box” where specific knowledge of the implementation is used to determine the test (for example fault insertion).

Testing may be waived or replaced by other verification or validation methods if permitted by the relevant requirements.

7.7.3 Verification

During the design process, it shall be checked and recorded after each design phase that the requirements of that design phase have been fulfilled. Verification can be performed using assessment, analysis, examination, review, and/or testing.

NOTE The verification can include for example:

– review of the documentation of the respective phase,

– design reviews,

– functional tests.

7.7.4 Validation

After the design process, it shall be checked and recorded that the IMD or IFLS fulfil all requirements of the safety requirements specification. Validation can be performed using assessment, analysis, examination, review, and/or testing. Recommendations for the avoidance of faults during validation are given in Table B.5 of IEC 61508-2:2010.

7.7.5 EMC requirements

7.7.5.1 General

EMC immunity tests for safety functions shall be carried out with the requirements of IEC 61326-3-1 and IEC 61326-2-4.

The performance criteria that shall be applied during EM immunity testing on the IMD or IFLS is specified in 7.7.5.3. These criteria do not apply to the additional (non-safety related) functions of the devices, for which only the requirements of IEC 61326-2-4 apply.

7.7.5.2 Intended environment

The EM environment specified or anticipated for intended use of an IMD or IFLS shall be used to determine the test levels for EM immunity. For immunity testing, the tests of IEC 61326-2-4:2006, Table 101 apply, however, with the increased test levels of IEC 61326-3-1:2008, Table 1a) to 1f).

7.7.5.3 Performance criteria

The performance criteria during EM testing of the functional safety of an IMD or IFLS are the same as for normal operation. The performance criteria of IEC 61326-2-4:2006, Table 102 apply, however with higher test levels as defined in 7.7.5.2.

7.7.5.4 Introduction of hazards

During EM immunity testing, no unsafe conditions or hazards shall be introduced by the IMD or IFLS. Unsafe conditions or hazard conditions shall be defined in the safety integrity specification.

7.7.5.5 Verification

When EM immunity tests are performed, the specified mitigation measures shall be in place.

Depending on the results of the analysis of the defined EM environment of the intended IMD or IFLS application, the increased immunity (as required by IEC 61508-2) shall be verified.

7.7.5.6 Emission test

Emission tests are identical as for normal IMD or IFLS that are not intended for functional safety applications (see IEC 61557-8 and IEC 61557-9).

8 Requirements for modifications

8.1 General

The objective of this Clause 8 is to ensure that the functional safety of the IMD and IFLS is maintained when design modifications are made after the original design is released for manufacture.

Prior to carrying out any modification activity, procedures shall be planned. Modifications shall be performed with at least the same level of expertise, automated tools, and planning and management as the initial development of the IMD and IFLS Modification shall be carried out as planned.

8.2 Modification request

The modification shall be initiated only by the issue of a modification request under the procedures for the management of functional safety (see Clause 6). The request shall detail the following:

– reasons for the change,

– proposed change (both hardware and software).

8.3 Impact analysis

An assessment shall be made of the impact of the proposed modification on the functional safety of the IMD and IFLS. The assessment shall include an analysis sufficient to determine the breadth and depth to which a return to appropriate development steps according to 7.4 will need to be undertaken.

8.4 Authorization

Authorization to carry out the requested modification shall be dependent on the results of the impact analysis.

9 Proven in use approach

The requirements of this standard shall be met by adherence of the proven-in-use process according to IEC 61508-2:2010, 7.4.10.

Annex A
(informative)

Risk analysis and SIL assignment for IMDs and IFLSs

A.1 General

This informative Annex A provides examples for risk estimation in IT systems which can be applied to assign safety integrity levels (SIL) to the safety functions of IMDs and IFLSs.

The SIL for the respective safety function of the IMD or IFLS depends on the risk estimation for this safety function in the respective IT system where the devices are used. For different safety functions of an IMD or IFLS different SILs can be assigned depending on the risk analysis for the respective safety function in the complete IT system.

In this part of IEC 61557, the EUC (equipment under control according to the IEC 61508 series) corresponds to the IT system, including the loads as defined in Figure A.1.

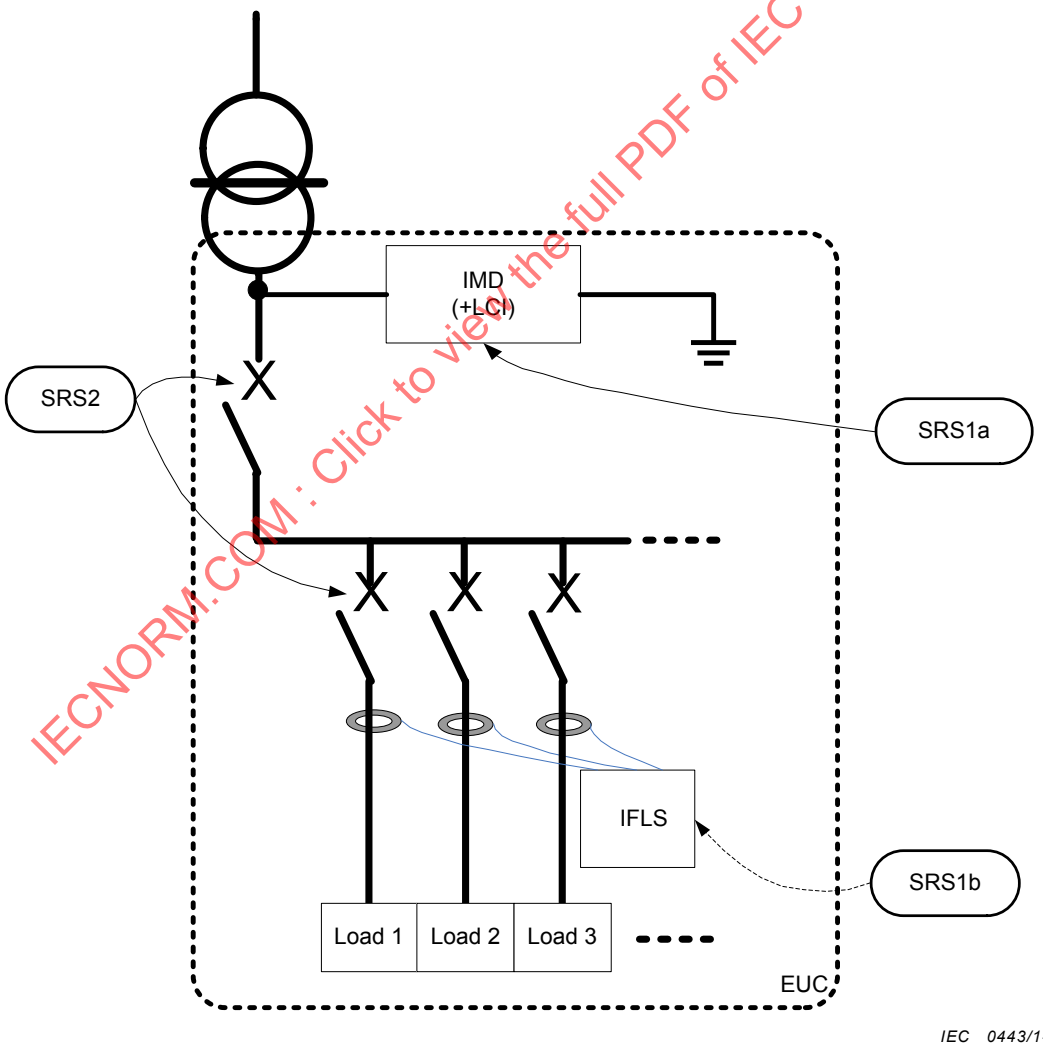


Figure A.1 – Functional elements of an IT system and their relationship to the definitions and abbreviations of the IEC 61508 series

The SRS (safety related system according to the IEC 61508 series) corresponds to the protective measures related to the EUC. This SRS can be split into different levels of protection measures:

– SRS 1a: safety related system in charge of monitoring the IT system and in charge of warning in case of single fault. SRS 1a is based on safety functions provided by IMD.
– SRS 1b: safety related system in charge of monitoring feeders and in charge of locating a single fault, thus easing maintenance operations. SRS 1b is optional and based on safety functions provided by IFLS.
– SRS 2: safety related system in charge of tripping the complete IT system or a part of this IT system when a second insulation fault occurs before the single fault was repaired. SRS 2 is based on safety functions provided by circuit-breakers.

IEC 61508 requirements are based on risk analysis, this risk analysis leading to the definition of the SIL level requested for SRS. The following Table A.1 provides an example of a risk analysis (based on Figure A.1) on various applications using IT systems:

Table A.1 – IT system risk analysis

Application	Reason	Risk analysis	Is functional safety applicable?
Use of IT system, SRS 1a for monitoring this IT system, SRS 2 for protecting this IT system.	IT system is used for continuity of supply reasons (no tripping when a first insulation fault occurs).	Availability is requested for economic reasons: – industry in general, – marine applications in general.	No, but optional.
		Availability is requested for safety, e.g.: – operating theatre and intensive care unit in hospitals (group 2 medical locations, – marine applications (ships, offshore, etc.), – chemistry, – railway applications, – parts of control systems in nuclear power plants.	Highly recommended, it should cover various risks with human impact.
	IT system is used in order to prevent circulation of hazardous current when a first insulation fault occurs.	First insulation fault may increase the risk of dangerous touch currents in the following application: – operating theatre and intensive care unit in hospitals.	Highly recommended, it should cover risks of shock with human impact.
		Current circulation may start a fire, e.g. in the following applications: – photovoltaic farms	Highly recommended, it should cover risks of fire with human impact.
	IT system is used in order to prevent an arc when a second insulation fault occurs (an arc occurs when the SRS 2 systems trips).	An electric arc may be hazardous, e.g. in the following applications: – mines, – chemistry (for risky locations), – offshore (for risky locations).	Highly recommended, it should cover risks of fire or explosion with human impact.

Use of optional SRS 1b in IT system.	All reasons	In case of a single insulation fault, it is urgent to localise the fault in order to minimize the MTTR and consequently minimize the time during which a second insulation fault may occur.	No, but optional.
NOTE Examples of typical applications are provided in Annex F.			

A.2 SIL assignment for IMDs and IFLSs

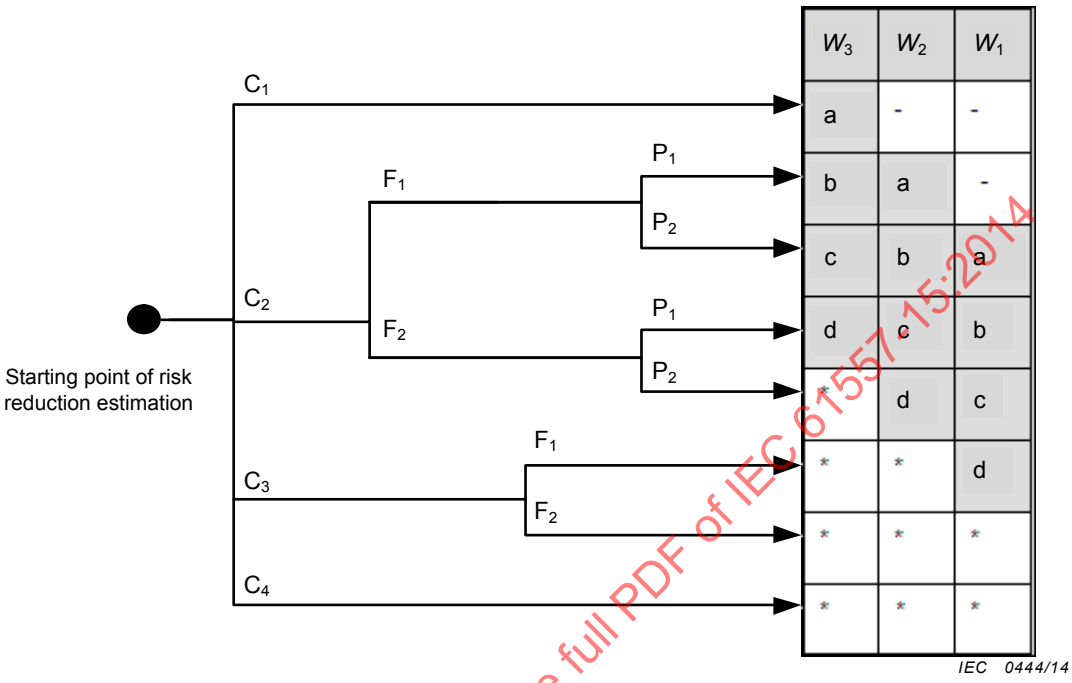
Table A.2 provides some guidance about the relevant applicable SIL level.

Figure A.2 – SIL assignment for IMDs and IFLSs

Applications using IMD functions	Applications using IFL functions	Requirement for the related devices
General purpose applications where IMD is installed to warn the maintenance team when a first fault occurs in an IT system.	General purpose applications where IFLS is installed to provide support to the maintenance team for the location of insulation faults in an IT system.	IMD complying with IEC 61557-8 IFLS complying with IEC 61557-9
Safety applications where IMD are intended to achieve safety functions with a SIL level coherent with the SIL level requested by the application (see risk analysis defined in Figure B.1), e.g. applications where: – Safety is based on the continuity of supply: SIL 1 is recommended. – Safety is based on the immediate reaction to a warning signal by the personnel supervising the IT system: SIL 1 is recommended. – Safety is based on the use of the warning signal as a way to activate additional safety functions or to trip: SIL 1 or SIL 2 is recommended.	Safety applications where IFLs are intended to achieve safety functions with a SIL level coherent with the SIL level requested by the application (see risk analysis defined in Figure B.1), e.g. applications where: – Safety is based on the localization of the insulation fault in a defined timeslot (e.g. critical time for repair): SIL 1 is recommended. – Safety is based on the immediate localization of an insulation fault below the response value of the IMD: SIL 1 is recommended. – Safety is based on the immediate reaction to a warning signal by the personnel supervising the IT system: SIL 1 is recommended. – Safety is based on the use of the warning signal as a way to activate additional safety functions or to trip: SIL 1 or SIL 2 is recommended.	IMD complying with IEC 61557-8 and IEC 61557-15 IFLS complying with IEC 61557-9 and IEC 61557-15

A.3 Example of risk graph

The risk graph of Figure A.2 is based on the example data in Table A.4. For the determination of SIL for IMD or IFLS the specified risks of the respective application should be assumed.



Key

a, b, c, d represent the necessary minimum risk reduction. The minimum risk reduction leads to the safety integrity level (SIL) shown in Table A.3.

C consequence risk parameter (see Table A.4)

F frequency and exposure time risk parameter (see Table A.4)

P possibility of avoiding hazard risk parameter (see Table A.4)

W probability of the unwanted occurrence (see Table A.4)

* Not covered by this standard.

Figure A.2 – Example of risk graph

Table A.3 – Link between minimum risk reduction and SIL

Necessary minimum risk reduction	Safety integrity level (SIL)
-	Requirements according to IEC 61557-8, IEC 61557-9
a	Requirements according to IEC 61557-8, IEC 61557-9
b, c	Requirements according to IEC 61557-8, IEC 61557-9 and SIL 1 requirements according to IEC 61557-15
d	Requirements according to IEC 61557-8, IEC 61557-9 and SIL 2 requirements according to IEC 61557-15

Table A.4 – Example of classifications according to risk graph Figure A.1

Risk parameter		Classification	Comments
Consequence *(C)*	C_1	Minor injury	Classification schemes for environmental or material damage e.g. through the failure of the power in the IT system, malfunction of control devices when insulation faults occur, explosion through heath should be respected according to the application
	C_2	Serious permanent injury to one or more persons; death to one person	
	C_3	Death to several people	
	C_4	Death to many people	
Frequency of and exposure time of the hazard *(F)*	F_1	Rare to more often exposure of the hazard	See comments to *(C)*
	F_2	Frequent to permanent exposure of the hazard	
Possibility of avoiding the hazard *(P)*	P_1	Possible under certain (defined) conditions	This parameter takes into account: operation of the IT system (supervised by skilled or unskilled persons or unsupervised); rate of development of the hazardous event (e.g. suddenly, quickly or slowly); ease of recognition of the hazard (e.g. detected immediately , by technical measures); avoidance of the hazard (e.g. by construction of the IT system); actual safety experience (e.g. proven in use).
	P_2	Almost impossible	
Probability of the unwanted occurrence (*W*)	W_1	Very slight probability that the unwanted occurrence will come and only a few unwanted occurrences are likely	Purpose of *W* is to estimate the frequency of the unwanted occurrence without the safety related system but including other risk reduction measures. If little or no experience exists with the IT system and the use of IMD or IFLS, or of similar systems, the *W* factor can be estimated by calculation under consideration of worst case predictions.
	W_2	Slight probability that the unwanted occurrences will come and few unwanted occurrences are likely	
	W_3	Relatively high probability that the unwanted occurrences will come and frequent unwanted occurrences are likely	
See also IEC 61508-5:2010, Table E.2 and E.3 for more detailed information on risk estimation.			

A.4 Alternative method of SIL assignment – quantitative method

See IEC 61508-5:2010, Annex D for SIL assignment using a quantitative method.

Annex B
(informative)

Examples for the determination of PFD, DC and SFF

B.1 General

This Annex B provides information and sources for calculating the probabilities of hardware failure (PFD), diagnostic coverage (DC) and safe failure fraction (SFF) derived from the respective SIL for the safety functions of IMDs or IFLSs that shall be developed according to this standard.

The information provided is informative in nature and should not be interpreted as the only evaluation techniques that might be used. Annex B uses a simplified approach for calculation that is explained in Annex B and Annex C of IEC 61508-6:2010 together with other approaches for PFD determination.

The calculation of DC and SFF is defined in IEC 61508-2:2010, Annex C. An example of DC and SFF calculation is included in IEC 61508-6:2010, Annex C.

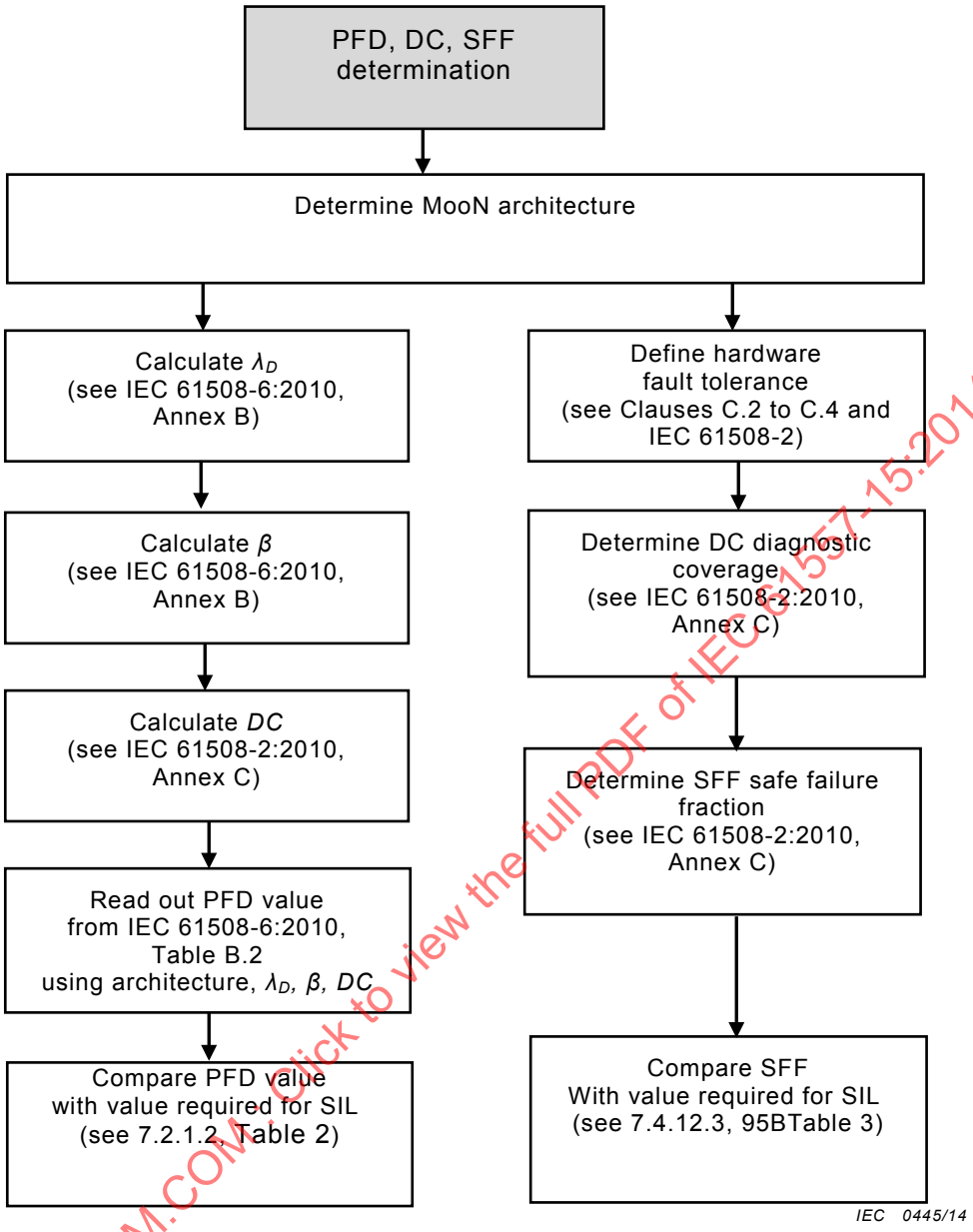


Figure B.1 – Flowchart for PFD, DC, SFF determination

B.2 Examples of IMD and IFLS architectures

For examples of MooN architectures see Annex B of IEC 61508-6:2010, IEC 62061 and ISO 13849-1. These examples are not exhaustive.

Annex C
(informative)

Failure rate databases

C.1 General

Annex C contains a non-exhaustive listing of standard references for failure rate data and for failure modes for electronic components. The different standard references may not always be in conformity and therefore care should be taken when applying the data.

C.2 Failure rate references in current standards

IEC/TR 62380, *Reliability data handbook, universal model for reliability prediction of electronic components, PCBs and equipment*

IEC 61709, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 60319, *Presentation and specification of reliability data for electronic components*

Annex D
(informative)

Guide to embedded software design and development

D.1 General

This informative Annex D provides guidance for the use of IEC 61508-3.

If IMD or IFLS contain embedded software, this Annex D should assist persons in the design and development of the embedded software for implementing safety functions within IMD or IFLS.

The major objective dealt with here is general guidance on the prevention of embedded software failures and any other unexpected behaviour of embedded software that might lead to dangerous faults in the system.

In order to satisfy these objectives, consideration is given to the following points:

– a description of the main characteristics that software elements of an IMD or IFLS should possess to guarantee its quality and safety (software element guidelines);
– the establishment of all relevant technical activities and provisions associated with software development, for those involved in software design. These can then be used to guide the designer during the production of this type of software (software development process guidelines);
– a reference framework for software evaluation. This allows the software designer and/or analyst to decide that software elements satisfy the safety requirements of the IMD or IFLS or their subsystem to be analysed (software verification guidelines).

D.2 Software element guidelines

D.2.1 General

Clause D.2 presents the guidelines that an embedded software element of IMD or IFLS or their subsystem should fulfil to be safe in operation and of satisfactorily high quality. To obtain such a software element, a number of activities, a certain organization and a number of principles should all be established. This should take place as early as possible in the development cycle.

D.2.2 Interface with system architecture

The list of constraints imposed by hardware architecture on software should be defined and documented. Consequences of any hardware/software interaction on the safety of the system being monitored should be identified and evaluated by the designer and taken into account in the software design.

NOTE Constraints include: protocols and formats, input/output frequencies, by rising and falling edge or by level, input data using reverse logic, etc. Listing these constraints allows them to be taken into account at the start of the development activity and reduces the risk of incompatibilities between software and hardware when the former is installed in the target hardware.

D.2.3 Software specifications

Software specifications should take the following into account:

– safety-related control functions with a quantitative description of the performance criteria (precision, exactness) and temporal constraints (response time), all with tolerances or margins when possible,

– system configuration or architecture,
– instructions relevant to hardware safety integrity,
– instructions relevant to software integrity,
– constraints related to memory capacity and system response time,
– operator and equipment interfaces,
– instructions for software self-monitoring and for hardware monitoring carried out by the software,
– instructions that allow all the safety-related control functions to be verified while the systems are working (e.g. on-line testing, capture time for fleeting signals, coincidence with scan rate).

The instructions for monitoring developed, taking safety objectives and operating constraints (duration of continuous operation, etc.) into account, can include devices such as watch dogs, central processing unit (CPU) load monitoring, feedback of output to input for software self-monitoring. For hardware monitoring, CPU and memory monitoring, etc. instructions for safety-related control function verification: for example, the possibility of periodically verifying the correct operation of safety devices should be included in the specifications.

Functional requirements should be specified for each functional mode. The transition from one mode to the other should be specified.

NOTE Functional modes can include nominal modes and one or more degraded modes. The objective is to specify the behaviour in all situations in order to avoid unexpected behaviours in non-nominal contexts.

D.2.4 Pre-existent software

The term "pre-existent" software refers to source modules that have not been developed specifically for the system at hand, and are integrated into the rest of the software. These include software elements developed by the designer for previous projects, or commercially available software (e.g. modules for calculations, algorithms for data sorting).

When dealing with this type of software, and especially in the case of commercial software elements, the designer does not always have access to all the elements needed to satisfy the previous requirements (e.g. what tests have been carried out, is the design documentation available). Specific co-ordination with the analyst can therefore be necessary at the earliest possible moment.

The designer should indicate the use of pre-existent software to the analyst, and the designer should demonstrate that pre-existent software has the same level as the other software elements. Such a demonstration should be done by either a) and b) or a) or b):

a) using the same verification activities on the pre-existent software as on the rest of the software,
b) practical experience where the pre-existent software has functioned on a similar system in a comparable executable environment (e.g. it may be necessary to evaluate the consequences of a change of the compiler or of a different software architecture format).

NOTE The goal of indicating the use of pre-existent software is to open up consultation with the analyst as early as possible about any eventual difficulties that this type of software might cause. The integration of pre-existent source modules can be the cause of certain anomalies or unsafe behaviour if they were not developed with the same specifications as the rest of the software.

Pre-existent software should be identified using the same configuration management and version control principles that are applied to the rest of the software.

Configuration management and version control should be exercised over all the software components, regardless of their origin.

D.2.5 Software design

Description of the software design should include a description of:

– software architecture that defines the structure decided to satisfy specifications,
– inputs and outputs (e.g. in the form of an internal and external data dictionary), for all the modules making up the software architecture,
– interrupts,
– global data,
– each software module (inputs/outputs, algorithm, design particularities, etc.),
– module or data libraries used,
– pre-existent software used. Software should be modular and written in a logical manner in order to facilitate its verification or maintenance:
  - each module or group of modules should correspond, if possible, to a function in the specification(s),
  - interfaces between modules should be as simple as possible.

NOTE The general characteristic of correct software architecture can be summed up in the following way: a module should possess a high level of functional cohesion and a simple interface with its environment.

Software should:

– limit the number or extent of global variables,
– control the layout of arrays in memory (to avoid a risk of array overflows).

D.2.6 Coding

The source code should:

– be readable, understandable and subject to tests,
– satisfy design specifications of the software module,
– obey the coding manual instructions.

D.3 Software development process guidelines

D.3.1 Development process: software lifecycle

The objective of the following guidance applicable to the software lifecycle is to obtain a formalized description of the organization of software development and, in particular, the different technical tasks making up this development.

The software development lifecycle should be specified and documented (e.g. in a software quality plan). The lifecycle should include all the technical activities and phases necessary and sufficient for software development.

Each phase of the lifecycle should be divided into its elementary tasks and should include a description of:

– inputs (documents, standards, etc.),
– outputs (documents produced, analytical reports, etc.),
– activities to be carried out,
– verifications to be performed (analyses, tests, etc.).

D.3.2 Documentation: documentation management

The documentation should conform to IEC 61508-1:2010, Clause 5.

D.3.3 Configuration and software modification management

Management of the configuration and therefore of the version is an indispensable part of any development which may require approval. Indeed, approval is only valid where a given configuration can be identified. Configuration management includes configuration identification activities, modification management, the establishment of reference points and the archiving of software elements, including the associated data (documents, records of tests, etc.).

Throughout the entire project lifecycle, the principal objectives are to provide:

– a defined and controlled software configuration that guarantee physical archiving and that can be used to reproduce an executable code coherently (with future software production or modification in mind),
– a reference basis for modifications management,
– a means of control so that any problems are properly analysed, and that the approved modifications are properly carried out.

Concerning the modifications, their reasons could arise from, for example:

– functional safety below that specified,
– systematic fault experience,
– new or amended safety legislation,
– modifications to the machine or its use,
– modification to the overall safety requirements,
– analysis of operations and maintenance performance, indicating that the performance is below target.

D.3.4 Configuration and archiving management

A procedure for configuration management and modifications management should be defined and documented. This procedure should, as a minimum, include the following items:

– articles managed by the configuration, at least: software specification, preliminary and detailed software design, source code modules, plans, procedures and results of the validation tests,
– identification rules (of a source module, of a software version, etc.),
– treatment of modifications (recording of requests, etc.).

For each article of configuration, it should be possible to identify any changes that may have occurred and the versions of any associated elements.

NOTE 1 The purpose is to be able to trace the historical development of each article: what modifications have been made, why, and when.

Software configuration management should allow a precise and unique software version identification to be obtained. Configuration management should associate all the articles (and their version) needed to demonstrate the functional safety.

All articles in the software configuration should be covered by the configuration management procedure before being tested or being requested by the analyst for final software version evaluation.

The objective here is to ensure that the evaluation procedure be performed on software with all elements in a precise state. Any subsequent change may necessitate revision of the software so that it can be identifiable by the analyst.

Procedures for the archiving of software and its associated data should be established (methods for storing backups and archives).

NOTE 2 These backups and archives can be used to maintain and modify software during its functional lifetime.

D.3.5 Software modifications management

Any software modification which has an impact on the functional safety of the IMD or IFLS should be subject to the rules established for modification and configuration management such that the development process is recommenced at the highest "upstream" point needed to take the modification into account without diminishing the functional safety.

NOTE In particular, the documentation should also be updated and all necessary verification activities carried out. This guarantees that the software will keep all its initial properties after any modification.

D.4 Development tools

Tools used during the development procedure (compiler, linker, tests, etc.) should be identified (name, reference, version, etc.) in the documentation associated with the software version (e.g. in the version control documentation).

NOTE Different versions of tools do not necessarily produce the same results. Precise identification of tools thus directly demonstrates the continuity of the process of generation of an executable version in the event that a version is modified.

D.5 Reproduction of executable code production

Any option or change in the generation, during the software production should be recorded (e.g. in the version sheet) so that it is possible to say how and when the software was generated.

All failures linked to safety functions brought to the attention of the designer of the system should be recorded and analysed.

NOTE This means that the designer is aware of any safety-related failures that are communicated to him and that he takes the appropriate action (e.g. warning other users, software modification, etc.).

D.6 Software verification and validation

The purpose of verification activities is to demonstrate that software elements stemming from a given phase of the development cycle conform to the specifications established during the previous phases and to any applicable standards or rules. They also serve as a means of detecting and accounting for any errors that might have been introduced during software development.

Software verification is not simply a series of tests, even though this is the predominant activity for the relatively small software element considered in this Annex. Other activities such as reviews and analyses, whether associated with these tests or not, are also considered to be verification activities. In certain cases, they can replace some tests (e.g. in the event that a test cannot be carried out because it would cause deterioration of a hardware component).

D.7 General verification and validation guidelines

The analyst should be able to carry out the evaluation of software conformity by conducting any audits or expertise deemed useful during the different software development phases. All technical aspects of software lifecycle processes are subject to evaluation by the analyst. The

analyst should be allowed to consult all verification reports (tests, analyses, etc.) and all technical documents used during software development.

The intervention of the analyst at the specification phase is preferable to an a posteriori intervention since it should limit the impact of any decisions made. On the other hand, financial and human aspects of the project are not subject to evaluation.

NOTE 1 It is in the interest of the applicant to provide satisfactory evidence of all activities carried out during software development.

The analyst should have all the necessary elements at his or her disposal in order to formulate an opinion.

Evaluation of software conformity is performed for a specific, referenced software version. Any modification of previously evaluated software that has received a final opinion from the analyst should be pointed out to the latter so that any additional evaluation activities can be carried out to update this opinion.

NOTE 2 Any modification can modify software behaviour; the evaluation performed by the analyst can therefore only be applied to a precise software version.

D.8 Verification and validation review

Analysis activities and software design verification should verify the conformity to specifications.

NOTE 1 The purpose is to ensure that the software specification and design (both detailed and preliminary) are coherent.

An external validation review (with the analyst) should be held at the end of the validation phase.

NOTE 2 This can be used to ascertain whether or not the element satisfies the specifications.

The result of each review should be documented and archived. It should include a list of all actions decided on in the review process, and the review conclusion (decision on whether or not to move on to the next activity). The activities defined in the review should be monitored and treated.

D.9 Software testing

D.9.1 General validation

Before writing the first test sheets, it is important to establish a test strategy in a test plan. This strategy indicates the adopted approach, the objectives that have been set in terms of test coverage, the environments and specific techniques used and the success criteria to be applied, etc.

The test objectives should be adapted to the type of software and to the specific factors. These criteria determine the types of test to be undertaken – functional tests, limit tests, out of limit tests, performance tests, load tests, external equipment failure tests, configuration tests – as well as the range of objects to be covered by the tests (functional mode tests, safety-related control function tests, tests of each element in the specification, etc.).

Verification of a new software version should include non-regression tests.

NOTE Non-regression tests are used to ensure that the modifications performed on the software have not modified the behaviour of the software in any unexpected way.

D.9.2 Software specification verification: validation tests

The purpose of these verifications is to detect errors associated with the software in the target system environment. Errors detected by this type of verification include: any incorrect mechanism to treat interruptions, insufficient respect of running time requirements, incorrect response from the software operating in transient mode (start-up, input flow, switching in a degraded mode, etc.), conflicts of access to different resources or organizational problems in the memory, inability of integrated tests to detect faults, software/hardware interface errors, stack overflows. Validation tests are the principal component of software specification verification.

The test coverage should be made explicitly in a traceability matrix and ensuring that:

– each element of the specification, including safety mechanisms, is covered by a validation test; and

– the real-time behaviour of the software in any operational mode can be verified.

Furthermore, the validation should be carried out in conditions representative of the operational conditions of the IMD or IFLS or their subsystems.

This guarantees that the software reacts as expected in operation. It applies only to cases where the test conditions can be destructive for hardware (e.g. physical fault of a component that cannot be simulated). To be significant, validation should be performed in the operational conditions of the IMD or IFLS subsystem (i.e. with the final versions of software and hardware, and the software installed in the target system). Any other combination could decrease the efficiency of the test and require analysis of its representation.

Validation results should be recorded in a validation report that should cover at least the following points:

– the versions of software and system that were validated,

– a description of the validation tests performed (inputs, outputs, testing procedures),

– the tools and equipment used to validate or evaluate the results,

– the results showing whether each validation test was a success or failure,

– a validation assessment: identified non-conformities, impact on safety, decision as to whether or not to accept the validation.

A validation report should be made available for each delivered software version and should correspond to the final version of each delivered software element.

NOTE This report can be used to provide proof that tests were indeed carried out, and that the results were correct (or contained explainable deviations). It can also be used to redo tests at a later date, for a future software version or for another project. It provides a guarantee that each delivered version has been validated in its final form. On the other hand, it does not impose a complete validation of each modification of an existing code – an impact analysis can, in certain cases, justify partial validation.

D.9.3 Software design verification: software integration tests

This verification focuses on the correct assembly of software modules and on the mutual relationships between software components. It can be used to reveal errors of the following kind: incorrect initialization of variables and constants, errors in the transfer of parameters, any data alteration, especially global data, incorrect sequencing of events and operations.

Software integration tests should be able to verify:

– correct sequencing of the software execution,

– exchange of data between modules,

– respect of the performance criteria,

– non-alteration of global data.

The test coverage should be given explicitly in a traceability matrix demonstrating the correspondence between the tests to be undertaken and the objectives of the tests defined. Integration test results should be recorded in a software integration test report, which should, as a minimum, contain the following points:

– version of the integrated software;
– description of the tests performed (inputs, outputs, procedures);
– integration tests results and their evaluation.

D.9.4 Detailed design verification: module tests

Module tests focus on software modules and their conformity with the detailed design. This activity can be indispensable for large and complex software elements, but is only recommended for the relatively small software elements dealt with here. This phase of the verification procedure allows detection of the following types of errors:

– inability of an algorithm to satisfy software specifications,
– incorrect loop operations,
– incorrect logical decisions,
– inability to compute valid combinations of input data correctly,
– incorrect responses to missed or altered input data,
– violation of array boundaries,
– incorrect calculation sequences,
– inadequate precision,
– accuracy or performance of an algorithm.

Each software module should be submitted to a series of tests to verify, using input data, that the module fulfils the functions specified at the detailed design stage.

The test coverage should be provided in a traceability matrix that demonstrates the correspondence between the test results and the objectives of the tests defined.

Annex E
(informative)

Information for the assessment of safety functions

E.1 General

This Annex E provides a list of documents that should be reviewed by an assessor during the conformity assessment process.

It is understood that in case of conformity assessment made by an independent organisation (e.g. a third party test institution) with a specific and well-defined conformity assessment process, this process may take precedence over the information of this Annex E.

In case of self-assessment, it is highly recommended to comply with the information of this Annex E.

E.2 Documentation management

The documentation provided during the entire development lifecycle should be developed and updated.

All documents should be marked with at least the following information:

– title and name of the document,
– name of the editor,
– date of preparation or modification,
– revision index.

The documentation should be:

– accurate and concise
– be easily understood by those persons having to make use of it
– suit the purpose for which it is intended
– be accessible and maintainable

All the relevant documentation should be revised, amended and approved under the control of an appropriate documentation control scheme.

E.3 Documentation provided for conformity assessment

The documents listed in Table E.1 should be provided during the assessment review, unless otherwise specified:

Table E.1 – Documentation to be provided

Tasks	Reference to clause	Reference to IEC 61508
IMD and IFLS design requirements specification	7.2	Parts 1 to 6
Functional safety plan	7.3.2	Parts 1 to 6
Specification of functional safety requirements, including: – selection of safety functions among the safety functions defined in IEC 61557-15 – selection of the relevant safety integrity level (SIL)	Clause 4 7.2.1 7.4.5	Parts 0 to 7
Provisions for the development of the selected safety functions	7.2.2	Parts 0, 1, 3, 6, 7
Verification plan for the development of selected safety functions	7.2.3	Parts 1 to 6
Validation plan for the development of selected safety functions	7.2.4	Parts 1 to 6
Planning of commissioning, installation and setting into operation	7.2.5	Parts 1 to 6
Planning of the user documentation	7.2.6	Parts 2, 6, 7
Requirements for design and development	7.4	Parts 1, 2, 3, 7
Design standards	7.4.2	
Realization	7.4.3	Parts 1, 2, 3, 7
Safety integrity and fault detection	7.4.4	Parts 1, 2, 3, 5, 6, 7
Safety integrity level (SIL) assignment	7.4.5	Parts 1, 2, 3, 5, 6, 7
Hardware requirements	7.4.6	Parts 0,1 2, 5
Software requirements	7.4.7	Part 3
Review of requirements	7.4.8	Parts 1, 2, 3, 6, 7
Requirements for the probability of dangerous failure on demand (PFD)	7.4.9	Parts 1, 6
Failure rate data	7.4.10	Part 2
Diagnostic test interval	7.4.11	Parts 2, 6, 7
Architectural constraints	7.4.12	Parts 2, 3
Estimation of safe failure fraction (SFF)	7.4.13	Part 2
Requirements for systematic safety integrity	7.4.14	Parts 1, 2, 3, 5, 6
IMD and IFLS safety validation	7.7	Part 2
EMC requirements	7.7.5	Parts 1, 2, 7
Information for the assessment of safety functions	Annex E	Parts 1, 2, 3, 7
Documentation management	Clause E.2	Parts 1, 2, 3, 7
Documentation provided for conformity assessment	Clause E.3	Part 1
Documentation of the development lifecycle	Clause E.4	Part 1
Design documentation	Clause E.5	Part 1
Documentation of verification and validation	Clause E.6	Part 1, 3
Test documentation	Clause E.7	Part 1
Documentation of modifications	Clause E.8	Part 1, 3
Information for use	Clause E.9	Part 1
IMD and IFLS safety validation	7.7	Parts 1 to 7
Test	7.7.2	Parts 1 to 7
Verification	7.7.3	Parts 1 to 7
Validation	7.7.4	Parts 1 to 7
Requirements for modifications, if any	Clause 8	Parts 1 to 7
Proven in use approach, if any	Clause 9	Parts 2, 3, 6, 7

E.4 Documentation of the development lifecycle

The documentation should contain sufficient information for each phase of the development lifecycle and should be updated during the entire development lifecycle.

E.5 Design documentation

Besides the documentation of the design and realization, the IMD or IFLS design documentation should indicate those techniques and measures used to achieve the desired SIL, for example failure mode and effects analysis (FMEA), fault tree analysis.

E.6 Documentation of verification and validation

Appropriate documentation concerning IMD and IFLS verification and validation should be developed, including:

– version(s) of the verification and validation plan(s) being used,
– safety function(s) under test (or analysis), along with the reference to the IMD or IFLS requirement(s) specified during safety verification and validation planning,
– tools and equipment used,
– results of each verification and validation.

E.7 Test documentation

During IMD and IFLS testing for safety functions, the following details should be documented:

– version of the test plan used,
– criteria for acceptance of tests,
– type and version of the IMD or IFLS being tested,
– tools and equipment used along with calibration data,
– conditions of the test,
– test personnel,
– detailed results of each test,
– any discrepancy between expected and actual results,
– conclusions of the test: either it has been passed or the reasons for failure.

E.8 Documentation of modifications

Appropriate documentation should be established and maintained for each IMD or IFLS modification activity. The documentation should include:

– the detailed specification of the modification,
– results of the impact analysis,
– all approvals for changes,
– test cases for components including revalidation data,
– IMD and IFLS configuration management history (hardware and software),
– deviation from previous operations and conditions,
– necessary changes to information for use,
– all applicable development steps according to 7.4.

E.9 Information for use

The information for use should be provided according to 7.6.4.

Annex F
(informative)

Example of applications

F.1 Overview

This informative Annex F includes examples of applications for IMDs and IFLSs where functional safety may be required.

The SIL level for the specific application depends on the functional safety assessment for the application which is based on a risk analysis.

F.2 Limitation in applications

Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4:2010), human factor requirements related to the design of E/E/PE safety-related systems are not considered in detail in IEC 61508 (see IEC 61508-1).

It is understood that a safety-related function cannot rely only on the reaction of a human being against a warning. The safety-related function shall take into account the effect of random human error if a person is required to take action to achieve the safety function. The design of the E/E/PE safety-related systems shall take into account human capabilities and limitations and be suitable for the actions assigned to operators and maintenance staff (see IEC 61508-2).

IEC 61557-15 will take into account safety functions involving human reaction, on the conditions that:

– at least one person is supposed to be present when the alarm occurs, e.g. in the operating theatre of a hospital (both surgeon and nurse are supposed to be present);
– the reaction of a human person facing an alarm is part of a well-defined alarming management process, e.g. a facility manager is supposed to be available on request.

F.3 Typical applications covered by IEC 61557-15

F.3.1 General

In Figure F.1 to Figure F.9, the dotted lines indicate the functional links. They can represent either an internal connection or an external connection; they can represent digital signals, communication signals or a combination of these signals.

F.3.2 Local alarming

The local alarming in Figure F.1 is based on the systematic presence of a skilled person and on a well-defined alarming management process.

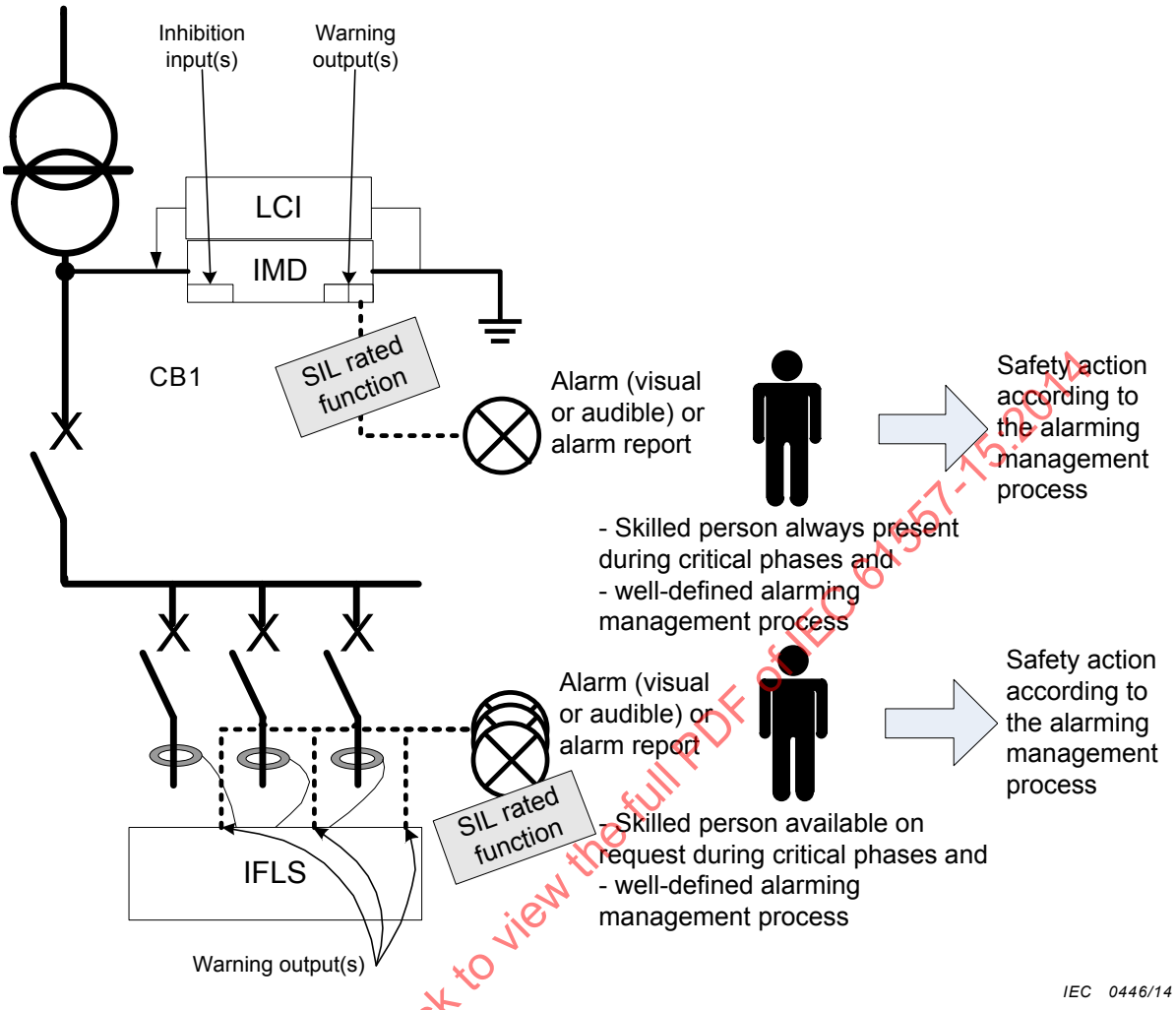


Figure F.1 – Local alarming, based on the systematic presence of one person and based on a well-defined alarming management process

In case of insulation fault detection, the relevant skilled person takes the actions in accordance with the well-defined alarming management process.

Risk covered: occurrence of a second fault, meaning a tripping of the protective device and the loss of power supply in the following application:

– hospitals where the continuity of supply is critical for safety reasons.

NOTE Switch CB1 is not applicable in hospital applications.

F.3.3 Local transformer monitoring warning

The local transformer monitoring in Figure F.2 warning is based on the systematic presence of a skilled person, and on a well-defined alarming management process.

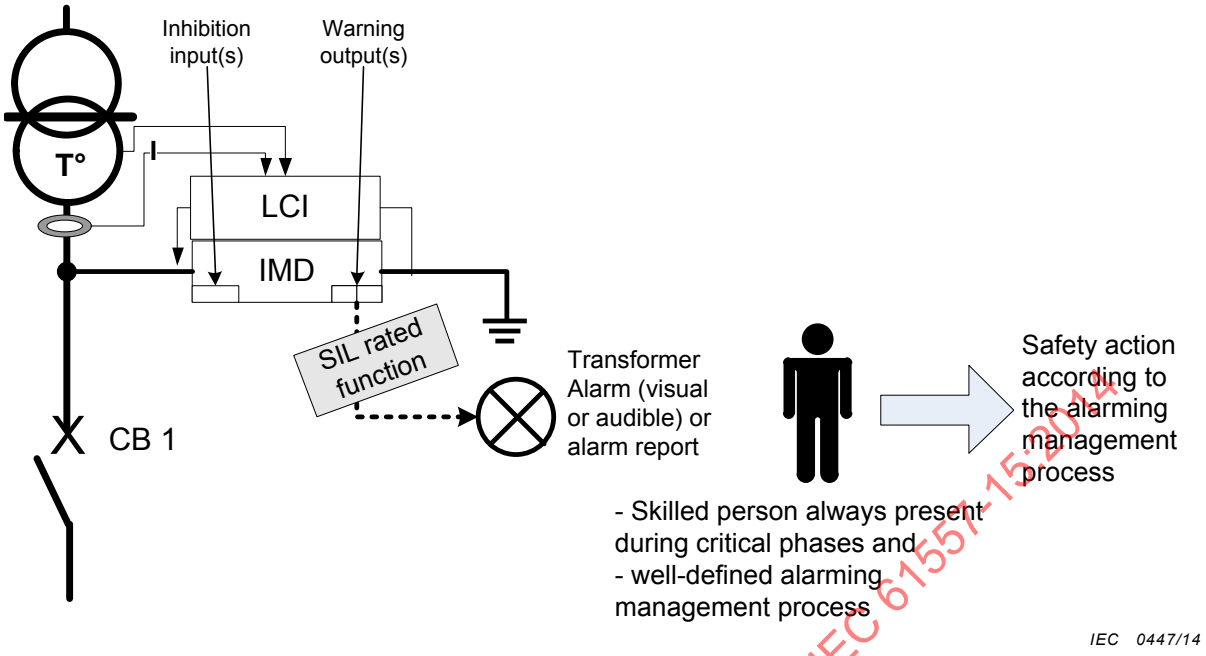


Figure F.2 – Local transformer monitoring warning, based on the systematic presence of a skilled person, and based on a well-defined alarming management process

In case of IT transformer overload, safety actions need to be taken.

Risk covered: Upcoming failure of the IT transformer with a consequent loss of power supply in the following application:

– hospitals where the continuity of supply is critical for safety reasons.

NOTE Switch CB1 is not applicable in hospital applications.

F.3.4 Alarming and processing of remote insulation warning and/or remote location warning

Figure F.3 shows the alarming and processing of the remote insulation warning and/or the remote location warning in a supervisory control system.

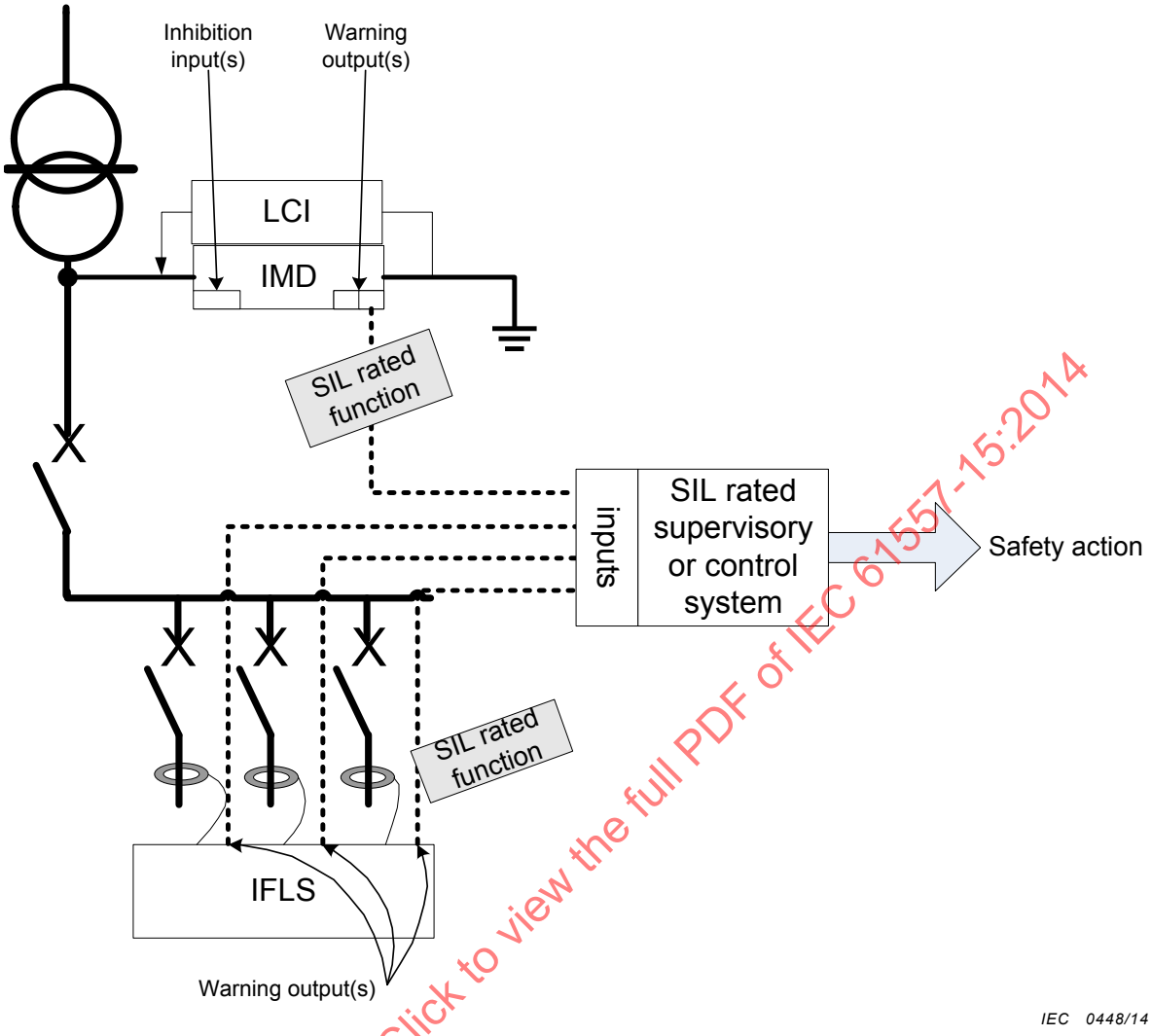


Figure F.3 – Alarming and processing of the remote insulation warning and/or the remote location warning in a supervisory control system

Risks covered: Risks in case of a first or second insulation fault which depend on the functional safety of the entire system.

Applications:

– railway signalling systems, where insulation faults can lead to failures in the signalling and where the reaction to insulation faults depends on the risk analysis for the system;
– control systems for critical processes where functional safety is required for the control system and where the reaction to insulation faults depends on the risk analysis for the system (e.g. control circuits for critical chemical processes);
– main circuits for critical loads where functional safety is required for the monitoring devices, e.g. shipboard power supply systems, variable frequency drives (VFD) in safety critical applications, supply systems on oil drilling platforms.

F.3.5 Automatic disconnection of the complete IT system in case of a first insulation fault

Figure F.4 shows the case of an automatic disconnection of the complete IT system when a first insulation fault is detected.

Figure F.5 shows the case of insulation fault detection which is related to a first threshold where warning information is issued. In case the second threshold is met, the complete IT system is disconnected.

Risk covered: Occurrence of a second fault, meaning a tripping of the protective device and possibly an electric arc.

Applications:

– mines, chemistry, where an electric arc may cause an explosion involving human risks;
– photovoltaic applications where the fault current may create fire involving severe damages;
– all applications where the non-detection of an insulation fault is critical,
– low-voltage generating sets.

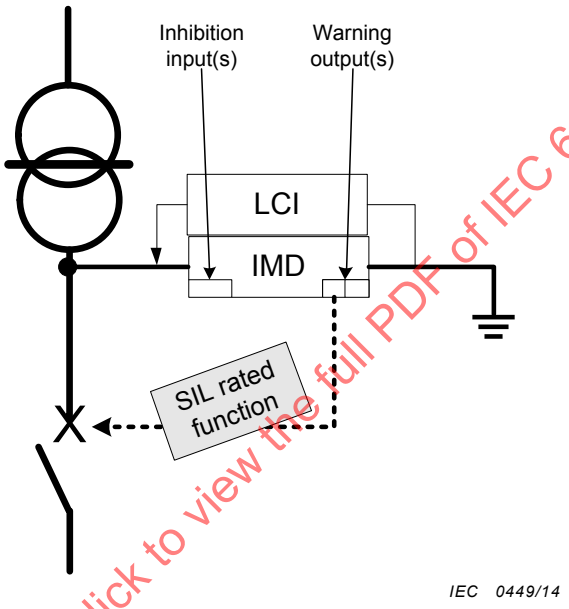


Figure F.4 – Disconnection of the complete IT system in case of insulation fault detection

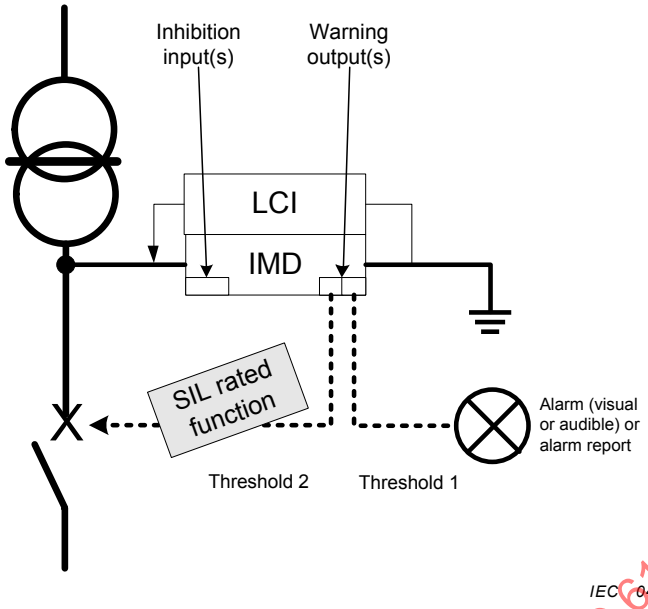


Figure F.5 – Threshold 1 warning information and threshold 2 disconnection of the complete IT system in case of an insulation fault detection

F.3.6 Automatic disconnection of an IT system sub-network

Figure F.6 and Figure F.7 show the automatic disconnection of the sub-network of an IT system in case of a first insulation fault.

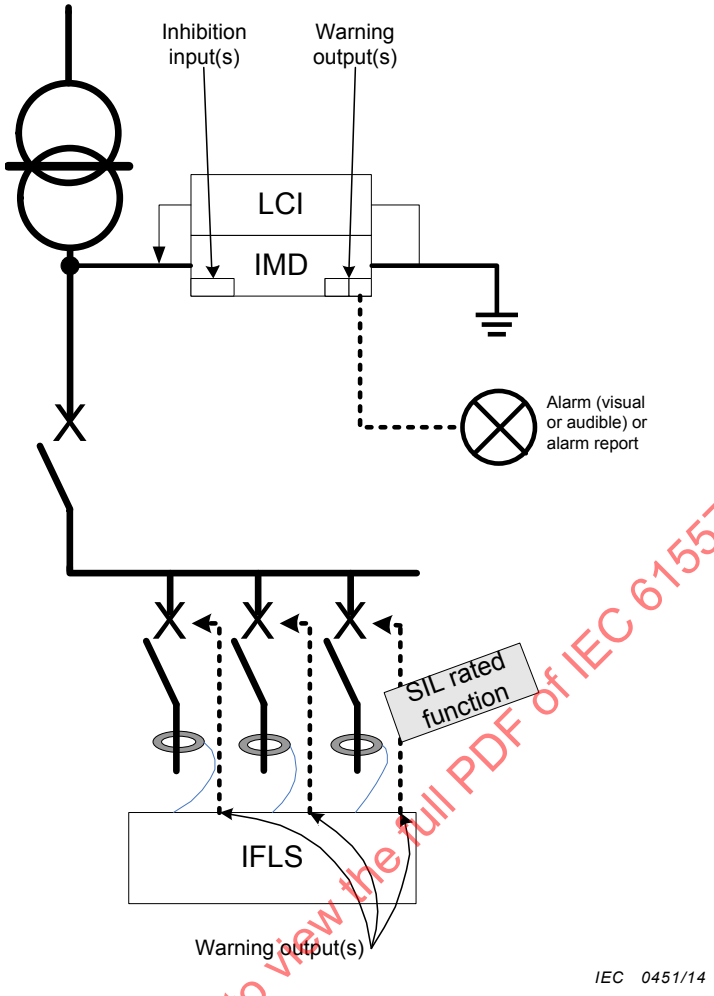


Figure F.6 – Automatic disconnection of a faulty feeder via direct signal from the IFLS

In case of insulation fault detection, the faulty feeder is automatically disconnected via a signal from the IFLS. Here, there is no automatic disconnection of the complete IT system (the IMD should not disconnect the complete system).

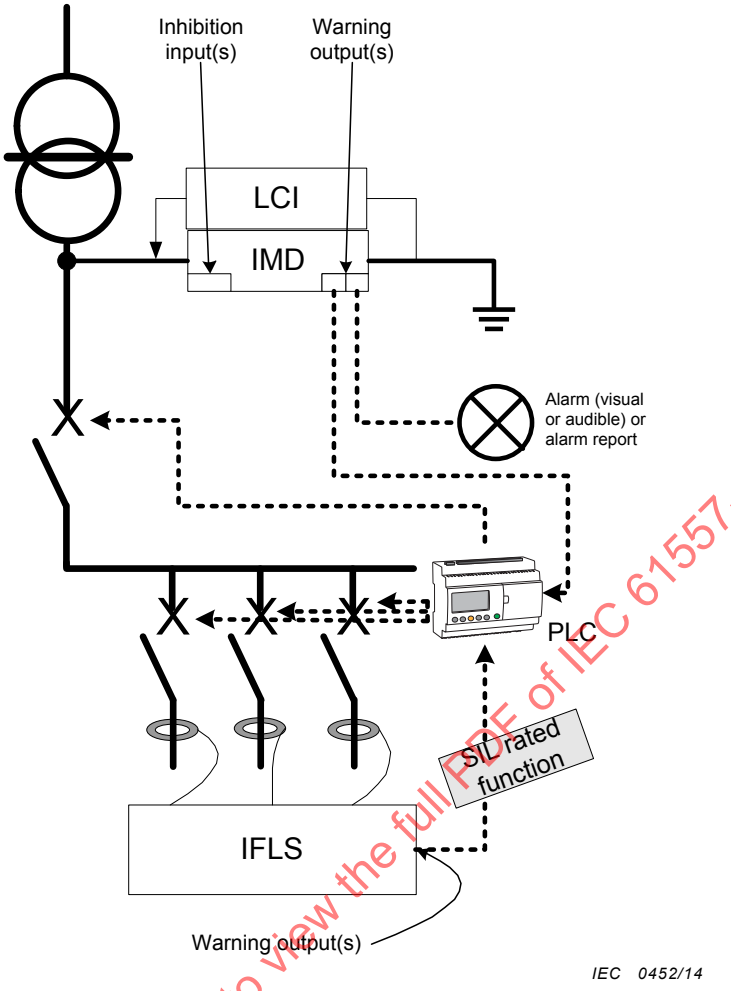


Figure F.7 – Automatic disconnection of a faulty feeder via a PLC

In case of insulation fault detection, the faulty feeder is automatically disconnected via a PLC. Optionally, the PLC can also manage the disconnection of the complete IT system.

Risks covered in Figure F.6 and Figure F.7: Disconnection of the complete IT system before an accident happens with potential human impact.

Applications:

– critical processes where it is better to stop a part of the process rather than stopping the full process.

F.3.7 Management of multiple source system (two incomers or of incomer plus generator)

Figure F.8 shows the management of a multiple source system and with two incomers or with one incomer plus generator.

In the case where two incomers are working at the same time, it may be necessary to disable one of the two IMD in the network. If this is not done, the two IMDs may interfere and dysfunction.

Risks covered: In some situations, two IMDs may be working at the same time causing the two IMDs to interfere and not monitor the IT system correctly. This may lead to a first fault which is not detected by the IMD and a following second fault which is tripping a protective device (RCD) and may cause an electric arc.

Applications are:

– mines, chemistry, where an electric arc may cause an explosion involving human risks,
– photovoltaic applications where fault current may create fire involving severe damages,
– all applications where the non-detection of an insulation fault is critical,
– low-voltage generating sets.

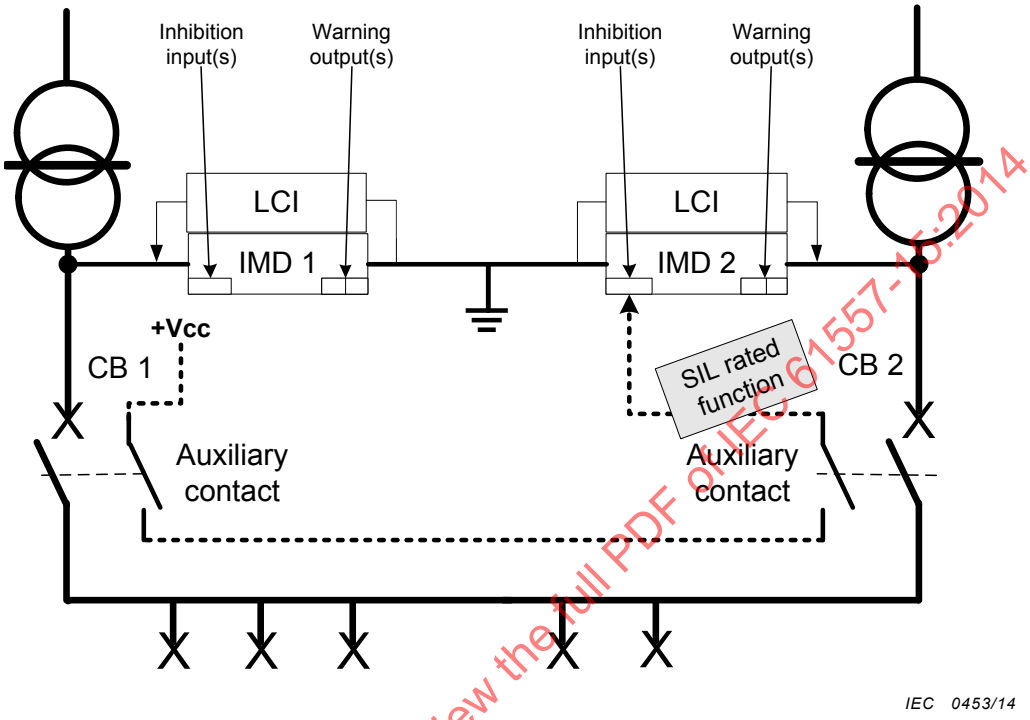


Figure F.8 – Management of multiple source systems (two incomers or of one incomer plus generator)

F.3.8 Management of multiple source systems (two incomers or of incomer plus generator – with a load shedder)

Figure F.9 shows the management of multiple source systems with a load shedder of two incomers or one incomer plus generator.

In the case where two incomers are working at the same time, it is necessary to disable one of the two IMDs on the network. If this is not done, the two IMDs may interfere and dysfunction.

In Figure F.9, IMD 2 is inhibited when circuit-breakers CB1, CB2 and CB3 are closed.

Risks covered: In some situations, two IMDs may be working at the same time causing the two IMDs to interfere and not monitor the IT system correctly. This may lead to a first fault which is not detected by the IMD and a following second fault which is tripping a protective device (RCD) and may cause an electric arc.

Applications are:

– mines, chemistry, where an electric arc may cause an explosion involving human risks,
– photovoltaic applications where fault current may create fire involving severe damages,
– all applications where the non-detection of an insulation fault is critical,
– low-voltage generating sets.

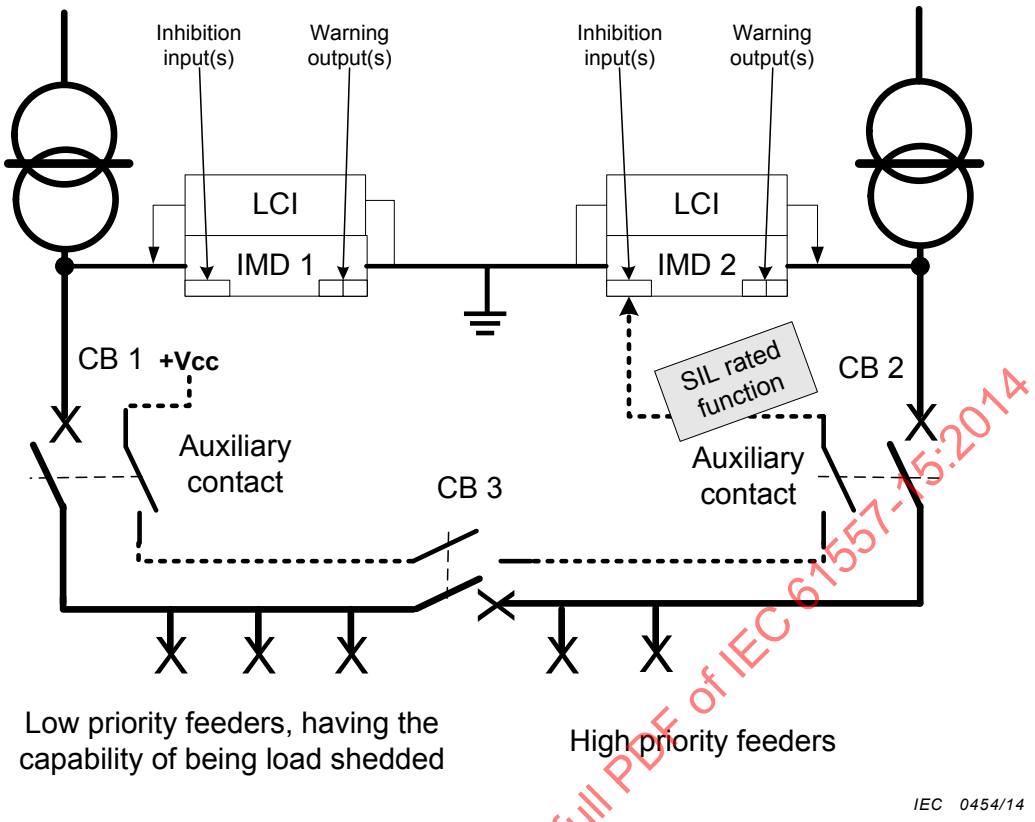


Figure F.9 – Management of multiple source system (two incomers or of one incomer plus generator, with a load shedder)

Bibliography

IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 60319:1999, *Presentation and specification of reliability data for electronic components*

IEC 60335-1:2006, *Household and similar electrical appliances – Safety – Part 1: General requirements*

IEC 60364-4-41:2005, *Low voltage electrical installations – Part 4-41: Protection for safety – Protection against electric shock*

IEC 60364-5-53:2002, *Low voltage electrical installations – Part 5-53: Selection and erection of electrical equipment – Protection, isolation, switching, control and monitoring*

IEC 60364-5-55: 2010, *Low voltage electrical installations – Part 5-55: Selection and erection of electrical equipment – other equipment – Clause 557: Auxiliary circuits*

IEC 60364-7-710:2002, *Low voltage electrical installations – Part 7-710: Requirements for special installations or locations – Medical locations*

IEC 60730-1:2010, *Automatic electrical controls for household and similar use – Part 1: General requirements*

IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61010-1:2010, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 1: General requirements*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety – related systems – Part 7: Overview of techniques and measures*

IEC 61709:1996, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 61784-3:2007, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61800-5-2:2007, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

IEC 62280-1:2010, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62380:2004, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

IEC Guide 109:2003, *Environmental aspects – Inclusion in electrotechnical product standards*

IEC Guide 116:2010, *Guidelines for safety related risk assessment and risk reduction for low voltage equipment*

ISO/IEC 31010:2009, *Risk Management – Risk assessment techniques*

ISO 6469:2010, *Electrically propelled road vehicles – Safety specifications – Part 3: Protection of persons against electric shock*

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

UL 1998:2000, *Software in programmable components*

SOMMAIRE

AVANT-PROPOS 80
INTRODUCTION 82
1 Domaine d'application 84
2 Référence normatives 84
3 Termes, définitions et abréviations 85
3.1 Termes et définitions 85
3.2 Abréviations 97
4 Définition des fonctions de sécurité intégrées dans les CPI et les DLD 98
4.1 Généralités 98
4.2 Définition des fonctions de sécurité 98
4.2.1 Alarme locale de défaut d'isolation (LIW) 98
4.2.2 Alarme distante de défaut d'isolation (RIW) 99
4.2.3 Alarme locale de localisation de défaut (LLW) 99
4.2.4 Alarme distante de localisation de défaut (RLW) 99
4.2.5 Commande distante d'activation/désactivation (REDC) 100
4.2.6 Alarme locale de surveillance du transformateur (LTMW) 100
5 Exigences applicables aux produits réalisant des fonctions relatives à la sécurité 101
5.1 Exigences applicables aux fonctions non relatives à la sécurité 101
5.2 Exigences de performance supplémentaires pour des produits mettant en œuvre des fonctions de sécurité 101
5.2.1 Généralités 101
5.2.2 Exigences de performance supplémentaires pour des CPI conformes au SIL 1 ou SIL 2 101
5.2.3 Exigences de performance supplémentaires pour des DLD conformes au SIL 1 ou SIL 2 101
6 Gestion de la sécurité fonctionnelle au cours du cycle de vie de développement 102
6.1 Gestion de la sécurité fonctionnelle pour le réseau IT 102
6.2 Utilisation des CPI et des DLD dans des réseaux IT 102
6.3 Cycle de vie de sécurité des CPI et des DLD en phase de réalisation 103
7 Gestion de la sécurité fonctionnelle au cours du cycle de vie de réalisation des CPI et des DLD 103
7.1 Généralités 103
7.2 Spécification des exigences de conception des CPI et des IFL (phase 10.1) 104
7.2.1 Spécification des exigences de sécurité fonctionnelle 104
7.2.2 Dispositions pour le développement de fonctions de sécurité 105
7.2.3 Plan de vérification du développement des fonctions de sécurité 105
7.2.4 Plan de validation du développement des fonctions de sécurité 105
7.2.5 Planification de la mise en service, de l'installation et de la mise en fonctionnement 106
7.2.6 Planification de la documentation utilisateur 106
7.3 Planification de la validation de la sécurité des CPI et des DLD (phase 10.2) 106
7.3.1 Généralités 106
7.3.2 Plan de sécurité fonctionnelle 106
7.4 Conception et développement des CPI et des DLD (phase 10.3) 107

7.4.1 Généralités 107
7.4.2 Normes de conception 107
7.4.3 Réalisation 108
7.4.4 Intégrité de sécurité et détection d'anomalie 108
7.4.5 Attribution du niveau d'intégrité de sécurité (SIL) 108
7.4.6 Exigences relatives au matériel 108
7.4.7 Exigences relatives au logiciel 109
7.4.8 Revue des exigences 109
7.4.9 Exigences relatives à la probabilité de défaillance dangereuse en cas de sollicitation (PFD) 109
7.4.10 Données relatives aux taux de défaillance 110
7.4.11 Intervalle entre essais de diagnostic 111
7.4.12 Contraintes architecturales 111
7.4.13 Estimation de la proportion de défaillances en sécurité (SFF) 113
7.4.14 Exigences relatives à l'intégrité de sécurité systématique 113
7.5 Intégration des CPI et des DLD (phase 10.4) 116
7.5.1 Intégration du matériel 116
7.5.2 Intégration du logiciel 116
7.5.3 Modifications en cours d'intégration 116
7.5.4 Essais d'intégration 116
7.6 Documentation des CPI et DLD relative aux procédures d'installation, de mise en service, d'exploitation et de maintenance (phase 10.5) 117
7.6.1 Généralités 117
7.6.2 Spécification fonctionnelle 117
7.6.3 Informations concernant la conformité 117
7.6.4 Informations de mise en service, d'installation, de mise en fonctionnement, d'exploitation et de maintenance 117
7.7 Validation de la sécurité des CPI et DLD (phase 10.6) 118
7.7.1 Généralités 118
7.7.2 Essais 118
7.7.3 Vérification 119
7.7.4 Validation 119
7.7.5 Exigences CEM 119
8 Exigences applicables aux modifications 120
8.1 Généralités 120
8.2 Demande de modification 120
8.3 Analyse d'impact 120
8.4 Autorisation 120
9 Approche "efficacité éprouvée par une utilisation antérieure" 120
Annexe A (informative) Analyse du risque et attribution du SIL aux CPI et DLD 121
A.1 Généralités 121
A.2 Attribution du SIL aux CPI et aux DLD 123
A.3 Exemple de graphique de risque 124
A.4 Méthode alternative d'attribution du SIL – méthode quantitative 126
Annexe B (informative) Exemples de détermination de la PFD, de la DC et de la SFF 127
B.1 Généralités 127
B.2 Exemples d'architectures des CPI et des DLD 128
Annexe C (informative) Bases de données de taux de défaillance 129
C.1 Généralités 129

C.2 Références de taux de défaillance dans les normes actuelles 129
Annexe D (informative) Guide pour la conception et le développement de logiciels intégrés 130
D.1 Généralités 130
D.2 Lignes directrices relatives aux éléments logiciels 130
D.2.1 Généralités 130
D.2.2 Interface avec l'architecture système 130
D.2.3 Spécifications du logiciel 131
D.2.4 Logiciel préexistant 131
D.2.5 Conception du logiciel 132
D.2.6 Codage 132
D.3 Lignes directrices relatives au processus de développement du logiciel 132
D.3.1 Processus de développement: cycle de vie du logiciel 132
D.3.2 Documentation: gestion de la documentation 133
D.3.3 Gestion de la configuration et des modifications du logiciel 133
D.3.4 Gestion de la configuration et de l'archivage 133
D.3.5 Gestion des modifications du logiciel 134
D.4 Outils de développement 134
D.5 Reproduction de la production du code exécutable 134
D.6 Vérification et validation du logiciel 135
D.7 Lignes directrices générales relatives à la vérification et à la validation du logiciel 135
D.8 Revue de vérification et de validation 135
D.9 Essais du logiciel 136
D.9.1 Lignes directrices générales relatives à la vérification et à la validation du logiciel 136
D.9.2 Vérification de la spécification du logiciel: essais de validation 136
D.9.3 Vérification de la conception du logiciel: essais d'intégration du logiciel 137
D.9.4 Vérification de la conception détaillée: essais des modules 137
Annexe E (informative) Informations concernant l'évaluation des fonctions de sécurité 139
E.1 Généralités 139
E.2 Gestion de la documentation 139
E.3 Documentation fournie pour évaluation de la conformité 139
E.4 Documentation relative au cycle de vie de développement 141
E.5 Documentation relative à la conception 141
E.6 Documentation de la vérification et de la validation 141
E.7 Documentation d'essai 141
E.8 Documentation des modifications 142
E.9 Informations pour l'utilisation 142
Annexe F (informative) Exemples d'applications 143
F.1 Vue d'ensemble 143
F.2 Limites des applications 143
F.3 Applications types couvertes par la CEI 61557-15 143
F.3.1 Généralités 143
F.3.2 Déclenchement d'une alarme locale 143
F.3.3 Alarme locale de surveillance du transformateur 144
F.3.4 Déclenchement d'alarme et traitement d'une alarme distante de défaut d'isolation et/ou d'une alarme distante de localisation de défaut 145

F.3.5 Déconnexion automatique de l'ensemble du réseau IT en cas de premier défaut d'isolement 147
F.3.6 Déconnexion automatique d'un sous-réseau IT 148
F.3.7 Gestion de systèmes à sources multiples (deux arrivées ou une arrivée plus un générateur) 150
F.3.8 Gestion de systèmes à sources multiples (deux arrivées ou une arrivée plus un générateur – avec un dispositif de délestage) 151
Bibliographie 153

Figure 1 – Rapport entre la CEI 61557-15 et les normes apparentées 82
Figure 2 – Cycle de vie de sécurité global applicable à un réseau IT 102
Figure 3 – Cycle de vie de sécurité des CPI et des DLD (en phase de réalisation) 103
Figure A.1 – Éléments fonctionnels d'un réseau IT et leur rapport avec les définitions et abréviations de la série de normes CEI 61508 121
Figure A.2 – Exemple de graphique de risque 125
Figure B.1 – Organigramme de détermination de la PFD, de la DC et de la SFF 128
Figure F.1 – Déclenchement d'une alarme locale, fondé sur la présence systématique d'une personne et sur un processus bien défini de gestion des alarmes 144
Figure F.2 – Alarme locale de surveillance du transformateur, fondée sur la présence systématique d'une personne qualifiée et sur un processus bien défini de gestion des alarmes 145
Figure F.3 – Déclenchement d'alarme et traitement de l'alarme distante de défaut d'isolation et/ou de l'alarme distante de localisation de défaut dans un système de commande de surveillance 146
Figure F.4 – Déconnexion de l'ensemble du réseau IT en cas de détection d'un défaut d'isolement 147
Figure F.5 – Information d'avertissement (seuil 1) et déconnexion (seuil 2) de l'ensemble du réseau IT en cas de détection d'un défaut d'isolement 148
Figure F.6 – Déconnexion automatique d'une alimentation défectueuse par l'intermédiaire d'un signal direct en provenance de l'DLD 149
Figure F.7 – Déconnexion automatique d'une alimentation défectueuse par l'intermédiaire d'un automate programmable 150
Figure F.8 – Gestion de systèmes à sources multiples (deux arrivées ou une arrivée plus un générateur) 151
Figure F.9 – Gestion de système à sources multiples (deux arrivées ou une arrivée plus un générateur- avec un dispositif de délestage) 152

Tableau 1 – Abréviations avec référence 97
Tableau 2 – Niveaux d'intégrité de sécurité (SIL) et probabilité d'une défaillance dangereuse en cas de sollicitation (PFD) des CPI et des DLD 104
Tableau 3 – Intégrité de sécurité du matériel: contraintes architecturales sur les sous-systèmes relatifs à la sécurité de type A et de type B 112
Tableau A.1 – Analyse du risque d'un réseau IT 122
Tableau A.2 – Attribution des SIL aux CPI et aux DLD 123
Tableau A.3 – Relation entre réduction minimale du risque et SIL 125
Tableau A.4 – Exemple de classement selon le graphique du risque de la Figure A.1 126
Tableau E.1 – Documentation à fournir 140

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ ÉLECTRIQUE DANS LES RÉSEAUX DE DISTRIBUTION BASSE TENSION DE 1 000 V C.A. ET 1 500 V C.C. – DISPOSITIFS DE CONTRÔLE, DE MESURE OU DE SURVEILLANCE DE MESURES DE PROTECTION –

Partie 15: Exigences de sécurité fonctionnelle pour les contrôleurs d'isolement de réseaux IT et les dispositifs de localisation de défauts d'isolement pour réseaux IT

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 61557-15 a été établie par le comité d'études 85 de la CEI: Équipements de mesure des grandeurs électriques et électromagnétiques.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
85/465/FDIS	85/470/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

La présente partie de la CEI 61557 doit être utilisée conjointement aux Parties 8 et 9.

Une liste de toutes les parties de la série CEI 61557, présentées sous le titre général *Sécurité électrique dans les réseaux de distribution basse tension de 1 000 V c.a. et 1 500 V.c.c. – Dispositifs de contrôle, de mesure ou de surveillance de mesures de protection*, 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

La CEI 61508 traite de la sécurité fonctionnelle, un sujet d'une importance primordiale pour les systèmes relatifs à la sécurité. La sécurité fonctionnelle peut être applicable aux réseaux IT lorsque la sécurité est fondée sur des contrôleurs d'isolement (CPI) et des systèmes de localisation de défauts d'isolement (DLD), ainsi que d'autres mesures complémentaires relatives à la sécurité (par exemple, des disjoncteurs).

Les contrôleurs d'isolement et les systèmes de localisation de défauts d'isolement comportent des composants électriques et électroniques et peuvent comprendre des logiciels intégrés.

Les exigences applicables à ces dispositifs sont définies dans les normes CEI 61557-8 et CEI 61557-9. Ces normes donnent des exigences élémentaires qu'il est nécessaire de prendre en compte pour l'approche "sécurité fonctionnelle" de la CEI 61557-15, mais ne couvrent pas toute la gamme d'exigences qui doivent être satisfaites pour l'attribution d'un niveau défini de sécurité fonctionnelle et la validation correspondante.

La série de normes internationales CEI 61508 traite des aspects fondamentaux à prendre en compte lorsque des systèmes électriques et électroniques sont utilisés pour réaliser des fonctions de sécurité. Un des principaux objectifs de cette série de normes est de faciliter l'élaboration de normes internationales d'applications ou de matériels par le comité d'études compétent. Ainsi, ce dernier pourra prendre pleinement en compte les exigences particulières de ces applications.

Il est admis qu'il existe une grande diversité d'applications de contrôleurs d'isolement et de systèmes de localisation de défauts d'isolement sur les réseaux IT. La présente partie de la CEI 61557 définit les fonctions de sécurité de base ainsi que les niveaux correspondants de sécurité fonctionnelle (SIL) et établit des mesures et principes de faisabilité permettant de développer et de valider ces dispositifs et systèmes du point de vue de la sécurité fonctionnelle.

La Figure 1 illustre les relations entre la CEI 61557-15 et les normes produit, sécurité et CEM pertinentes ainsi que ses liens avec la série de normes CEI 61508.

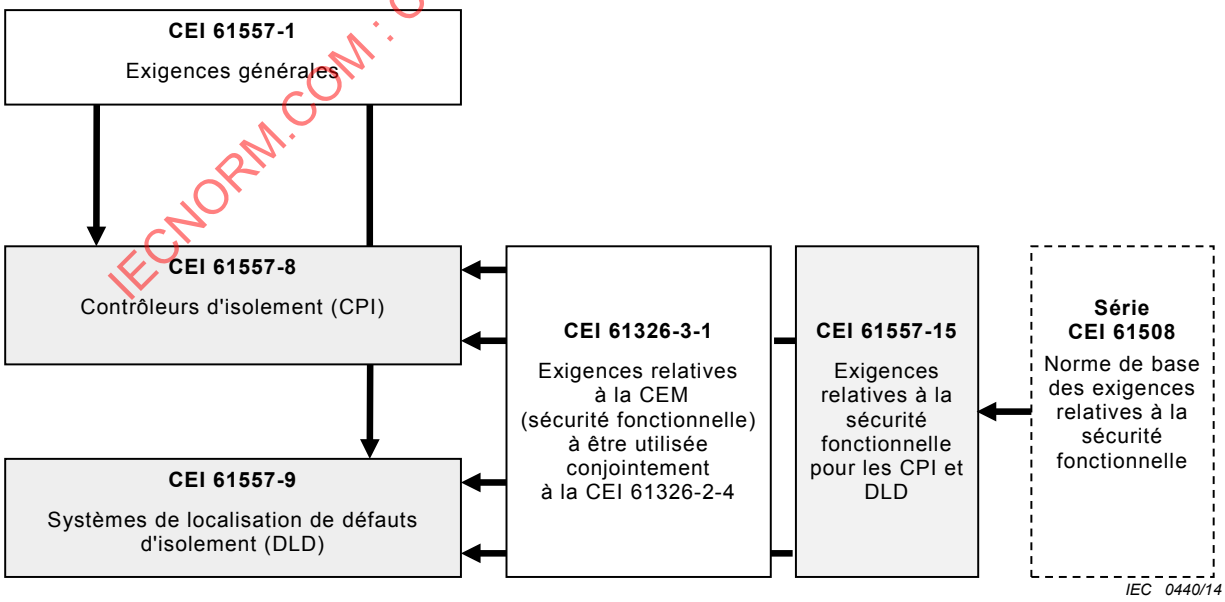


Figure 1 – Rapport entre la CEI 61557-15 et les normes apparentées

La présente partie de la CEI 61557 ne couvre pas les phases 1 à 9 et 11 à 16 de la CEI 61508-1 pour l'ensemble des réseaux IT. Plus particulièrement, la présente norme ne couvre pas l'utilisation des CPI et des DLD dans l'application client.

NOTE 1 Conformément à la CEI 61557-9, un système de localisation de défauts d'isolement (DLD) peut comprendre plusieurs dispositifs: un localisateur de défaut d'isolement (IFL), un injecteur de courant de localisation (LCI), un capteur de courant de localisation (LCS), un contrôleur d'isolement (CPI) conforme à la CEI 61557-8.

Les CPI et les DLD ne sont pas en général des dispositifs de protection, mais ils font partie des mesures de protection de réseaux IT. Les CPI et DLD fonctionnent en tant que surveillance permanente de la résistance d'isolement du réseau IT non relié à la terre et de localisation de défauts d'isolement n'importe où sur le réseau peuvent être perçus comme des fonctions de sécurité qui font partie des mesures de protection d'un réseau IT.

La présente partie de la CEI 61557 s'applique uniquement aux CPI et DLD qui mettent en œuvre des fonctions de sécurité correspondantes SIL 1 et SIL 2. La présente norme ne spécifie pas de niveaux SIL plus élevés, car, en général, ces niveaux ne sont pas exigés pour les CPI et DLD de réseaux IT.

La conformité des CPI ou DLD à la présente norme peut être requise lorsque la sécurité fonctionnelle est exigée dans l'application de réseaux IT correspondante. Cependant, de manière générale, elle ne stipule pas qu'il est exigé pour ces dispositifs un niveau défini de sécurité fonctionnelle conformément à la présente norme.

NOTE 2 Des exemples d'application pour lesquelles la sécurité fonctionnelle peut être demandée en fonction de l'analyse du risque sont:

– chimie,
– mines,
– milieu marin,
– hôpitaux,
– parcs photovoltaïques,
– systèmes de signalisation ferroviaire,
– systèmes de contrôle-commande (par exemple dans des centrales nucléaires),
– etc.

Des exemples d'applications types sont donnés en Annexe F.

SÉCURITÉ ÉLECTRIQUE DANS LES RÉSEAUX DE DISTRIBUTION BASSE TENSION DE 1 000 V C.A. ET 1 500 V C.C. – DISPOSITIFS DE CONTRÔLE, DE MESURE OU DE SURVEILLANCE DE MESURES DE PROTECTION –

Partie 15: Exigences de sécurité fonctionnelle pour les contrôleurs d'isolement de réseaux IT et les dispositifs de localisation de défauts d'isolement pour réseaux IT

1 Domaine d'application

La présente partie de la CEI 61557 spécifie les exigences relatives à la sécurité fonctionnelle; elle se fonde sur la série de normes CEI 61508 pour la réalisation de contrôleurs d'isolement (CPI) tels que spécifiés dans la CEI 61557-8 et de systèmes de localisation de défauts d'isolement (DLD) conformes à la CEI 61557-9 et à la phase 10 du cycle de vie de la CEI 61508-1. Ces dispositifs assurent des fonctions relatives à la sécurité pour des réseaux IT.

La présente partie de la CEI 61557:

– traite uniquement des exigences de sécurité fonctionnelle visant à réduire le risque fonctionnel lors de l'utilisation des CPI et des DLD;
– se limite aux risques résultant directement du dispositif proprement dit ou de plusieurs dispositifs CPI ou DLD collaborant au sein d'un réseau donné;
– vise à définir les fonctions de sécurité de base assurées par les dispositifs.

La présente partie de la CEI 61557:

– ne traite pas de la sécurité électrique selon la CEI 61010-1 et des exigences des normes CEI 61557-8 et CEI 61557-9;
– ne couvre pas l'analyse des dangers et des risques d'un usage particulier de l'CPI ou de l'DLD;
– n'identifie pas toutes les fonctions de sécurité de l'application où l'CPI ou l'DLD est utilisé;
– ne couvre pas le processus de fabrication de l'CPI ou de l'DLD.

Les exigences de sécurité fonctionnelle dépendent de l'application et il convient d'en tenir compte dans le cadre de l'appréciation globale du risque de l'application spécifique. Le fournisseur des CPI et des DLD n'est pas responsable de l'application qui en est faite. Le concepteur de l'application est responsable de l'appréciation du risque et il lui incombe de spécifier les exigences globales de sécurité fonctionnelle de l'ensemble du réseau IT et il convient qu'il sélectionne le niveau de sécurité fonctionnelle (SIL) de l'CPI et/ou de l'DLD lorsque leur fonction de sécurité fait partie de l'évaluation de la sécurité fonctionnelle du réseau IT.

2 Référence 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 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 concernant 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 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

CEI 61508-6:2010, *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 61557-1, *Sécurité électrique dans les réseaux de distribution basse tension de 1 000 V c.a. et 1 500 V c.c. – Dispositifs de contrôle, de mesure ou de surveillance de mesures de protection – Partie 1: Exigences générales*

CEI 61557-8, *Sécurité électrique dans les réseaux de distribution basse tension de 1 000 V c.a. et 1 500 V c.c. – Dispositifs de contrôle, de mesure ou de surveillance de mesures de protection – Partie 8: Contrôleurs d'isolement pour réseaux IT*

CEI 61557-9:2009, *Sécurité électrique dans les réseaux de distribution basse tension de 1 000 V c.a. et 1 500 V c.c. – Dispositifs de contrôle, de mesure ou de surveillance de mesures de protection – Partie 9: Dispositifs de localisation de défauts d'isolement pour réseaux IT*

CEI 61326-2-4:2012, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 2-4: Exigences particulières – Configurations d'essai, conditions de fonctionnement et critères de performance pour les contrôleurs d'isolement conformes à la CEI 61557-8 et pour les dispositifs de localisation de défaut d'isolation conformes à la CEI 61557-9*

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*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les définitions données dans la CEI 61557-1, la CEI 61557-8 et la CEI 61557-9 ainsi que les suivantes s'appliquent.

3.1.1
danger
source potentielle de dommage

Note 1 à l'article: Ce terme comprend le danger sur des personnes survenant dans un laps de temps très court (par exemple, feu et explosion), mais aussi le danger à long terme sur la santé d'une personne (par exemple, dégagement d'une substance toxique).

[SOURCE: ISO/CEI Guide 51:1999, 3.5, modifiée – La note a été adaptée.]

3.1.2
danger électrique
source potentielle de dommage due à la présence d'énergie électrique dans une installation ou un matériel électrique

[SOURCE: CEI 60050-651:1999, 651-01-30, modifiée – La note a été supprimée.]

3.1.3
situation dangereuse
situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs dangers

[SOURCE: CEI 61508-4:2010, 3.1.3]

3.1.4
événement dangereux
événement susceptible de conduire à un dommage

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés aux conséquences de l'événement dangereux et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence.

[SOURCE: CEI 61508-4:2010, 3.1.4]

3.1.5
événement préjudiciable
événement préjudiciable dangereux
situation dangereuse ou événement dangereux qui conduit à un dommage

Note 1 à l'article: Adapté du Guide 'ISO/CEI 51:1999, 3.4, pour tenir compte d'un événement dangereux.

[SOURCE: CEI 61508-4:2010, 3.1.5]

3.1.6
risque
combinaison de la probabilité d'un dommage et de sa gravité

[SOURCE: Guide ISO/CEI 51:1999, 3.2]

3.1.7
risque tolérable
risque accepté dans un certain contexte et fondé sur les valeurs admises par la société

Note 1 à l'article: On parvient au risque tolérable par le processus itératif d'appréciation du risque (analyse du risque et évaluation du risque) et de réduction du risque.

[SOURCE: Guide ISO/CEI 51:1999, 3.7, modifiée – La note 1 à l'article a été ajoutée.]

3.1.8
risque résiduel
risque subsistant après que des mesures de prévention ont été prises

[SOURCE: Guide ISO/CEI 51:1999, 3.9]

3.1.9
sécurité
absence de risque inacceptable

[SOURCE: ISO/CEI Guide 51:1999, 3.1, modifiée – La note a été supprimée.]

3.1.10
sécurité fonctionnelle
sous-ensemble de la sécurité globale se rapportant à l'EUC et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque

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

3.1.11
état de sécurité
état de l'EUC lorsque la sécurité est réalisée

Note 1 à l'article: Pendant son évolution depuis un état potentiellement dangereux vers un état de sécurité final, l'EUC est susceptible de passer par un certain nombre d'états de sécurité intermédiaires. Dans certaines situations, l'état de sécurité n'est atteint que durant le temps où l'EUC est continuellement commandé. Cette commande continuée peut s'étendre sur une période courte ou indéfinie.

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

3.1.12
mauvais usage raisonnablement prévisible
utilisation d'un produit, procédé ou service dans des conditions ou à des fins non prévues par le fournisseur, mais qui peut provenir d'un comportement humain envisageable

[SOURCE: Guide ISO/CEI 51:1999, 3.14]

3.1.13
environnement
tous les paramètres pertinents susceptibles d'affecter la réalisation de la sécurité fonctionnelle pour l'application spécifique considérée et dans toute phase du cycle de vie de sécurité

Note 1 à l'article: Il peut s'agir, par exemple, de l'environnement physique, de l'environnement d'exploitation, de l'environnement légal et de l'environnement de maintenance.

[SOURCE: CEI 61508-4:2010, 3.2.2]

3.1.14
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

[SOURCE: CEI 61508-4:2010, 3.6.1; basée sur l'ISO/CEI 2382-14:1997, 14-01-10]

3.1.15
évitement des anomalies
utilisation de techniques et procédures destinées à éviter l'apparition d'anomalies durant chacune des phases du cycle de vie de sécurité du système relatif à la sécurité

[SOURCE: CEI 61508-4:2010, 3.6.2]

3.1.16
tolérance aux anomalies
aptitude d'une unité fonctionnelle à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs

Note 1 à l'article: La définition dans le CEI 60050-191-15-05 ne prend en compte que les pannes de sous entités (qualifie une entité qui est capable d'accomplir une fonction requise malgré certaines panes de ses sous-entités).

[SOURCE: CEI 61508-4:2010, 3.6.3, modifiée – La note a été adaptée; basée sur l'ISO/CEI 2382-14:1997, 14-01-10]

3.1.17
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

Note 1 à l'article: Cette définition est fondée sur le CEI 60050-191-04-01 avec des modifications apportées pour inclure les défaillances systématiques dues, par exemple, à des lacunes dans la spécification ou le logiciel.

Note 2 à l'article: Voir la Figure 4 de la CEI 61508-4:2010 pour la relation entre anomalies (pannes) et défaillances, tant dans la série CEI 61508 que dans la CEI 60050-191.

Note 3 à l'article: L'accomplissement des fonctions requises exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportement à éviter. L'occurrence d'un comportement à éviter est une défaillance.

Note 4 à l'article: Les défaillances sont soit aléatoires (dans le matériel), soit systématiques (dans le logiciel ou le matériel).

[SOURCE: CEI 61508-4:2010, 3.6.4, modifiée – La Figure 4 a été supprimée.]

3.1.18
cycle de vie de sécurité
activités nécessaires à la mise en œuvre des systèmes relatifs à la sécurité, se déroulant au cours d'une période allant de la phase de conception d'un projet jusqu'au moment où aucun des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque ne sont plus disponibles pour une utilisation

[SOURCE: CEI 61508-4:2010, 3.7.1, modifiée – Les Notes 1 et 2 ont été supprimées.]

3.1.19
éprouvé par une utilisation antérieure
démonstration, réalisée sur la base d'une analyse de l'expérience d'exploitation pour une configuration spécifique d'un élément, que la probabilité d'anomalies systématiques dangereuses est suffisamment faible pour que chaque fonction de sécurité qui utilise l'élément puisse atteindre son niveau d'intégrité de sécurité requis

[SOURCE: CEI 61508-4:2010, 3.8.18]

3.1.20
niveau d'intégrité de sécurité
SIL
niveau discret (parmi deux possibles), correspondant à une gamme de valeurs d'intégrité de sécurité, utilisé pour spécifier les exigences concernant l'intégrité de sécurité d'une fonction de sécurité allouée (en tout ou en partie) à un CPI ou à un DLD

Note 1 à l'article: Le niveau SIL 2 possède le plus haut niveau d'intégrité de sécurité et le niveau SIL 1 possède le plus bas selon la présente norme.

Note 2 à l'article: Les niveaux SIL 3 et SIL 4 ne sont pas pris en compte dans la présente Norme car ils ne sont pas pertinents pour les exigences de réduction des risques normalement associées aux CPI et aux DLD. Pour les exigences applicables aux niveaux SIL 3 et SIL 4, voir la CEI 61508.

[SOURCE: CEI 61508-4:2010, 3.5.8, modifiée – La Note 3 a été supprimée.]

3.1.21
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

EXEMPLE: Des exemples de fonctions de sécurité comprennent:

– les fonctions devant être réalisées en tant qu'actions positives pour éviter des situations dangereuses (par exemple, arrêt d'un moteur); et

– les fonctions de prévention de réalisation d'actions (par exemple, empêcher le démarrage d'un moteur).

[SOURCE: CEI 61508-4:2010, 3.5.1]

3.1.22
défaillance dangereuse
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la fonction de sécurité qui:

a) empêche le fonctionnement nécessaire de la fonction de sécurité (mode de sollicitation) ou provoque la défaillance d'une fonction de sécurité (mode continu) de sorte que l'EUC est mis dans un état dangereux ou potentiellement dangereux, ou

b) diminue la probabilité que la fonction de sécurité fonctionne correctement lorsque c'est nécessaire

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

3.1.23
défaillance en sécurité
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la fonction de sécurité qui:

a) conduit au fonctionnement parasite de la fonction de sécurité avec la potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité, ou

b) augmente la probabilité du fonctionnement parasite de la fonction de sécurité avec potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité

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

3.1.24
couverture du diagnostic
DC
proportion de défaillances dangereuses détectées par les essais de diagnostic en ligne automatiques

Note 1 à l'article: La proportion de défaillances dangereuses est calculée en divisant les taux de défaillance dangereuse associés aux défaillances dangereuses détectées par le taux total des défaillances dangereuses.

Note 2 à l'article: La couverture du diagnostic de défaillance dangereuse est calculée selon l'équation suivante, dans laquelle *DC* est la couverture du diagnostic, λ_{DD} est la probabilité de détection d'une défaillance dangereuse et $\lambda_{D\ total}$ est la probabilité de toutes les défaillances dangereuses:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{D\,total}}$$

Note 3 à l'article: Cette définition s'applique sous réserve que les composants individuels présentent des taux de défaillance constants.

[SOURCE: CEI 61508-4:2010, 3.8.6, modifiée – Une partie de la définition a été déplacée dans la Note 1 à l'article et les autres notes ont été renumérotées en conséquence.]

3.1.25
essai(s) de diagnostic
essai(s) visant à détecter d'éventuels défauts ou défaillances et à produire des informations ou activités spécifiques au moment de la détection d'un défaut ou d'une défaillance

Note 1 à l'article: Des essais de diagnostic peuvent être lancés par une action manuelle ou par un autotest automatique des dispositifs.

[SOURCE: CEI 61800-5-2:2007, 3.4, modifiée – La Note 1 à l'article a été ajoutée.]

3.1.26
validation
confirmation, par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique prévu sont satisfaites

Note 1 à l'article: La présente norme spécifie trois phases de validation:

– validation de sécurité générale (voir Figure 2 de la CEI 61508-1:2010);
– validation des systèmes E/E/PE (voir Figure 3 de la CEI 61508-1:2010);
– validation du logiciel (voir Figure 4 de la CEI 61508-1:2010).

Note 2 à l'article: La validation est l'activité qui consiste à démontrer que le système relatif à la sécurité considéré, avant ou après installation, correspond en tout point aux exigences de sécurité contenues dans la spécification de ce système relatif à la sécurité. Ainsi, par exemple, la validation du logiciel consiste en la confirmation, par examen et apport de preuves tangibles, que le logiciel répond à la spécification des exigences de sécurité du logiciel.

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

3.1.27
vérification
confirmation, par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique prévu sont satisfaites

Note 1 à l'article: Dans le contexte de la présente norme, la vérification est l'activité qui consiste, pour chaque phase du cycle de vie de sécurité correspondant (général, système E/E/PE et logiciel), à démontrer par analyse, raisonnement mathématique et/ou essais que, pour les entrées spécifiques, les éléments livrables remplissent en tout point les objectifs et les exigences fixés pour la phase spécifique.

EXEMPLE Les activités de vérification incluent:

– les revues relatives aux sorties d'une phase (documents concernant toutes les phases du cycle de vie de sécurité) destinées à assurer la conformité aux objectifs et aux exigences de la phase, en tenant compte des entrées spécifiques à cette phase;
– les revues de conception;
– les essais réalisés sur les produits conçus afin d'assurer que leur fonctionnement est conforme à leur spécification;
– les essais d'intégration réalisés lors de l'assemblage, élément par élément, de différentes parties d'un système et la réalisation d'essais d'environnement afin de s'assurer que toutes les parties fonctionnent les unes avec les autres conformément aux spécifications.

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

3.1.28
contrôleur d'isolement
CPI
instrument destiné à surveiller en permanence, et quelle que soit la méthode de mesure, la résistance d'isolement par rapport à la terre de réseaux IT c.a. non mis à la terre, ou de réseaux IT c.a. comprenant des circuits à courant continu reliés galvaniquement dont les tensions nominales sont au plus égales à 1 000 V c.a., et de réseaux IT c.c. dont les tensions nominales sont au plus égales à 1 500 V c.c.

[SOURCE: CEI 61557-8:2007, Article 1, modifié – Le domaine d'application a été adapté sous la forme d'une définition.]

3.1.29
système de localisation de défaut d'isolement
DLD
instrument ou combinaison d'instruments utilisés pour la localisation de défauts d'isolement dans les réseaux IT

Note 1 à l'article: Le système de localisation de défaut d'isolement est utilisé en complément d'un contrôleur d'isolement. Il injecte un courant de localisation entre le réseau et la terre et localise les défauts d'isolement.

[SOURCE: CEI 61557-9:2009, 3.1, modifiée – Une partie de la définition a été déplacée dans la Note 1 à l'article.]

3.1.30
équipement commandé
EUC
équipement, machine, appareil ou installation utilisé(e) pour des activités de fabrication, de traitement, de transport, médicales ou autres, dont le réseau d'alimentation est un réseau IT tel que décrit dans la CEI 60364-4-41

Note 1 à l'article: Le SRS est séparé et distinct de l'EUC.

Note 2 à l'article: Dans la CEI 61557-15, l'EUC est le réseau IT sur lequel l'CPI ou l'DLD est monté.

[SOURCE: CEI 61508-4:2010, 3.2.1 modifiée – Les Notes 1 et 2 à l'article ont été ajoutées.]

3.1.31
système relatif à la sécurité
SRS
système désigné qui, à la fois,

– met en œuvre les fonctions de sécurité requises pour atteindre ou maintenir un état de sécurité de l'EUC et
– est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/PE relatifs à la sécurité, et aux dispositifs externes de réduction de risque, l'intégrité de sécurité nécessaire pour les fonctions de sécurité requises

Note 1 à l'article: Ce terme fait référence aux systèmes désignés comme systèmes relatifs à la sécurité, qui sont prévu ensemble avec les autres mesures de réduction de risque (voir la CEI 61508-4:2010, 3.4.2), sont destinés à réaliser la réduction de risque nécessaire, afin de satisfaire au niveau de risque tolérable requis (voir la CEI 61508-4:2010, 3.1.7). Voir également l'Annexe A de la CEI 61508-5 :2010.

Note 2 à l'article: Les systèmes relatifs à la sécurité sont conçus pour empêcher l'EUC d'entrer dans un état dangereux en prenant les mesures appropriées de détection d'une condition susceptible d'occasionner un événement dangereux. La défaillance d'un système relatif à la sécurité serait incluse dans les événements à l'origine du ou des dangers déterminés. Bien qu'il puisse exister d'autres systèmes possédant des fonctions de sécurité, ce sont les systèmes relatifs à la sécurité qui ont été choisis pour obtenir à leur façon le niveau de risque tolérable requis. Les systèmes relatifs à la sécurité peuvent globalement être répartis en systèmes relatifs à la sécurité de commande et en systèmes relatifs à la sécurité de protection.

Note 3 à l'article: Les systèmes relatifs à la sécurité peuvent faire partie intégrante du système de commande de l'EUC ou peuvent être interfacés avec l'EUC par l'intermédiaire de capteurs et/ou d'actionneurs. Cela signifie qu'il est possible d'atteindre le niveau d'intégrité de sécurité requis en mettant en œuvre les fonctions de sécurité dans le système de commande de l'EUC (et éventuellement également par l'adjonction de systèmes séparés et indépendants) ou que ces fonctions de sécurité peuvent être exécutées par des systèmes séparés et indépendants dédiés à la sécurité.

Note 4 à l'article: Un système relatif à la sécurité peut:

a) être conçu pour prévenir un événement dangereux (c'est-à-dire qu'aucun événement dangereux ne survient tant que les systèmes relatifs à la sécurité exécutent leurs fonctions de sécurité);
b) être conçu pour réduire les effets de l'événement préjudiciable, réduisant ainsi le risque en limitant les conséquences de ce risque;
c) être conçu pour réaliser une combinaison de a) et de b).

Note 5 à l'article: Une personne peut faire partie d'un système relatif à la sécurité. Par exemple, une personne peut recevoir des informations d'un dispositif électronique programmable et exécuter une activité de sécurité à partir de cette information, ou exécuter une activité de sécurité par l'intermédiaire d'un dispositif électronique programmable.

Note 6 à l'article: Un système relatif à la sécurité recouvre l'ensemble des matériels, logiciels, ainsi que tous les équipements annexes (par exemple, alimentation) nécessaires pour exécuter la fonction de sécurité spécifiée (les capteurs, les autres dispositifs d'entrée, les éléments terminaux (actionneurs) ainsi que les autres dispositifs de sortie sont par conséquent compris dans le système relatif à la sécurité).

Note 7 à l'article: Un système relatif à la sécurité peut être basé sur une large gamme de technologies, comprenant les technologies électrique, électronique, électronique programmable, hydraulique et pneumatique.

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

3.1.32
probabilité de défaillance dangereuse en cas de sollicitation
PFD
indisponibilité de sécurité (voir CEI 60050-191) d'un système E/E/PE relatif à la sécurité pour réaliser la fonction de sécurité spécifiée sur sollicitation de l'EUC ou de son système de commande

Note 1 à l'article: L'indisponibilité [instantanée] (selon la CEI 60050-191) est la probabilité qu'un article ne soit pas en mesure de réaliser une fonction requise dans des conditions données à un moment donné, en supposant l'existence des ressources externes requises. Elle est généralement exprimée par U (t).

Note 2 à l'article: La disponibilité [instantanée] ne dépend pas des états (en fonctionnement ou en défaillance) dans lesquels l'article se trouve avant t. Elle caractérise un article qui doit uniquement être apte à fonctionner lorsqu'il doit le faire, par exemple, un système E/E/PE relatif à la sécurité fonctionnant en mode faible sollicitation.

Note 3 à l'article: Si elle est vérifiée périodiquement, la PFD d'un système E/E/PE relatif à la sécurité est, par rapport à la fonction de sécurité spécifiée, représentée par une courbe en dents de scie avec une large gamme de probabilités comprises entre un niveau minimal, juste après un essai, et un niveau maximal, juste avant un essai.

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

3.1.33
intégrité de sécurité
probabilité pour qu'un CPI ou un DLD exécute de manière satisfaisante les fonctions de sécurité spécifiées dans toutes les conditions énoncées et au cours d'une période de temps spécifiée

Note 1 à l'article: Plus le niveau d'intégrité de sécurité d'un système relatif à la sécurité est élevé, plus la probabilité d'une défaillance du système dans l'exécution des fonctions de sécurité spécifiées ou dans l'adoption d'un état spécifié lorsque cela est requis est faible.

Note 2 à l'article: La CEI 61508 définit quatre niveaux d'intégrité de sécurité (SIL). Pour les CPI et les DLD seuls les niveaux SIL 1 et SIL 2 sont spécifiés.

Note 3 à l'article: Il convient que l'évaluation de l'intégrité de sécurité prenne en compte toutes les causes de défaillance (à la fois les défaillances aléatoires du matériel et les défaillances systématiques) conduisant à un état de non-sécurité, par exemple les défaillances de matériel, les défaillances induites du logiciel et les défaillances dues aux perturbations électriques. Certaines de ces défaillances, en particulier les défaillances aléatoires du matériel, peuvent être quantifiées à l'aide de mesures telles que la fréquence moyenne de défaillance en mode de défaillance dangereux, ou la probabilité de non fonctionnement en cas de sollicitation d'un système de protection relatif à la sécurité. Cependant, l'intégrité de sécurité dépend également de plusieurs facteurs qui ne peuvent pas être précisément quantifiés, mais peuvent être simplement considérés d'un point de vue qualitatif.

Note 4 à l'article: L'intégrité de sécurité comprend l'intégrité de sécurité du matériel ainsi que l'intégrité de sécurité systématique.

Note 5 à l'article: Cette définition est centrée sur la fiabilité des systèmes relatifs à la sécurité dans l'exécution des fonctions de sécurité (voir CEI 60050-191-12-01 pour une définition de la fiabilité).

[SOURCE: CEI 61508-4:2010, 3.5.4, modifiée – "un système E/E/PE relatif à la sécurité" a été remplacé par "un CPI ou un DLD".]

3.1.34
cycle de vie de développement
manière dont les activités suivantes de développement relatives à la sécurité des CPI et DLD sont incluses:

– la définition des fonctions de sécurité
– la planification de la sécurité fonctionnelle
– la conception et le développement
– l'intégration et les essais
– la documentation
– l'organisation des modifications
– vérification
– la validation

3.1.35
mode de fonctionnement
manière dont une fonction de sécurité fonctionne

[SOURCE: CEI 61508-4:2010, 3.5.16, modifiée – Le mode de sollicitation faible, le mode de sollicitation élevée et le mode continu ont été séparés en de nouvelles définitions.]

3.1.35.1
mode de sollicitation faible
mode de fonctionnement qui est effectué uniquement sur sollicitation, afin de faire passer l'Équipement commandé (EUC) dans un état de sécurité spécifié et où la fréquence des sollicitations n'est pas supérieure à une par an

Note 1 à l'article: Le système E/E/PE relatif à la sécurité qui réalise la fonction de sécurité n'a normalement aucune influence sur l'Équipement commandé (EUC) ou sur le système de contrôle de l'Équipement commandé jusqu'à ce qu'une sollicitation survienne. Toutefois, si le système E/E/PE relatif à la sécurité est défaillant de telle sorte qu'il est incapable d'effectuer la fonction de sécurité, alors il peut provoquer le passage de l'Équipement commandé à un état de sécurité (voir 7.4.6 de la CEI 61508-2:2010).

3.1.35.2
mode de sollicitation élevée
lorsque la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et où la fréquence des sollicitations est supérieure à une par an

3.1.35.3
mode continu
lorsque la fonction de sécurité maintient l'Équipement commandé (EUC) dans un état sûr en fonctionnement normal la fonction de sécurité maintient l'EUC dans un état de sécurité en fonctionnement normal

3.1.36
anomalies systématiques
anomalies ou défauts qui peuvent apparaître au cours des différentes phases du cycle de vie comprenant:

– les erreurs de spécification,
– les erreurs de conception et de développement,
– les erreurs d'intégration,
– les erreurs au cours de la vérification ou de la validation,
– les erreurs dans la documentation et
– les erreurs au cours de l'installation et de l'utilisation

3.1.37
fonctions supplémentaires
fonctions d'un CPI ou d'un DLD relatif à la sécurité qui ne sont pas désignées comme fonctions de sécurité

3.1.38
intégrité de sécurité systématique
partie de l'intégrité de sécurité d'un système relatif à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux

Note 1 à l'article: L'intégrité de sécurité systématique ne peut normalement pas être quantifiée (à la différence de l'intégrité de sécurité du matériel qui, habituellement, peut l'être).

[SOURCE: CEI 61508-4:2010, 3.5.6]

3.1.39
défaillance de cause commune
défaillance résultant d'un ou plusieurs événements qui, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance du système

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

3.1.40
Intervalle entre essais de diagnostic
intervalle de temps entre les essais en ligne qui permettent de détecter les anomalies d'un système relatif à la sécurité, dont la couverture du diagnostic est spécifiée

[SOURCE: CEI 61508-4:2010, 3.8.7]

3.1.41
proportion de défaillances en sécurité
SFF
propriété d'un élément relatif à la sécurité définie par le rapport des taux de défaillance moyens des défaillances en sécurité et dangereuses détectées et des défaillances en sécurité et dangereuses

Note 1 à l'article: Ce rapport est représenté par l'équation suivante:

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

lorsque les taux de défaillance sont basés sur des taux de défaillance constants, l'équation peut être simplifiée comme suit:

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

[SOURCE: CEI 61508-4:2010, 3.6.15, modifiée – Une partie de la définition a été déplacée dans la Note 1 à l'article.]

3.1.42
durée moyenne de rétablissement
MTTR
durée prévue de rétablissement effectif

Note 1 à l'article: La MTTR comprend:

– le temps de détection de la défaillance (a); et,
– le temps écoulé avant de commencer la réparation (b); et,
– le temps de réparation effectif (c); et,
– le temps écoulé avant la remise en fonctionnement du composant (d)

– le temps de démarrage applicable à (b) est la fin du temps (a); le temps de démarrage applicable à (c) est la fin du temps (b) et le temps de démarrage applicable à (d) est la fin du temps (c).

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

3.1.43
architecture MooN
architecture constituée d'un nombre (M) de canaux indépendants, où chacun des canaux (N) suffit à exécuter correctement la fonction de sécurité

3.1.44
architecture MooND
architecture constituée d'un nombre (M) de canaux indépendants, où chacun des canaux (N) suffit à exécuter correctement la fonction de sécurité plus le diagnostic (D)

3.1.45
défaillance dangereuse
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la fonction de sécurité qui:

– empêche le fonctionnement nécessaire de la fonction de sécurité (mode de sollicitation) ou provoque la défaillance d'une fonction de sécurité (mode continu) de sorte que l'EUC est mis dans un état dangereux ou potentiellement dangereux, ou

– diminue la probabilité que la fonction de sécurité fonctionne correctement lorsque c'est nécessaire

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

3.1.46
défaillance en sécurité
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la fonction de sécurité qui:

– conduit au fonctionnement parasite de la fonction de sécurité avec la potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité, ou

– augmente la probabilité du fonctionnement parasite de la fonction de sécurité avec potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité

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

3.1.47
défaillance dépendante
défaillance dont la probabilité ne peut être exprimée en tant que simple produit des probabilités non conditionnelles des événements individuels qui l'ont provoquée

Note 1 à l'article: Deux événements A et B sont dépendants si, et seulement si: P (A et B) > P (A) × P (B).

[SOURCE: CEI 61508-4:2010, 3.6.9]

3.1.48
fin de vie
EOL
phase du cycle de vie d'un produit débutant lorsqu'il est définitivement retiré de sa phase d'utilisation prévue

[SOURCE: CEI Guide 109:2012, 3.1]

3.1.49
durée moyenne de fonctionnement avant défaillance
MTTF
espérance mathématique de la durée de fonctionnement avant défaillance

[SOURCE: CEI 60050-191:1990, 191-12-07]

3.1.50
défaut d'isolement
défectuosité de l'isolation d'une installation électrique ou d'un matériel qui peut entraîner soit un courant anormal à travers cette isolation, soit une décharge disruptive

[SOURCE: CEI 60050-604:1987, 604-02-02, modifiée – Ajout de "installation électrique".]

3.1.50.1
défaut d'isolement symétrique
défectuosité de l'isolation d'une installation ou d'un matériel électrique qui génère un trajet résistif par rapport à la terre ayant environ les mêmes valeurs de résistance entre tous les conducteurs de phase et la terre

3.1.50.2
défaut d'isolement asymétrique
défectuosité de l'isolation d'une installation ou d'un matériel électrique qui génère un trajet résistif par rapport à la terre ayant des valeurs de résistance différentes entre les conducteurs de phase et la terre

3.1.51
résistance d'isolement
R_F
résistance dans le système sous surveillance, comprenant la résistance de tous les appareils qui sont connectés au réseau de distribution

[SOURCE: CEI 61557-8:2007, 3.2]

3.1.52
essai périodique
essai périodique destiné à détecter les défaillances dangereuses cachées d'un système relatif à la sécurité de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition «comme neuf» ou dans une condition aussi proche que possible de celle-ci

[SOURCE: CEI 61508-4:2010, 3.8.5, modifiée – Les notes ont été supprimées.]

3.1.53
temps de sécurité du processus
durée entre l'occurrence d'une défaillance, avec potentialité de donner lieu à un événement dangereux, se produisant dans l'EUC ou son système de commande et le temps nécessaire pour accomplir l'action dans l'EUC pour empêcher l'occurrence de l'événement dangereux

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

3.1.54
capacité de fuite au réseau de distribution
C_e
valeur maximale admissible de la capacité totale par rapport à la terre du réseau à surveiller et de tous les matériels connectés, jusqu'à laquelle le contrôleur permanent d'isolement peut travailler conformément aux caractéristiques indiquées

[SOURCE: CEI 61557-8:2007, 3.6]

3.1.55
électrique/électronique/ électronique programmable
E/E/PE
basé sur une technologie électrique (E) et/ou électronique (E) et/ou électronique programmable (PE)

Note 1 à l'article: Dans la CEI 61557-15, les CPI ou les DLD sont les dispositifs relatifs à la sécurité désignés comme étant un système E/E/PE dans la série de normes CEI 61508.

[SOURCE: CEI 61508-4:2010, 3.2.13, modifiée – La note et l'exemple ont été remplacés par la Note 1 à l'article.]

3.1.56
sensibilité de déclenchement
valeur du courant d'évaluation ou de la résistance d'isolement à laquelle le localisateur réagit dans des conditions données

[SOURCE: CEI 61557-9:2009, 3.4, modifiée – La note a été supprimée.]

3.2 Abréviations

Pour les besoins du présent document, les abréviations données dans la CEI 61557-1, la CEI 61557-8 et la CEI 61557-9 ainsi que les abréviations suivantes énumérées dans le Tableau 1 s'appliquent:

Tableau 1 – Abréviations avec référence

Abréviation	Termes en anglais	Termes en français	Référence
DC	Diagnostic coverage	Couverture du diagnostic	CEI 61508-4:2010, 3.8.6
E/E/PE	Electric, electronic, programmable electronic	Électrique/électronique/électronique programmable	CEI 61508-4:2010, 3.2.13
CEM	Electromagnetic compatibility (EMC)	Compatibilité électromagnétique	CEI 61000-1-1
EOL	End of life	Fin de vie	CEI Guide 109:2012, 3.1
EUC	Equipment under control	Équipement commandé	CEI 61508-4
AMDE	Failure mode and effect analysis (FMEA)	Analyse des modes de défaillance et de leurs effets	CEI 60812
IFL	Insulation fault locator	Localisateur de défaut d'isolement	CEI 61557-9
DLD	Insulation fault location system (IFLS)	Système de localisation de défaut d'isolement	3.1.29
CPI	Insulation monitoring device (IMD)	Contrôleur d'isolement	3.1.28
IT (système)	I: all live parts isolated from earth (power system to earth) T: direct connection of exposed-conductive parts to earth (terre) independently of the earthing of any point of the power system	I: toutes les parties actives isolées de la terre (système d'alimentation à la terre) T: raccordement direct des parties exposées-conductrices à la masse (terre), indépendamment de la mise à la terre d'un point quelconque du système d'alimentation	IEC 60364-1:2005, 312.2
LCI	Locating current injector	Injecteur de courant de localisation	IEC 61557-9:2009, 3.7
LIW	Local Insulation warning	Alarme locale de défaut d'isolation	4.2.1
LLW	Local location warning	Alarme locale de localisation de défaut	4.2.3
LTMW	Local transformer monitoring warning	Alarme locale de surveillance du transformateur	4.2.6

Abréviation	Termes en anglais	Termes en français	Référence
MooN	Number (M) out of (N) independent channels	Nombre (M) parmi (N) canaux indépendants	CEI 61508-6
MooND	Number (M) out of (N) independent channels with diagnostics (D)	Nombre (M) parmi (N) canaux indépendants avec diagnostique	IEC 61508-4:2010, Table 1
MTTF	Mean time to failure	Durée moyenne de fonctionnement avant défaillance	CEI 60050,191-12-07
MTTR	Mean time to restoration	Durée moyenne de rétablissement	CEI 61508-4:2010, 3.6.21
PFD	Probability of dangerous failure on demand	Probabilité de défaillance dangereuse en cas de sollicitation	CEI 61508-4:2010, 3.6.17
PFH	Probability of dangerous failure per hour	Probabilité de défaillance dangereuse par heure	CEI 61508-4:2010, 3.6.19
REDC	Remote enabling / disabling command	Commande distante d'activation/désactivation	4.2.5
RIW	Remote insulation warning	Alarme distante de défaut d'isolation	4.2.2
RLW	Remote Location warning	Alarme distante de localisation de défaut	4.2.4
SFF	Safe failure fraction	Proportion de défaillances en sécurité	CEI 61508-4:2010, 3.6.15
SIL	Safety integrity level	Niveau d'intégrité de sécurité	CEI 61508-4:2010, 3.5.8
SRS	Safety related system	Système relatif à la sécurité	CEI 61508-4:2010, 3.2.1

4 Définition des fonctions de sécurité intégrées dans les CPI et les DLD

4.1 Généralités

L'Article 4 décrit les fonctions d'un CPI ou d'un DLD qui, conformément à la présente norme, peuvent être qualifiées de "fonctions de sécurité". La liste des fonctions de sécurité décrites dans l'Article 4 est considérée comme exhaustive. Éventuellement, toute autre fonction spécifique de sécurité doit être conforme à la CEI 61508.

Il n'est pas obligatoire qu'un CPI ou un DLD dispose de toutes ces fonctions. En général, il n'est pas obligatoire d'attribuer un niveau SIL à ces fonctions. Cependant, si un niveau SIL est attribué à l'une de ces fonctions, celle-ci doit satisfaire aux exigences spécifiées dans la présente norme.

Un niveau SIL est attribué à une fonction et non à un produit. Par conséquent, les différentes fonctions de sécurité d'un CPI ou d'un DLD peuvent avoir différents niveaux SIL.

Lorsqu'une fonction de sécurité dépend de valeurs limites de paramètres, les tolérances maximales de ces valeurs limites doivent être définies.

Le niveau d'intégrité de sécurité de l'application dépend de l'intégration correcte de la fonction de sécurité assurée par l'CPI ou l'DLD au sein du réseau IT (voir la documentation de l'utilisateur en 7.2.6).

4.2 Définition des fonctions de sécurité

4.2.1 Alarme locale de défaut d'isolation (LIW)

Cette fonction génère un signal d'avertissement lorsque la résistance d'isolement entre le réseau et la terre chute sous un niveau préétabli.

Cette fonction comprend la mesure de la résistance d'isolement R_f d'un réseau IT, y compris des défauts d'isolement symétrique et asymétrique, une évaluation de cette résistance et une alarme locale de sécurité.

La position de sécurité doit être la position d'alarme. Il convient que l'alarme locale de sécurité soit fournie par des indicateurs visuels et/ou des signaux sonores générés par le produit qui met en œuvre la fonction.

NOTE Cette fonction est généralement assurée par l'CPI.

Outre les exigences de la présente CEI 61557-15, les produits revendiquant un niveau SIL pour ladite fonction doivent être conformes à la CEI 61557-8 et notamment aux exigences de performance supplémentaires définies en 5.2.

4.2.2 Alarme distante de défaut d'isolation (RIW)

Cette fonction génère un signal de sortie d'avertissement lorsque la résistance d'isolement entre le réseau et la terre chute sous un niveau préétabli.

Cette fonction comprend la mesure de la résistance d'isolement d'un réseau IT, y compris des défauts d'isolement symétrique et asymétrique, une évaluation de cette résistance et une sortie d'avertissement.

La sortie d'avertissement doit être rapportée à distance avec une sortie de sécurité.

La position de sécurité doit être la position d'avertissement.

NOTE 1 Il est possible d'utiliser une sortie de contact de relais ou une sortie de commutation électronique ou une communication de données sécurisée pour rapporter à distance l'avertissement de sécurité.

NOTE 2 Dans certaines applications, la sortie d'avertissement peut également être utilisée pour la commutation.

Outre les exigences de la présente CEI 61557-15, les produits revendiquant un niveau SIL pour ladite fonction doivent être conformes à la CEI 61557-8 et notamment aux exigences de performance supplémentaires définies en 5.2.

4.2.3 Alarme locale de localisation de défaut (LLW)

Cette fonction génère un signal d'avertissement lorsque la résistance d'isolement entre le réseau et la terre chute sous la sensibilité de déclenchement.

Cette fonction localise un défaut d'isolement de réseau IT, y compris des défauts d'isolement symétrique et asymétrique, évalue ce défaut et génère une alarme locale de sécurité.

La position de sécurité doit être la position d'avertissement.

Il convient que l'alarme locale de sécurité soit fournie par des indicateurs visuels ou des signaux sonores générés par le produit qui met en œuvre la fonction.

NOTE Cette fonction est généralement assurée par l'DLD.

Outre les exigences de la présente CEI 61557-15, les produits revendiquant un niveau SIL pour ladite fonction doivent être conformes à la CEI 61557-9 et notamment aux exigences de performance supplémentaires définies en 5.2.

4.2.4 Alarme distante de localisation de défaut (RLW)

Cette fonction génère un signal d'avertissement lorsque la résistance d'isolement entre le réseau et la terre chute sous la sensibilité de déclenchement.

Cette fonction comprend la localisation d'un défaut d'isolement de réseau IT, y compris des défauts d'isolement symétrique et asymétrique, une évaluation de ce défaut et une alarme distante de sécurité.

La sortie d'avertissement doit être rapportée à distance avec une sortie de sécurité.

La position de sécurité doit être la position d'avertissement.

NOTE 1 Il est possible d'utiliser une sortie de contact de relais ou une sortie de commutation électronique ou une communication de données sécurisée pour rapporter à distance l'avertissement de sécurité.

NOTE 2 Dans certaines applications, la sortie d'avertissement peut également être utilisée pour la commutation.

Outre les exigences de la présente CEI 61557-15, les produits revendiquant un niveau SIL pour ladite fonction doivent être conformes à la CEI 61557-9 et notamment aux exigences de performance supplémentaires définies en 5.2.

4.2.5 Commande distante d'activation/désactivation (REDC)

Ces fonctions prennent en charge une commande à distance, soit pour activer la mesure de la résistance d'isolement d'un réseau IT, soit pour la désactiver.

La position de sécurité doit être l'activation de la mesure de la résistance d'isolement d'un réseau IT.

NOTE Il est possible d'utiliser une sortie de contact de relais, une sortie de commutation électronique ou une communication de données sécurisée pour fournir la commande à distance.

Outre les exigences de la présente CEI 61557-15, les produits revendiquant un niveau SIL pour ladite fonction doivent être conformes à la CEI 61557-8 ou à la CEI 61557-9, et notamment aux exigences de performance supplémentaires définies en 5.2.

4.2.6 Alarme locale de surveillance du transformateur (LTMW)

Cette fonction génère un signal d'alarme locale lorsque le fonctionnement du transformateur d'isolement pour réseaux IT est anormal; soit le courant du côté du secondaire du transformateur est trop élevé, soit la température du transformateur est trop élevée.

Cette fonction comprend une surveillance du courant de sortie assigné, une surveillance de la température du transformateur, une évaluation des mesures effectuées et une alarme locale de sécurité.

La position de sécurité doit être la position d'avertissement.

Il convient que l'alarme locale de sécurité soit fournie par des indicateurs visuels et/ou des signaux sonores générés par le produit qui met en œuvre la fonction.

NOTE Cette fonction est généralement assurée par l'CPI.

Outre les exigences de la CEI 61557-15, les produits revendiquant un niveau SIL pour ladite fonction doivent être conformes à la CEI 61557-8 et notamment aux exigences de performance supplémentaires définies en 5.2.

5 Exigences applicables aux produits réalisant des fonctions relatives à la sécurité

5.1 Exigences applicables aux fonctions non relatives à la sécurité

Lorsqu'un CPI et un DLD comportent des fonctions supplémentaires qui ne sont pas désignées comme étant des fonctions de sécurité, l'ensemble du matériel et du logiciel doit alors être traité comme étant relatif à la sécurité, sauf s'il peut être démontré que la mise en œuvre des fonctions de sécurité et des fonctions supplémentaires est suffisamment indépendante (c'est-à-dire que la défaillance d'une quelconque fonction supplémentaire n'entraîne pas de défaillance dangereuse des fonctions de sécurité).

NOTE 1 On peut établir que l'indépendance est suffisante en montrant que la probabilité d'une défaillance dépendante entre les parties relatives à la sécurité et les parties non relatives à la sécurité est suffisamment faible en comparaison à la probabilité de défaillance dangereuse avec le niveau d'intégrité de sécurité le plus élevé associé aux fonctions de sécurité impliquées.

NOTE 2 Une fonction supplémentaire de l'CPI et de l'DLD peut être, par exemple, un moyen indiquant la valeur mesurée de la résistance d'isolement R_f.

5.2 Exigences de performance supplémentaires pour des produits mettant en œuvre des fonctions de sécurité

5.2.1 Généralités

Outre les exigences de la norme de produit CEI 61557-8 ou CEI 61557-9, les CPI et DLD conformes au niveau SIL 1 ou SIL 2 selon la présente norme doivent satisfaire aux exigences suivantes de performance supplémentaires.

NOTE D'autres spécifications et essais de conformité aux exigences sont inclus dans la CEI 61557-8 et dans la CEI 61557-9.

5.2.2 Exigences de performance supplémentaires pour des CPI conformes au SIL 1 ou SIL 2

5.2.2.1 Performances de l'CPI en cas de coupure de la connexion au réseau à surveiller

Les CPI conformes au SIL 1 ou SIL 2 doivent fournir une indication en cas de perte de la connexion au réseau à surveiller telle que la fonction de surveillance n'est plus assurée. Cette fonction comprend la surveillance de la connexion à la terre et aux conducteurs de phase du réseau à surveiller.

5.2.2.2 CEM

Les fonctions de sécurité de l'CPI doivent être conformes à la CEI 61326-3-1 et à la CEI 61326-2-4 selon 7.7.5.

5.2.3 Exigences de performance supplémentaires pour des DLD conformes au SIL 1 ou SIL 2

5.2.3.1 Performances des DLD en cas de coupure de la connexion au capteur de courant de localisation

Les DLD conformes au SIL 1 ou SIL 2 doivent fournir une indication en cas de perte de la connexion à un ou plusieurs capteurs de courant de localisation.

5.2.3.2 CEM

Les fonctions de sécurité de l'DLD doivent être conformes à la CEI 61326-3-1 et à la CEI 61326-2-4, selon 7.7.5

6 Gestion de la sécurité fonctionnelle au cours du cycle de vie de développement

6.1 Gestion de la sécurité fonctionnelle pour le réseau IT

Il incombe à l'intégrateur du système et à l'utilisateur final de s'assurer que les exigences de la CEI 61508 sont appliquées au réseau IT correspondant dont le cycle de vie de développement est tel que défini en Figure 2.

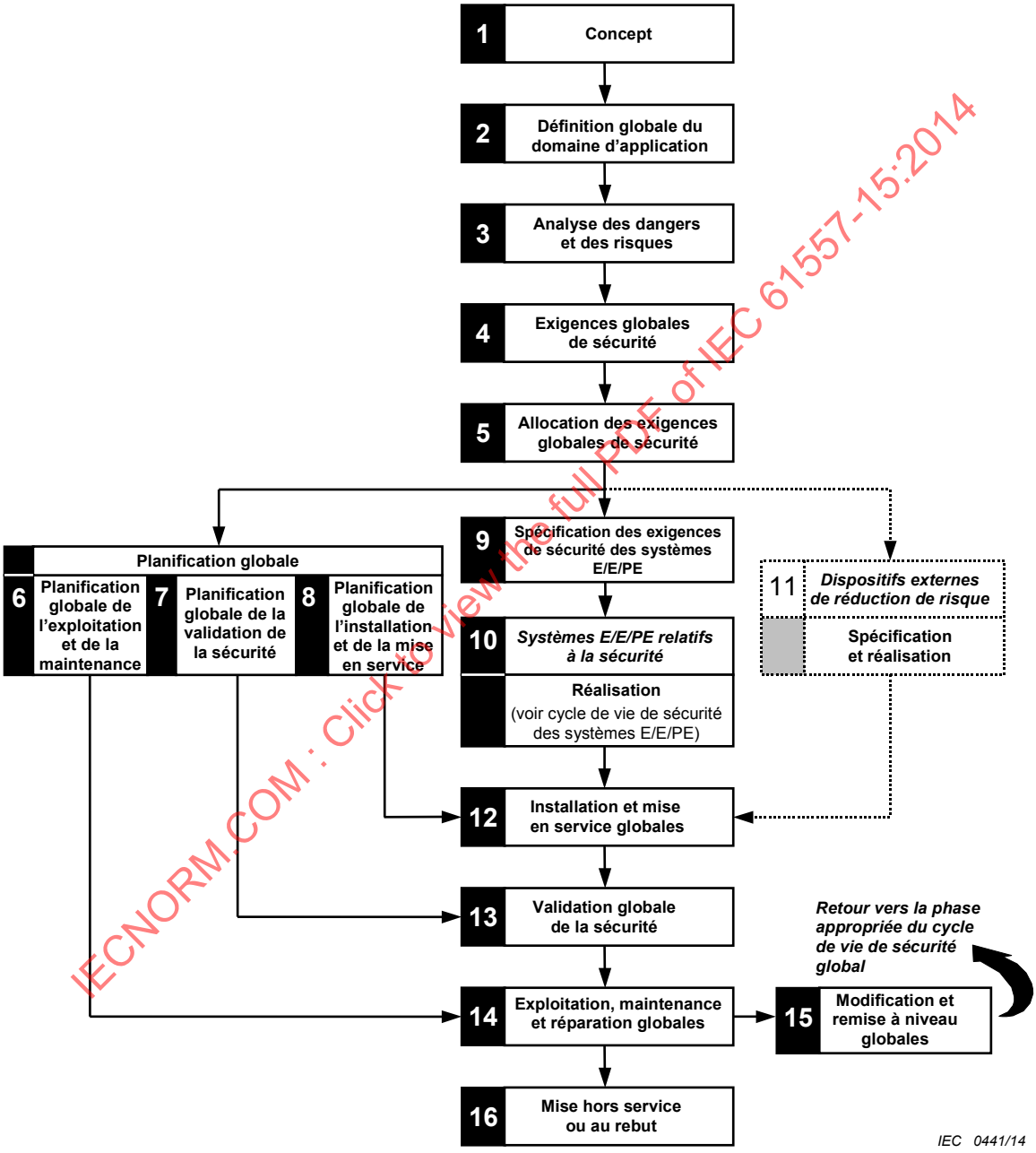


Figure 2 – Cycle de vie de sécurité global applicable à un réseau IT

6.2 Utilisation des CPI et des DLD dans des réseaux IT

Les objectifs de gestion de la sécurité fonctionnelle des CPI et des DLD font partie intégrante de la gestion de la sécurité fonctionnelle du réseau IT où ils sont montés.

La présente norme couvre, uniquement pour les CPI et les DLD, la phase 10 du cycle de vie de sécurité global applicable à un réseau IT. La présente norme ne couvre pas la phase 10 de la réalisation du réseau IT.

6.3 Cycle de vie de sécurité des CPI et des DLD en phase de réalisation

Les CPI et les DLD font partie des mesures de protection dans les réseaux IT. La présente norme définit les exigences de sécurité fonctionnelle pour la réalisation des CPI et des DLD conformément à la Figure 3.

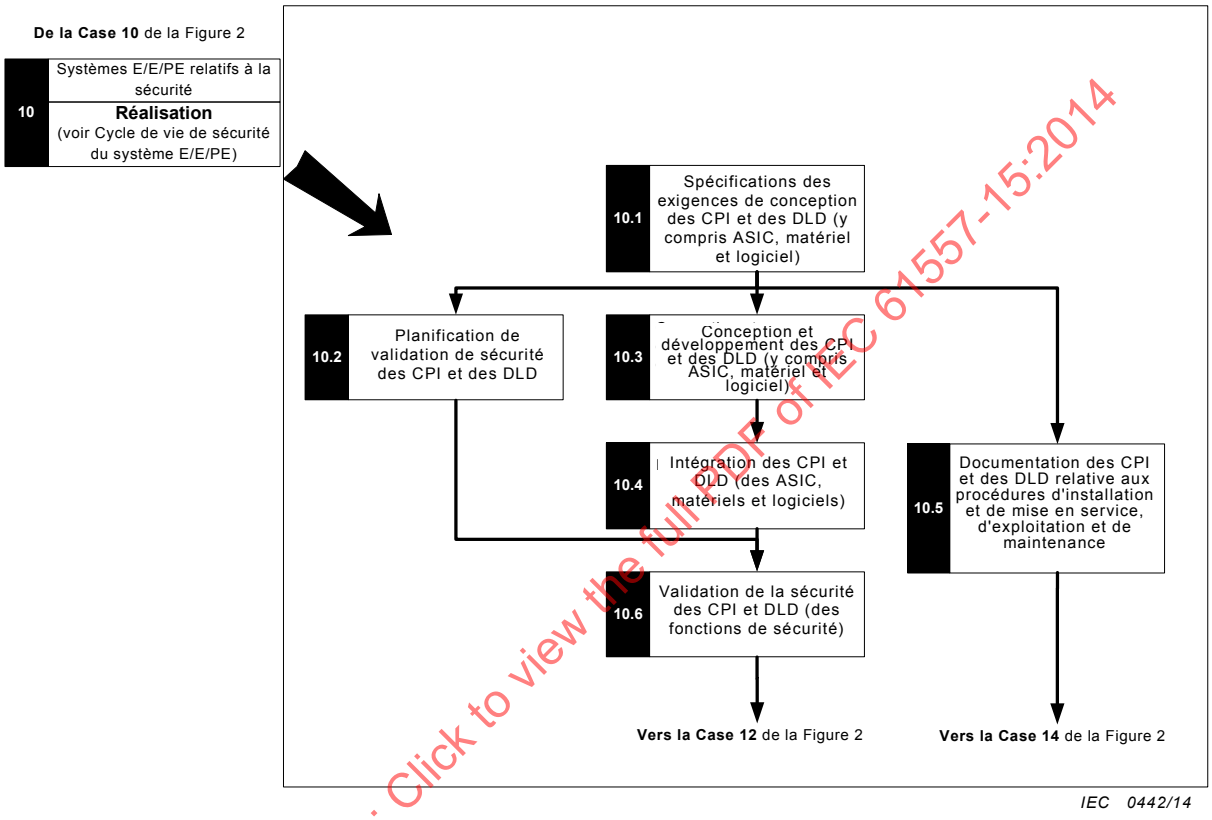


Figure 3 – Cycle de vie de sécurité des CPI et des DLD (en phase de réalisation)

7 Gestion de la sécurité fonctionnelle au cours du cycle de vie de réalisation des CPI et des DLD

7.1 Généralités

L'Article 7 identifie les activités nécessaires à l'ensemble du processus de réalisation des CPI et des DLD afin de garantir la satisfaction des objectifs de sécurité fonctionnelle. La gestion de la sécurité fonctionnelle est assurée à toutes les étapes du cycle de vie de sécurité des CPI et des DLD. Le cycle de vie de développement en est une partie importante. Un plan de sécurité fonctionnelle doit être établi et documenté pour chaque projet de conception d'CPI et d'DLD.

Les activités générales suivantes sont incluses dans le cycle de vie de développement:

– planification, organisation, contrôle et communication du processus de développement de la sécurité fonctionnelle,

– vérification de la compétence des personnes chargées des activités de sécurité fonctionnelle,

– établissement, documentation et contrôle du processus du cycle de vie de sécurité,

– définition et contrôle des exigences techniques de sécurité fonctionnelle,
– développement des CPI et des DLD du point de vue de la sécurité fonctionnelle,
– suivi, revue et validation du processus de développement de la sécurité fonctionnelle.

NOTE Si l'évaluation de la conformité selon l'ISO 9001 est fournie, le processus de développement de la sécurité fonctionnelle peut faire référence aux procédures qualité pertinentes.

7.2 Spécification des exigences de conception des CPI et des IFL (phase 10.1)

7.2.1 Spécification des exigences de sécurité fonctionnelle

7.2.1.1 Spécification des exigences de fonctionnalité de la sécurité

Des exigences complètes et détaillées concernant la fonctionnalité de la sécurité, y compris les fonctions de sécurité, doivent être incluses dans la spécification de développement ou définies dans un document séparé.

Les exigences de fonctionnalité de la sécurité sont déterminées sur la base de la stratégie de réduction du risque présentée en Annexe A.

La spécification des exigences de fonctionnalité de la sécurité doit comprendre:

– la spécification des exigences fonctionnelles:
  - conditions de fonctionnement des CPI et des DLD
  - description fonctionnelle des CPI et des DLD
  - caractéristiques de réponse exigées
  - description des fonctions de sécurité et des contraintes correspondantes
  - description des réactions aux défauts et des contraintes correspondantes
  - description de l'environnement d'exploitation
  - essais et conditions d'essai
– les exigences CEM
– la spécification des exigences d'intégrité de sécurité.

7.2.1.2 Spécification des exigences d'intégrité de sécurité

Les exigences d'intégrité de sécurité doivent être exprimées en valeur cible de probabilité de défaillance dangereuse en cas de sollicitation (PFD) pour chaque CPI et DLD.

Les CPI et les DLD sont considérés fonctionner en mode faible sollicitation conformément à la CEI 61508-2.

Les exigences d'intégrité de sécurité doivent être spécifiées en termes de SIL conformément au Tableau 2. Une méthode d'attribution du niveau SIL est décrite en Annexe A.

Tableau 2 – Niveaux d'intégrité de sécurité (SIL) et probabilité d'une défaillance dangereuse en cas de sollicitation (PFD) des CPI et des DLD

Niveau d'intégrité de sécurité (SIL)	Probabilité de défaillance dangereuse en cas de sollicitation (PFD)	Facteur de réduction du risque
1	$\geq 10^{-2}$ à 10^{-1}	>10 à ≤ 100
2	$\geq 10^{-3}$ à 10^{-2}	>100 à ≤ 1 000
Dans la présente norme, seuls les niveaux d'intégrité de sécurité 1 et 2 s'appliquent aux CPI et DLD.		

7.2.2 Dispositions pour le développement de fonctions de sécurité

Les CPI et les DLD doivent être développés de manière à satisfaire aux exigences du plan de sécurité fonctionnelle selon 7.3.2 et de la spécification des exigences de sécurité fonctionnelle selon 7.2.1 et doivent satisfaire aux exigences suivantes:

– conception et développement (voir 7.4);
– normes de conception;
– exigences d'intégrité de sécurité et de détection des défauts;
– contraintes architecturales relatives à l'intégrité de sécurité du matériel
– probabilité de défaillances dangereuses aléatoires du matériel
– intégrité de sécurité systématique;
– évitement des défaillances;
– maîtrise des anomalies systématiques;
– comportement en cas de détection d'anomalie;
– conception et développement du logiciel relatif à la sécurité.

La conception de l'CPI et de l'DLD doit tenir compte des aptitudes et des limites humaines ainsi que de toute mauvaise utilisation raisonnablement prévisible.

La conception comprend les fonctions de diagnostic et de réaction aux défaillances; celles-ci doivent être documentées et vérifiées à des étapes appropriées conformément au plan de sécurité fonctionnelle.

7.2.3 Plan de vérification du développement des fonctions de sécurité

Le plan de vérification doit être élaboré et couvrir au moins les points suivants:

– la description des stratégies de vérification,
– la structure organisationnelle de la vérification,
– la sélection et l'utilisation du matériel d'essai,
– la description des activités de vérification,
– le plan de revue des spécifications:
  - plan de sécurité fonctionnelle,
  - spécification des exigences de sécurité fonctionnelle,
  - spécification des exigences de fonctionnalité de la sécurité,
  - spécification des exigences d'intégrité de sécurité,
  - spécification de mise en service, d'installation et de mise en fonctionnement.

Le cas échéant, le plan doit être revu et mis à jour au cours du cycle de vie de développement.

7.2.4 Plan de validation du développement des fonctions de sécurité

Le plan de validation doit être élaboré et couvrir au moins les points suivants:

– la description des stratégies de validation
– la structure organisationnelle de la validation,
– les critères d'acceptation de la validation,
– les mesures en cas de non-respect des critères d'acceptation.

Le cas échéant, le plan doit être revu et mis à jour au cours du cycle de vie de développement.

7.2.5 Planification de la mise en service, de l'installation et de la mise en fonctionnement

Le plan de mise en service, d'installation et de mise en fonctionnement doit être élaboré et couvrir au moins les points suivants:

– la description des actions spéciales,
– les exigences en termes d'organisation et de personnes,
– la documentation de mise en fonctionnement,
– la documentation des essais de mise en fonctionnement.

Le cas échéant, le plan doit être revu et mis à jour au cours du cycle de vie de développement.

7.2.6 Planification de la documentation utilisateur

Le plan relatif à la documentation utilisateur doit être élaboré et couvrir au moins les points suivants:

– les informations concernant la fonctionnalité de la sécurité,
– les informations concernant l'intégrité de sécurité,
– les informations relatives aux activités de l'utilisateur en matière de mise en service, d'installation, de mise en fonctionnement, d'exploitation, de modification et de mise hors service,
– les informations de fin de vie, le cas échéant.

Le cas échéant, le plan doit être revu et mis à jour au cours du cycle de vie de développement.

7.3 Planification de la validation de la sécurité des CPI et des DLD (phase 10.2)

7.3.1 Généralités

Un plan de sécurité fonctionnelle doit être établi pour l'ensemble du cycle de vie de développement des CPI et des DLD. Le plan doit définir les activités au cours du cycle de vie conformément aux exigences des Articles 5 à 9 et doit être, si nécessaire, mis à jour au cours du processus de développement. Le plan doit également décrire les détails organisationnels des activités à entreprendre. Il doit être intégré au plan de management de la qualité comme une section intitulée “plan de sécurité fonctionnelle” ou il peut s'agir d'un document séparé.

7.3.2 Plan de sécurité fonctionnelle

Le plan de sécurité fonctionnelle doit au moins couvrir les points suivants:

– l'identification des activités pertinentes spécifiées aux Articles 6, 7 et 8;
– l'identification de l'organisation (personnes, services ou autres unités ou ressources) chargée d'exécuter et de revoir chacune des activités spécifiée aux Articles 6, 7 et 8;
– l'identification ou établissement des procédures et ressources nécessaires à l'enregistrement et à la conservation des informations relatives à la sécurité fonctionnelle des CPI et des DLD:
  - les résultats de l'identification des dangers et de l'appréciation du risque;
  - les fonctions de sécurité ainsi que les exigences de sécurité correspondantes;
  - l'organisation chargée de maintenir la sécurité fonctionnelle;

- les procédures nécessaires à la réalisation et au maintien de la sécurité fonctionnelle pour les CPI et les DLD.

– la description de la stratégie de gestion de la configuration en tenant compte des problématiques organisationnelles pertinentes, telles que les personnes autorisées et les structures internes de l'organisation.
– l'établissement d'un plan de vérification qui doit couvrir:
  - l'intégration de la vérification dans le management de la qualité;
  - les informations détaillées concernant les personnes, les services ou les unités qui doivent effectuer la vérification;
  - la sélection des techniques et des stratégies de vérification;
  - la sélection des activités de vérification;
  - les critères d'acceptation;
  - les moyens à utiliser pour évaluer les résultats de vérification.
– l'établissement d'un plan de validation précisant:
  - les exigences de validation;
  - l'identification des modes de fonctionnement pertinents des CPI et des DLD;
  - la stratégie technique de validation, par exemple des méthodes analytiques ou des essais statistiques;
  - les critères d'acceptation;
  - les actions à entreprendre en cas de non-respect des critères d'acceptation.

Il convient que le plan de validation indique si, oui ou non, les CPI et les DLD sont tenus de faire l'objet d'essais individuels de série, d'essais de type et/ou d'essais par échantillonnage et quels essais particuliers sont nécessaires du point de vue de la sécurité fonctionnelle.

7.4 Conception et développement des CPI et des DLD (phase 10.3)

7.4.1 Généralités

Du point de vue de la sécurité fonctionnelle, la conception et le développement des CPI et des DLD doivent être conformes à la spécification des exigences de sécurité fonctionnelle. Lorsque les CPI et les DLD comportent des fonctions de sécurité et des fonctions supplémentaires, tous les matériels et logiciels susceptibles de nuire à une quelconque fonction de sécurité dans des conditions normales et de défaut, doivent être traités comme une fonction de sécurité et doivent satisfaire au niveau SIL correspondant. Ceci n'est pas nécessaire si les fonctions de sécurité et les fonctions supplémentaires sont suffisamment indépendantes les unes des autres.

Il convient, dans toute la mesure du possible, de séparer les fonctions de sécurité des fonctions supplémentaires, tant au niveau matériel que logiciel, et de définir clairement les liaisons ou interfaces existant entre elles.

NOTE L'expression "suffisamment indépendantes" signifie que la défaillance d'une éventuelle fonction supplémentaire, dans le matériel ou le logiciel, est incapable d'entraîner une défaillance dangereuse d'une quelconque fonction de sécurité.

La conception des CPI et des DLD doit prendre en compte les aptitudes et des limites humaines et doit être adaptée aux tâches des opérateurs et du personnel de maintenance des dispositifs.

7.4.2 Normes de conception

Les CPI et les DLD doivent être respectivement conçus conformément à la CEI 61557-8 et à la CEI 61557-9.

7.4.3 Réalisation

Les CPI et les DLD doivent être réalisés conformément à leur plan de sécurité fonctionnelle et aux spécifications des exigences de sécurité fonctionnelle (voir 7.3.2 et 7.2.1).

7.4.4 Intégrité de sécurité et détection d'anomalie

Les CPI et les DLD doivent satisfaire aux exigences suivantes:

– en termes d'intégrité de sécurité du matériel, ce qui couvre:
  - les exigences du matériel (voir 7.4.6);
  - les contraintes architecturales relatives à l'intégrité de sécurité du matériel (voir 7.4.12);
  - les exigences relatives à la probabilité de défaillance dangereuse en cas de sollicitation (PFD) (voir 7.4.9);
– les exigences du logiciel (voir 7.4.7);
– en termes d'intégrité de sécurité systématique, ce qui couvre:
  - les exigences relatives au niveau d'intégrité de sécurité (SIL) (voir 7.4.5);
  - les exigences CEM (voir 7.7.5);
  - les exigences de communication de données, le cas échéant (voir 7.4.14.3.4);
  - les exigences d'évitement des défaillances (voir 7.4.14.1)
  - les exigences de maîtrise des anomalies systématiques (voir 7.4.14.2)
  - l'approche "efficacité éprouvée par une utilisation antérieure" (voir l'Article 9), preuve que les composants satisfont aux exigences applicables
– le comportement en cas de détection d'anomalie (voir 7.4.14.3)

7.4.5 Attribution du niveau d'intégrité de sécurité (SIL)

Le niveau SIL de la fonction de sécurité doit s'appliquer au logiciel et au matériel correspondants.

Si des niveaux SIL différents sont attribués à des fonctions de sécurité différentes d'un même dispositif, le SIL le plus élevé doit être utilisé à moins qu'il ne puisse être démontré que les différentes fonctions de sécurité sont suffisamment indépendantes en termes de matériel et de logiciel.

L'indépendance suffisante doit être prouvée en démontrant que la probabilité de défaillance dépendante entre les parties appliquant des fonctions de sécurité de niveaux d'intégrité différents est suffisamment faible par rapport à la probabilité de défaillance dangereuse pour le niveau d'intégrité de sécurité le plus élevé associé aux fonctions de sécurité impliquées.

7.4.6 Exigences relatives au matériel

Les CPI et les DLD doivent être conçus pour satisfaire aux exigences de la spécification des exigences de sécurité fonctionnelle.

Le matériel conçu et la documentation rédigée au cours des phases de conception et de documentation du cycle de vie des CPI et des DLD doivent satisfaire à l'ensemble des exigences suivantes:

– les exigences d'intégrité de sécurité du matériel, qui couvrent les contraintes architecturales relatives à l'intégrité de sécurité du matériel (7.4.12) et les exigences relatives à la probabilité de défaillance aléatoire (PFD) du matériel (7.4.9);

– les exigences relatives à l'intégrité de sécurité systématique qui couvrent les exigences d'évitement des défaillances (7.4.14.1) et les exigences de maîtrise des anomalies systématiques (7.4.14.2);
– les exigences relatives au comportement des CPI et des DLD suite à la détection d'un défaut (7.4.14.3);
– l'indépendance des fonctions de sécurité et des fonctions supplémentaires, à moins qu'elles ne soient toutes considérées comme relatives à la sécurité. L'indépendance doit être telle que les défaillances de parties intégrant des fonctions supplémentaires ne doivent pas entraîner de défaillances dangereuses des parties intégrant des fonctions de sécurité. La méthode utilisée pour obtenir cette indépendance et la justification correspondante doivent être documentées.

7.4.7 Exigences relatives au logiciel

Les logiciels utilisés pour les fonctions de sécurité doivent être conformes aux exigences définies dans la CEI 61508-3 pour le SIL correspondant.

NOTE L'Annexe D fournit un certain nombre d'instructions et de recommandations concernant l'utilisation de la CEI 61508-3.

7.4.8 Revue des exigences

Les exigences applicables aux matériels et logiciels relatifs à la sécurité doivent être revues afin de s'assurer qu'elles sont spécifiées de manière appropriée. Les points suivants doivent notamment être pris en considération:

– les fonctions de sécurité;
– les exigences d'intégrité de sécurité;
– les interfaces entre équipements et opérateurs.

7.4.9 Exigences relatives à la probabilité de défaillance dangereuse en cas de sollicitation (PFD)

7.4.9.1 Généralités

La PFD de chaque fonction de sécurité (ou groupe de fonctions de sécurité utilisées simultanément) devant être respectée par les CPI et les DLD, estimée conformément à 7.4.9 et à l'Annexe B, doit être inférieure ou égale aux données de défaillance cible (voir le Tableau 2) telles que spécifiées dans la spécification des exigences d'intégrité de sécurité (voir 7.2.1.2).

La valeur de la PFD, telle que définie par le SIL, se rapporte à l'ensemble d'une fonction de sécurité donnée.

La PFD doit être estimée séparément pour chaque fonction de sécurité (ou groupe de fonctions de sécurité utilisées simultanément) de l'CPI ou de l'DLD.

NOTE 1 Il existe nombre de méthodes de modélisation et la méthode la plus appropriée est à la discrétion de chaque analyste et dépend des circonstances particulières. Les méthodes possibles sont, entre autres:

– l'analyse par arbre de panne (voir la CEI 61025);
– les modèles de Markov (voir la CEI 61165);
– les blocs diagrammes de fiabilité (voir la CEI 61078).
– voir également la CEI 60300-3-1.

NOTE 2 La durée moyenne de rétablissement (MTTR) prise en considération dans le modèle de fiabilité tient compte des intervalles d'essais de diagnostic et d'essais périodiques, du temps de réparation et de tout autre délai précédant le rétablissement, ainsi que la durée de la mission.

NOTE 3 Les défaillances dues aux effets de cause commune et aux processus de communication de données peuvent avoir pour origine des effets autres que les défaillances réelles des composants du matériel (par exemple,

des erreurs de décodage). Toutefois, pour les besoins de la présente norme, les défaillances de ce type sont considérées comme étant des défaillances aléatoires du matériel (voir l'Annexe D de la CEI 61508-6:2010).

NOTE 4 L'Annexe B de la CEI 61508-6:2010 décrit une approche simplifiée qui peut être utilisée pour évaluer la probabilité de défaillance dangereuse d'une fonction de sécurité due à une défaillance aléatoire du matériel, permettant de déterminer si une architecture donnée respecte la mesure cible de défaillance exigée.

7.4.9.2 Estimation de la PFD

La PFD de chaque fonction de sécurité à réaliser par l'CPI ou l'DLD, due à des défaillances aléatoires du matériel, doit être estimée conformément à l'Annexe A de la CEI 61508-2:2010, en tenant compte des éléments suivants:

– l'architecture de l'CPI et de l'DLD, car elle dépend de chaque fonction de sécurité étudiée;

– le taux de défaillance estimé de chaque sous-système de l'CPI et de l'DLD, dans n'importe quel mode susceptible d'entraîner une défaillance dangereuse de l'CPI et de l'DLD, mais qui est détectée par les essais de diagnostic;

– le taux de défaillance estimé de chaque sous-système de l'CPI et de l'DLD, dans n'importe quel mode susceptible d'entraîner une défaillance dangereuse de l'CPI et de l'DLD, qui n'est pas détectée par les essais de diagnostic;

– la susceptibilité des CPI et des DLD aux défaillances de cause commune (voir l'Annexe D de la CEI 61508-6:2010);

– la couverture du diagnostic (DC) des essais de diagnostic (déterminée selon les Annexes A et C de la CEI 61508-2:2010), ainsi que l'intervalle entre essais de diagnostic correspondant;

NOTE 1 Pour établir l'intervalle entre essais de diagnostic, il faut tenir compte des intervalles entre tous les essais qui contribuent à la couverture du diagnostic.

– les intervalles de réalisation des essais périodiques, afin de révéler d'éventuelles défaillances dangereuses qui ne sont pas détectées par les essais de diagnostic;

En pratique, la mise en place d'essais périodiques pour certaines parties de l'CPI et de l'DLD peut s'avérer difficile. Dans ce cas, la durée de mission de ces parties ou de l'CPI et de l'DLD proprement dits peut servir d'intervalle entre essais périodiques.

– les temps de réparation des défaillances détectées;

NOTE 2 Le temps de réparation comprend une partie de la durée moyenne de rétablissement (MTTR), qui inclut également le temps nécessaire pour détecter une défaillance, ainsi que toute période au cours de laquelle aucune réparation n'est possible (l'Annexe B de la CEI 61508-6:2010 donne un exemple de la façon d'utiliser la durée moyenne de rétablissement pour calculer la probabilité de défaillance). Dans les cas où la réparation ne peut être effectuée qu'au cours d'une période spécifique, par exemple lorsque le réseau IT est à l'arrêt et à l'état de sécurité, il est particulièrement important de bien prendre en compte la période au cours de laquelle toute réparation est impossible, notamment lorsque celle-ci est relativement longue.

– le cas échéant, la probabilité de défaillance dangereuse de tout processus de communication des données (voir 7.4.14.3.4).

7.4.10 Données relatives aux taux de défaillance

Les données relatives aux taux de défaillance des composants doivent être obtenues à partir des éléments suivants:

– une source reconnue; ou

– des estimations fondées sur des composants dont l'efficacité est considérée éprouvée par une utilisation antérieure (voir l'Article 9).

Il convient d'utiliser la température moyenne de fonctionnement prévue d'un composant donné pour estimer son taux de défaillance.

Il convient que le niveau de confiance de toutes les données relatives aux taux de défaillance utilisées soit au moins égal à 60 % lorsque les valeurs sont extraites d'un recueil de données de fiabilité, et au moins égal à 70 % lorsque les valeurs proviennent d'autres types d'évaluation (par exemple, une auto-évaluation ou une évaluation par le fabricant).

NOTE Les valeurs peuvent être déduites de données publiées dans certaines normes (voir l'Annexe C) et sources industrielles.

On utilisera préférentiellement les données relatives aux défaillances spécifiques à un composant, si elles sont disponibles. À défaut, il convient d'utiliser les données génériques.

Bien que les méthodes d'estimation les plus probabilistes supposent un taux de défaillance constant, cela ne s'applique qu'à condition que la durée de vie utile des composants ne soit pas dépassée. Au-delà de cette durée de vie utile (sachant que la probabilité de défaillance augmente considérablement avec le temps), les résultats des méthodes de calcul les plus probabilistes ne sont donc plus représentatifs. Ainsi, il convient que toute estimation probabiliste comprenne une spécification de la durée de vie utile des composants. Cette durée de vie utile dépend en grande partie du composant lui-même et de ses conditions de fonctionnement, notamment la température (par exemple, les condensateurs électrolytiques peuvent y être très sensibles).

7.4.11 Intervalle entre essais de diagnostic

L'intervalle entre essais de diagnostic des CPI et des DLD doit permettre aux CPI et aux DLD de satisfaire aux exigences relatives à la PFD (voir 7.4.9.2).

Lorsqu'une panne dangereuse peut entraîner la perte de la fonction de sécurité, il est nécessaire de détecter cette panne dans les limites de couverture de diagnostic et de lancer une réaction au défaut afin de prévenir tout danger.

Les diagnostics et les fonctions de réaction aux défaillances doivent être réalisés dans le temps maximal spécifié de réaction aux défauts. Le temps maximal de réaction aux défauts doit être inférieur à 8 h pour les CPI et les DLD.

Pour tout sous-système d'un CPI ou d'un DLD ayant une tolérance zéro aux anomalies du matériel dont dépend entièrement une fonction de sécurité, l'intervalle entre essais de diagnostic doit être tel que la somme de l'intervalle entre essais de diagnostic et de la durée de réalisation d'une action donnée (fonction de réaction aux défaillances) pour atteindre ou maintenir un état de sécurité soit inférieure au temps maximal spécifié de réaction aux défauts.

7.4.12 Contraintes architecturales

7.4.12.1 Limitations du SIL

Dans le contexte de l'intégrité de sécurité du matériel, le niveau d'intégrité de sécurité le plus élevé qui peut être revendiqué pour une fonction de sécurité donnée est limité par la tolérance aux anomalies du matériel et par la proportion de défaillances en sécurité des sous-systèmes d'CPI ou d'DLD qui réalisent la fonction de sécurité. Une tolérance aux anomalies du matériel *N* signifie que *N*+1 anomalies risquent d'entraîner la perte de la fonction de sécurité.

Le Tableau 3 de la présente norme combine le contenu du Tableau 1 et du Tableau 2 spécifiés dans la CEI 61508-1:2010. Il spécifie le niveau d'intégrité de sécurité le plus élevé qui peut être revendiqué pour une fonction de sécurité qui utilise un sous-système donné, en tenant compte de la tolérance aux anomalies du matériel et de la proportion de défaillances en sécurité de ce sous-système (voir l'Annexe C de la CEI 61508-2:2010). Les exigences du Tableau 3 doivent être appliquées à chaque sous-système réalisant une fonction de sécurité et de ce fait, à toute partie de l'CPI ou de l'DLD dans ces sous-systèmes.

Pour ce qui concerne ces exigences:

– lors de la détermination de la tolérance aux anomalies du matériel, aucune autre mesure susceptible de contrôler les effets des défauts (telle que les diagnostics) ne doit être prise en compte;

– lorsqu'une anomalie donne directement lieu à l'apparition d'un ou de plusieurs défauts subséquents, ces derniers sont considérés comme un défaut unique.

– lors de la détermination de la tolérance aux anomalies du matériel, certains défauts peuvent être exclus, à condition que leur probabilité d'occurrence soit très faible par rapport aux exigences d'intégrité de sécurité du sous-système. Toute exclusion de défauts doit être justifiée et documentée.

7.4.12.2 Sous-systèmes de type A et de type B

7.4.12.2.1 Sous-système de type A

Un sous-système peut être considéré être un sous-système de type A si, pour les composants nécessaires à la réalisation de la fonction de sécurité:

– les modes de défaillance de tous les composants qui le constituent sont bien définis; et

– le comportement du sous-système dans des conditions de défaut peut être entièrement déterminé; et

– il existe suffisamment de données de défaillance fiables, obtenues à partir d'expériences sur le terrain, pour démontrer que les taux de défaillance revendiqués pour les défaillances dangereuses détectées et non détectées sont respectés.

7.4.12.2.2 Sous-système de type B

Un sous-système doit être considéré être un sous-système de type B si, pour les composants nécessaires à la réalisation de la fonction de sécurité, un ou plusieurs des critères applicables au sous-système de type A ne sont pas satisfaits.

En d'autres termes, si au moins l'un des composants d'un sous-système satisfait aux conditions applicables à un sous-système de type B, il convient alors de considérer l'ensemble du sous-système comme étant un sous-système de type B, et non un sous-système de type A.

NOTE À titre d'exemple, la section de commande constituée de microcontrôleurs, etc. est considérée comme étant un sous-système de type B.

7.4.12.3 Contraintes architecturales eu égard aux tolérances aux anomalies du matériel et à la proportion de défaillances en sécurité (SFF)

Les contraintes architecturales dans le Tableau 3 s'appliquent à chaque sous-système de type A ou de type B qui fait partie de l'CPI ou de l'DLD.

Tableau 3 – Intégrité de sécurité du matériel: contraintes architecturales sur les sous-systèmes relatifs à la sécurité de type A et de type B

Proportion de défaillances en sécurité[a]		Tolérance aux anomalies du matériel *N* (voir 7.4.12)		
Type A	Type B	0	1	2
–	<0 % à 60 %	Aucun SIL	SIL 1	SIL 2
<0 % à <60 %	60 % à < 90 %	SIL 1	SIL 2	–[b]
60 % à < 90 %	90 % à < 99 %	SIL 2	–[b]	–[b]
[a] Voir 7.4.13 pour plus de détails concernant l'estimation de la proportion de défaillances en sécurité (SFF). [b] La présente norme s'applique uniquement aux CPI et DLD ayant un niveau d'intégrité de sécurité inférieur ou égal à SIL 2				
NOTE Voir l'Annexe B.2 pour des exemples d'architectures d'CPI et d'DLD.				

7.4.13 Estimation de la proportion de défaillances en sécurité (SFF)

7.4.13.1 Méthodes d'analyse

Pour estimer la SFF d'un sous-système, une analyse (par exemple, une analyse par arbre de panne ou une analyse des modes de défaillance et de leurs effets (AMDE)) doit être effectuée afin d'identifier tous les défauts significatifs, ainsi que les modes de défaillance correspondants. La probabilité de chaque mode de défaillance du sous-système doit être déterminée en s'appuyant sur la probabilité du ou des défauts correspondants.

7.4.13.2 Bases de données

L'estimation de la SFF doit s'appuyer:

– soit sur des données relatives aux taux de défaillance significatives d'un point de vue statistique, obtenues à partir d'expériences sur le terrain; ou

– soit sur des données relatives aux défaillances des composants, obtenues à partir d'une source reconnue.

Voir également en 7.4.13.

7.4.13.3 Calcul de la SFF

La proportion de défaillances en sécurité d'un sous-système doit être calculée conformément à l'Annexe A et à l'Annexe C de la CEI 61508-2:2010.

7.4.14 Exigences relatives à l'intégrité de sécurité systématique

7.4.14.1 Exigences relatives à l'évitement des défaillances

7.4.14.1.1 Généralités

Des techniques et mesures doivent être utilisées pour réduire le plus possible la présence de défauts lors de la conception et du développement du matériel des CPI et des DLD.

Des essais, planifiés conformément à 7.4.14.1.4, doivent être effectués. Voir également en 7.7.2.

7.4.14.1.2 Sélection des méthodes de conception

En fonction du niveau d'intégrité de sécurité exigé, la méthode de conception choisie doit assurer:

– la transparence, la modularité et autres caractéristiques permettant de simplifier au maximum et d'améliorer la compréhension de la conception;

– une spécification claire et précise
  - de la fonctionnalité,
  - des interfaces des sous-systèmes,
  - de la séquence et des informations temporelles,
  - de la simultanéité et de la synchronisation;

– une documentation claire et précise ainsi que la communication d'informations;

– la vérification et la validation.

7.4.14.1.3 Mesures de conception

Les mesures de conception suivantes doivent être appliquées:

– conception appropriée de l'CPI ou l'DLD et/ou des sous-systèmes, y compris:

- l'utilisation de composants conformes aux spécifications des fabricants, concernant par exemple la température, le chargement, l'alimentation, la puissance assignée et les paramètres de temporisation;
- le déclassement des paramètres de conception afin d'améliorer la fiabilité si cela est nécessaire pour atteindre les taux de défaillance cibles;
- la combinaison et le montage corrects des sous-systèmes, par exemple pour ce qui concerne le câblage et les interconnexions;
- le recours à des revues et à des inspections pour la détection précoce d'éventuels défauts de conception.

– compatibilité:

- utilisation de sous-systèmes dont les caractéristiques de fonctionnement sont compatibles.

– résistance aux conditions d'environnement spécifiées:

- conception des CPI ou des DLD de sorte que leur fonctionnement soit sûr dans tous les environnements spécifiés, par exemple en termes de température, d'humidité, de vibrations, de phénomènes électromagnétiques, de degré de pollution, de catégorie de surtensions, d'altitude.

7.4.14.1.4 Planification des essais

Lors de la conception, les différents types d'essais suivants doivent être planifiés selon les besoins:

– essais des sous-systèmes;
– essais d'intégration;
– essais de validation;
– essais de configuration.

La documentation relative à la planification des essais doit préciser les points suivants:

– les types d'essais à réaliser ainsi que les procédures à suivre;
– l'environnement, les outils, la configuration et les programmes d'essai;
– les critères de réussite/échec aux essais.

Des outils d'essais automatiques et des outils de développement intégrés doivent, le cas échéant, être utilisés.

NOTE L'intégrité de ce type d'outils peut être démontrée grâce à des essais spécifiques, à une expérience d'utilisation longue et satisfaisante ou à une vérification indépendante de leurs résultats avec l'CPI ou l'DLD particulier en cours de conception.

7.4.14.1.5 Exigences relatives à la maintenance de la conception

Un processus relatif à la maintenance et aux nouveaux essais de conception doit être défini lors de la phase de conception, afin de s'assurer que l'intégrité de sécurité de l'CPI ou de l'DLD continue à respecter le niveau exigé après les différentes révisions de sa conception.

7.4.14.2 Exigences relatives à la maîtrise des anomalies systématiques

7.4.14.2.1 Caractéristiques de conception

Pour la maîtrise des anomalies systématiques, la conception doit utiliser des moyens qui confèrent à l'CPI ou l'DLD et à leurs sous-systèmes, une certaine tolérance à des anomalies telles que:

– les éventuelles anomalies résiduelles de conception du matériel, à moins que la probabilité d'anomalies de conception du matériel puisse être exclue en appliquant le Tableau A.15 de la CEI 61508-2:2010;
– les contraintes environnementales, notamment les perturbations électromagnétiques, en appliquant le Tableau A.16 de la CEI 61508-2:2010;
– les erreurs imputables à l'opérateur de l'CPI ou de l'DLD (voir le Tableau A.17 de la CEI 61508-2:2010);
– les anomalies résiduelles de conception du logiciel (voir 7.4.3 de la CEI 61508-3:2010 et le Tableau A.2);
– les erreurs et, le cas échéant, d'autres effets imputables à un quelconque processus de communication de données (voir 7.4.14.3.4).

7.4.14.2.2 Testabilité et maintenabilité

La testabilité et la maintenabilité doivent être prises en compte au cours des activités de conception et de développement, afin de faciliter la mise en œuvre de ces propriétés dans l'CPI ou l'DLD final.

7.4.14.2.3 Contraintes humaines

La conception de l'CPI ou de l'DLD doit tenir compte des aptitudes et des limites humaines et être adaptée aux tâches attribuées aux opérateurs et au personnel de maintenance. La conception des interfaces opérateur doit permettre une utilisation pratique pour l'homme et doit tenir compte du niveau probable de formation ou de sensibilisation des opérateurs.

7.4.14.2.4 Protection contre les modifications non intentionnelles

L'CPI ou l'DLD doit intégrer des mesures visant à le protéger (ou à faciliter sa protection) contre toute modification non intentionnelle du logiciel, du matériel, du paramétrage et de la configuration.

NOTE Voir la CEI 61508-7:2010, B.4.8.

7.4.14.2.5 Perte de l'alimentation électrique

L'CPI ou l'DLD doit être spécifié et conçu en tenant compte des effets d'une perte et d'un rétablissement de l'alimentation électrique.

7.4.14.3 Comportement en cas de détection d'anomalie

7.4.14.3.1 Détection d'anomalie

En cas de détection d'une défaillance dangereuse susceptible d'entraîner la perte de la fonction de sécurité, le système doit passer en position de sécurité dans le délai maximal imparti par le temps de sécurité du processus.

Pour les CPI et les DLD, le temps de sécurité du processus doit être inférieur à 8 h.

7.4.14.3.2 Tolérance aux anomalies supérieure à zéro

La détection d'une anomalie dangereuse (par des autotests ou tout autre moyen) dans tout sous-système ayant une tolérance aux anomalies du matériel supérieure à zéro doit entraîner:

– soit une fonction de réaction aux défaillances,
– soit l'isolement de l'CPI ou de l'DLD défectueux, pour permettre la poursuite du fonctionnement du système en toute sécurité pendant la réparation de la partie défectueuse. Si la réparation n'est pas terminée dans les délais de la durée moyenne de rétablissement (MTTR) supposée lors du calcul de la probabilité de défaillance dangereuse (voir 7.4.9), une fonction de réaction aux défaillances doit être lancée.

7.4.14.3.3 Tolérance zéro aux anomalies

La détection d'une anomalie dangereuse (par des autotests automatiques ou tout autre moyen) dans tout sous-système ayant une tolérance aux anomalies du matériel égale à zéro et dont dépend entièrement une fonction de sécurité doit entraîner une fonction de réaction aux défaillances.

7.4.14.3.4 Exigences pour la communication de données

En cas de recours à la communication de données pour la mise en œuvre d'une fonction de sécurité, la probabilité de défaillance non détectée du processus de communication doit être estimée en tenant compte des erreurs de transmission, des répétitions, des suppressions, des insertions, des modifications de séquence, de la corruption, du retard et du masquage. Cette probabilité doit être prise en compte pour l'estimation de la PFD de la fonction de sécurité due à des défaillances aléatoires du matériel (voir 7.4.9.2).Les actions nécessaires pour assurer la mesure exigée des défaillances du processus de communication doivent être mises en œuvre conformément aux exigences de la CEI 61508-2 et de la CEI 61508-3.

En cas de recours à la communication de données pour échanger des données relatives à la sécurité avec des sous-systèmes externes à l'CPI ou à l'DLD, les exigences ci-dessus s'appliquent à l'CPI ou à l'DLD ainsi qu'aux sous-systèmes correspondants.

7.5 Intégration des CPI et des DLD (phase 10.4)

7.5.1 Intégration du matériel

L'CPI ou l'DLD doit être intégré conformément à sa conception spécifiée.

Lors de l'intégration de l'ensemble des sous-systèmes et composants à l'CPI ou à l'DLD, ce dernier doit être soumis aux essais d'intégration spécifiés. Ces essais sont spécifiés dans le plan de vérification et doivent démontrer que tous les modules interagissent correctement pour remplir leurs fonctions prévues et qu'ils sont conçus de manière à ne pas réaliser de fonctions non prévues.

Les exigences relatives à l'intégration du matériel sont également satisfaites lorsque l'CPI ou l'DLD satisfait aux essais de type, conformément à la CEI 61557-8 ou à la CEI 61557-9, ainsi que selon 7.7.

7.5.2 Intégration du logiciel

L'intégration des modules/parties du logiciel relatif à la sécurité à l'CPI ou à l'DLD doit être réalisée conformément à la CEI 61508-3. Elle doit comporter les essais spécifiés dans le plan de vérification du logiciel, afin d'assurer la compatibilité du logiciel avec le matériel, de façon à satisfaire aux exigences fonctionnelles et de performances de sécurité.

NOTE Il n'est pas nécessaire de soumettre à essai toutes les combinaisons d'entrée. Les essais peuvent être effectués conformément à l'Annexe B de la CEI 61508-3.

7.5.3 Modifications en cours d'intégration

Pendant l'intégration, toute modification ou tout changement effectué sur l'CPI ou l'DLD doit faire l'objet d'une analyse d'impact qui doit permettre d'identifier tous les composants affectés, puis d'une vérification supplémentaire.

7.5.4 Essais d'intégration

L'essai ou les essais d'intégration doivent être spécifiés dans un plan de vérification. Un essai fonctionnel doit être réalisé, l'CPI ou l'DLD y recevant les données d'entrée ou valeurs de consigne qui définissent de manière appropriée le fonctionnement normal prévu. La fonction de sécurité est invoquée (en simulant un défaut d'isolement, par exemple) et son fonctionnement constaté est étudié et comparé avec celui qui est donné par la spécification.

7.6 Documentation des CPI et DLD relative aux procédures d'installation, de mise en service, d'exploitation et de maintenance (phase 10.5)

7.6.1 Généralités

Des instructions de fonctionnement doivent être fournies conformément aux exigences de la CEI 61557-8 pour les CPI et de la CEI 61557-9 pour les DLD. Les informations supplémentaires nécessaires à l'utilisateur et définies en 7.6 doivent être fournies en annexe aux instructions de fonctionnement ou dans des documents séparés.

Les instructions destinées à l'utilisateur contiennent des informations essentielles quant à la manière d'utiliser et d'entretenir les dispositifs relatifs à la sécurité. Il convient que toutes les consignes soient faciles à comprendre. Il convient d'utiliser des figures et des schémas pour décrire des procédures et situations complexes.

7.6.2 Spécification fonctionnelle

La spécification fonctionnelle doit décrire les fonctions de sécurité ainsi que leurs conditions de fonctionnement et les restrictions correspondantes.

7.6.3 Informations concernant la conformité

Les informations concernant la conformité de la sécurité fonctionnelle aux exigences de la présente norme doivent être fournies à l'utilisateur sur demande.

Ces informations doivent comprendre les points obligatoires suivants:

– le niveau d'intégrité de sécurité (SIL) et les conditions correspondantes,
– la probabilité de défaillance en cas de sollicitation (PFD).

7.6.4 Informations de mise en service, d'installation, de mise en fonctionnement, d'exploitation et de maintenance

7.6.4.1 Généralités

Les informations selon 7.6.4.2 à 7.6.4.6 permettant d'assurer et de maintenir le niveau défini de sécurité fonctionnelle des CPI et des DLD dans l'application doivent être fournies.

7.6.4.2 Informations de mise en service

Ces informations doivent inclure toutes les conditions et restrictions d'application des CPI et des DLD à respecter pour que les fonctions de sécurité remplissent leur rôle.

7.6.4.3 Informations d'installation

Ces informations doivent inclure toutes les conditions et restrictions d'installation des CPI et des DLD qui doivent être respectées pour que les fonctions de sécurité remplissent leur rôle ainsi que les informations d'identification des versions matérielles et logicielles.

7.6.4.4 Information de mise en fonctionnement

Ces informations doivent fournir toutes les exigences de mise en service des CPI et des DLD afin qu'ils assurent leurs fonctions de sécurité.

Ceci doit comprendre:

– les réglages des fonctions de sécurité et des fonctions supplémentaires,
– les mesures destinées à prévenir toute modification non autorisée des réglages,
– les essais à effectuer sur l'CPI ou l'DLD proprement dit et sur le réseau IT,

– la documentation des essais, avec identification des différents essais, les résultats escomptés et les personnes chargées des essais.

7.6.4.5 Informations relatives à l'exploitation

Ces informations doivent fournir toutes les exigences et restrictions de fonctionnement des CPI et des DLD afin qu'ils assurent correctement leurs fonctions de sécurité.

Ceci doit comprendre:

– les intervalles entre les essais nécessaires au maintien des fonctions de sécurité et de la couverture du diagnostic (DC);
– les réactions nécessaires aux défaillances observées au cours des essais et aux éventuelles indications d'anomalie des dispositifs;
– la documentation et/ou la surveillance des essais et du fonctionnement.

7.6.4.6 Informations de maintenance

Ces informations doivent fournir toutes les exigences de maintenance pendant toute la durée de vie des CPI et des DLD, afin que ces dispositifs assurent correctement leurs fonctions de sécurité.

Ceci doit comprendre:

– les actions courantes éventuellement requises pour l'entretien des dispositifs afin qu'ils assurent leurs fonctions de sécurité;
– les actions de maintenance nécessaires suite à des échecs aux essais ou à des indications d'anomalie des dispositifs;
– les mesures après réparation et réinstallation des dispositifs;
– les mesures de mises à jour des logiciels et, le cas échéant, les essais qui en découlent;
– les informations de fin de vie pour le remplacement des dispositifs, si nécessaire.

7.7 Validation de la sécurité des CPI et DLD (phase 10.6)

7.7.1 Généralités

Les essais, la vérification et la validation doivent être effectués pour s'assurer de la conformité au plan de sécurité fonctionnelle (voir 7.3.2).

7.7.2 Essais

Les essais des fonctions de sécurité de l'CPI ou de l'DLD doivent être effectués simultanément à chaque phase du processus de développement.

Les essais doivent être documentés et doivent comporter une description détaillée:

– des essais fonctionnels de chaque fonction de sécurité;
– des essais fonctionnels de chaque fonction de diagnostic pour chaque fonction de sécurité,
– des critères d'acceptation.

Il peut s'agir soit d'essais en boîte noire, c'est-à-dire ne tenant pas compte de la mise en œuvre interne de la fonction de sécurité, soit d'essais en boîte blanche, c'est-à-dire reposant sur une connaissance spécifique de la mise en œuvre de la fonction de sécurité permettant de déterminer l'essai (par exemple, l'insertion d'anomalies).

Les essais peuvent être supprimés ou remplacés par d'autres méthodes de vérification ou de validation si les exigences pertinentes le permettent.

7.7.3 Vérification

Au cours du processus de conception, on doit vérifier, après chaque phase de conception, que les exigences de la phase concernée ont été remplies et enregistrer les résultats correspondants. Pour la vérification, il peut être procédé à une évaluation, une analyse, un examen, une revue et/ou des essais.

NOTE La vérification peut comporter, par exemple:

– une revue de la documentation de la phase correspondante,

– des revues de conception,

– des essais fonctionnels.

7.7.4 Validation

À l'issue du processus de conception, on doit vérifier que l'CPI ou l'DLD satisfait à toutes les exigences de la spécification des exigences de sécurité et enregistrer les résultats correspondants. Pour la validation, il peut être procédé à une évaluation, une analyse, un examen, une revue et/ou des essais. Le Tableau B.5 de la CEI 61508-2:2010 fournit des recommandations permettant d'éviter les anomalies pendant la validation.

7.7.5 Exigences CEM

7.7.5.1 Généralités

Des essais d'immunité CEM doivent être réalisés, pour les fonctions de sécurité, conformément aux exigences de la CEI 61326-3-1 et de la CEI 61326-2-4.

Les critères de performance qui doivent être appliqués lors de la réalisation des essais d'immunité électromagnétique sur l'CPI ou l'DLD sont spécifiés en 7.7.5.3. Ces critères ne s'appliquent pas aux fonctions supplémentaires (non relatives à la sécurité) des dispositifs, auxquelles s'appliquent uniquement les exigences de la CEI 61326-2-4.

7.7.5.2 Environnement prévu

L'environnement électromagnétique spécifié ou anticipé pour l'usage prévu d'un CPI ou d'un DLD doit servir de base pour déterminer les niveaux d'essais d'immunité électromagnétique. Pour les essais d'immunité, les essais du Tableau 101 de la CEI 61326-2-4:2006 s'appliquent, et ce, en utilisant toutefois les niveaux d'essais renforcés des Tableaux 1a) à 1f) de la CEI 61326-3-1:2008.

7.7.5.3 Critères de performance

Les critères de performance applicables aux essais d'immunité électromagnétique d'un CPI ou d'un DLD de sécurité fonctionnelle sont les mêmes qu'en fonctionnement normal. Les critères de performance du Tableau 102 de la CEI 61326-2-4:2006 s'appliquent, et ce, en utilisant toutefois des niveaux d'essai plus élevés tels que définis en 7.7.5.2.

7.7.5.4 Introduction de dangers

Lors d'un essai d'immunité électromagnétique, aucune condition non sûre et aucun danger ne doivent être introduits par l'CPI ou l'DLD. Les conditions non sûres ou les situations dangereuses doivent être définies dans la spécification d'intégrité de sécurité.

7.7.5.5 Vérification

Lors de la réalisation des essais d'immunité électromagnétique, les mesures d'atténuation spécifiées doivent être mises en place.

En fonction des résultats de l'analyse de l'environnement électromagnétique défini de l'application prévue de l'CPI ou de l'DLD, l'immunité renforcée (conformément aux exigences de la CEI 61508-2) doit être vérifiée.

7.7.5.6 Essai d'émission

Les essais d'émission sont identiques à ceux réalisés pour des CPI ou des DLD ordinaires non destinés à des applications de sécurité fonctionnelle (voir la CEI 61557-8 et la CEI 61557-9).

8 Exigences applicables aux modifications

8.1 Généralités

L'objectif de cet Article 8 est de garantir le maintien de la sécurité fonctionnelle de l'CPI et de l'DLD en cas de modification de la conception, une fois lancée la fabrication de la conception initiale.

Avant de procéder à une modification, des procédures doivent être planifiées. Les modifications doivent être apportées avec au moins le même niveau d'expertise, les mêmes outils automatiques, la même planification et la même gestion que ceux utilisés lors du développement initial de l'CPI et de l'DLD. Les modifications doivent être réalisées conformément à la planification.

8.2 Demande de modification

La modification doit être lancée uniquement après soumission d'une demande de modification, conformément aux procédures de gestion de la sécurité fonctionnelle (voir l'Article 6). La demande doit comporter les indications suivantes:

– les motifs de cette modification,

– la modification proposée (tant du point de vue matériel que logiciel).

8.3 Analyse d'impact

L'impact de la modification proposée sur la sécurité fonctionnelle de l'CPI et de l'DLD doit faire l'objet d'une évaluation. Cette dernière doit inclure une analyse permettant de déterminer dans quelle mesure il est nécessaire de revenir aux étapes de développement concernées selon 7.4.

8.4 Autorisation

L'autorisation de procéder à la modification demandée doit reposer sur les résultats de l'analyse d'impact.

9 Approche "efficacité éprouvée par une utilisation antérieure"

Les exigences de la présente norme doivent être satisfaites en adhérant au processus "efficacité éprouvée par l'utilisation antérieure" selon 7.4.10 de la CEI 61508-2:2010.

Annexe A
(informative)

Analyse du risque et attribution du SIL aux CPI et DLD

A.1 Généralités

La présente Annexe A est informative et fournit des exemples d'estimation du risque sur des réseaux IT, qui peuvent être appliqués pour attribuer des niveaux d'intégrité de sécurité (SIL) aux fonctions de sécurité des CPI et des DLD.

Le SIL de la fonction de sécurité correspondante de l'CPI ou de l'DLD dépend de l'estimation du risque lié à cette fonction de sécurité sur le réseau IT où les dispositifs sont utilisés. Pour des fonctions de sécurité différentes d'un CPI ou d'un DLD, il peut être assigné des SIL différents en fonction de l'analyse du risque pour la fonction de sécurité correspondante du réseau IT dans son ensemble.

Dans la présente Partie de la CEI 61557, l'EUC (équipement commandé selon la série de normes CEI 61508) fait référence au réseau IT et comprend également les charges telles que définies à la Figure A.1.

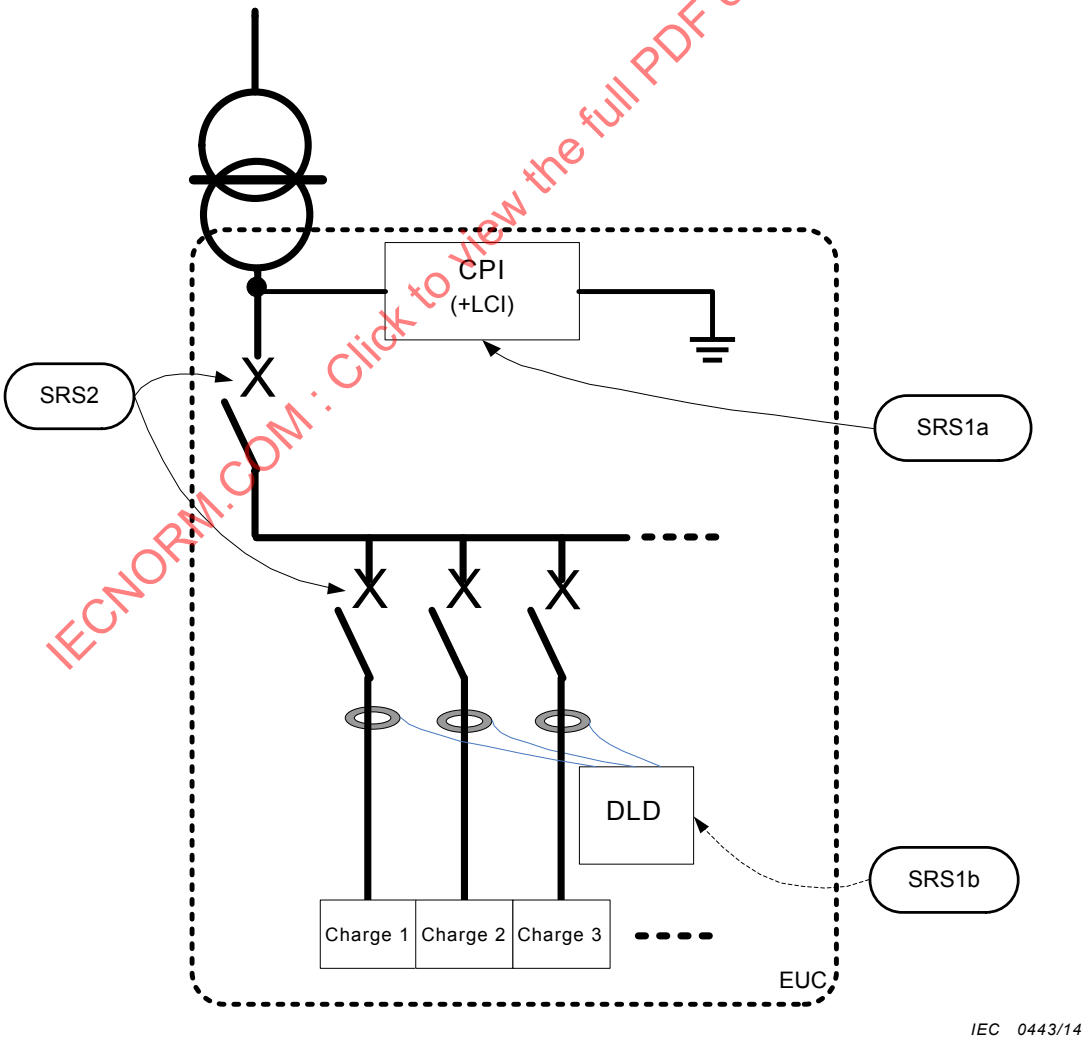


Figure A.1 – Éléments fonctionnels d'un réseau IT et leur rapport avec les définitions et abréviations de la série de normes CEI 61508

Le SRS (système relatif à la sécurité selon la série de normes CEI 61508) fait référence aux mesures de protection relatives à l'EUC. Ce SRS peut être divisé en différents niveaux de mesures de protection:

– SRS 1a: Système relatif à la sécurité chargé de la surveillance du réseau IT et qui émet une alarme en cas de défaut unique. Le SRS 1a est fondé sur des fonctions de sécurité assurées par des CPI.
– SRS 1b: système relatif à la sécurité chargé de la surveillance des lignes d'alimentation et de la localisation d'un premier défaut, de manière à faciliter les opérations de maintenance. Le SRS 1b est facultatif et fondé sur des fonctions de sécurité assurées par des DLD.
– SRS 2: système relatif à la sécurité chargé du déclenchement de l'ensemble du réseau IT ou d'une partie de ce réseau IT lorsqu'un deuxième défaut d'isolement apparaît avant d'avoir remédié au premier défaut. Le SRS 2 est fondé sur des fonctions de sécurité assurées par des disjoncteurs.

Les exigences de la CEI 61508 sont fondées sur une analyse du risque qui donne lieu à la définition du niveau SIL demandé pour le SRS. Le Tableau A.1 ci-après fournit un exemple d'analyse du risque (fondée sur la Figure A.1) portant sur diverses applications utilisant des réseaux IT:

Tableau A.1 – Analyse du risque d'un réseau IT

Application	Motif	Analyse du risque	La sécurité fonctionnelle est-elle applicable?
Utilisation du réseau IT, SRS 1a pour la surveillance de ce réseau IT, SRS 2 pour la protection de ce réseau IT.	Le réseau IT est utilisé à des fins de continuité de l'alimentation (pas de déclenchement en présence d'un premier défaut d'isolement).	La disponibilité est demandée pour des raisons économiques: – industrie en général, – applications marines en général.	Non, mais facultative.
		La disponibilité est requise pour des raisons de sécurité, par exemple: – salles d'opération et unités de soins intensifs dans des hôpitaux (locaux à usages médicaux de groupe 2), – applications marines (navires, installations au large des côtes, etc.), – chimie, – applications ferroviaires, – parties de systèmes de contrôle-commande dans des centrales nucléaires.	Hautement recommandée, il convient qu'elle couvre divers risques ayant un impact sur l'homme.
	Le réseau IT est utilisé pour prévenir la circulation de courants dangereux en présence d'un premier défaut d'isolement.	Le premier défaut d'isolement peut augmenter les risques de courants de contact dangereux dans les applications suivantes: – salles d'opération et unités de soins intensifs dans des hôpitaux.	Hautement recommandée, il convient qu'elle couvre les risques de choc ayant un impact sur l'homme.

Application	Motif	Analyse du risque	La sécurité fonctionnelle est-elle applicable?
		La circulation du courant peut être à l'origine d'un incendie, par exemple dans les applications suivantes: – parcs photovoltaïques	Hautement recommandée, il convient qu'elle couvre les risques d'incendie ayant un impact sur l'homme.
	Le réseau IT est utilisé pour prévenir la formation d'arcs en présence d'un deuxième défaut d'isolement (il y a formation d'arc lorsqu'il y a déclenchement du système SRS 2).	Un arc électrique peut être dangereux, par exemple dans les applications suivantes: – mines, – chimie (pour les zones à risques), – installations au large des côtes (pour les zones à risques).	Hautement recommandée, il convient qu'elle couvre les risques d'incendie ou d'explosion ayant un impact sur l'homme.
Utilisation de systèmes SRS 1b facultatifs dans les réseaux IT.	Tout motif	En cas de défaut d'isolement unique, il est urgent de localiser le défaut afin de réduire la durée moyenne de rétablissement (MTTR) et par conséquent la période au cours de laquelle un second défaut d'isolement peut apparaître.	Non, mais facultative.
NOTE Des exemples d'applications types sont donnés en Annexe F.			

A.2 Attribution du SIL aux CPI et aux DLD

Le Tableau A.2 donne un certain nombre d'instructions et de recommandations concernant le niveau SIL applicable pertinent.

Tableau A.2 – Attribution des SIL aux CPI et aux DLD

Applications utilisant des fonctions d'CPI	Applications utilisant des fonctions d'IFL	Exigences applicables aux dispositifs correspondants
Applications d'usage général utilisant des CPI pour avertir l'équipe de maintenance qu'un premier défaut a lieu sur un réseau IT donné.	Applications d'usage général utilisant des DLD pour apporter une aide à l'équipe de maintenance en matière de localisation des défauts d'isolement d'un réseau IT.	CPI conforme à la CEI 61557-8 DLD conforme à la CEI 61557-9

Applications utilisant des fonctions d'CPI	Applications utilisant des fonctions d'IFL	Exigences applicables aux dispositifs correspondants
Applications de sécurité dans lesquelles des CPI sont supposés réaliser des fonctions de sécurité avec un niveau SIL compatible avec le niveau SIL demandé par l'application (voir l'analyse du risque définie en Figure B.1), par exemple des applications où: – la sécurité est fondée sur la continuité d'alimentation: il est recommandé un niveau SIL 1. – la sécurité est fondée sur la réaction immédiate à un signal d'avertissement par le personnel qui surveille le réseau IT: il est recommandé un niveau SIL 1. – la sécurité est fondée sur l'utilisation d'un signal d'avertissement comme moyen d'activer des fonctions supplémentaires de sécurité ou un déclenchement: un niveau SIL 1 ou SIL 2 est recommandé.	Applications de sécurité dans lesquelles des DLD sont supposés réaliser des fonctions de sécurité avec un niveau SIL compatible avec le niveau SIL demandé par l'application (voir l'analyse de risque définie en Figure B.1), par exemple des applications où: – la sécurité est fondée sur la localisation d'un défaut d'isolement en un intervalle de temps défini (par exemple, le temps critique de réparation): il est recommandé un niveau SIL 1. – la sécurité est fondée sur la localisation immédiate d'un défaut d'isolement sous la valeur de réponse de l'CPI: il est recommandé un niveau SIL 1. – la sécurité est fondée sur la réaction immédiate à un signal d'avertissement par le personnel qui surveille le réseau IT: il est recommandé un niveau SIL 1. – la sécurité est fondée sur l'utilisation d'un signal d'avertissement comme moyen d'activer des fonctions supplémentaires de sécurité ou un déclenchement: un niveau SIL 1 ou SIL 2 est recommandé.	CPI conforme à la CEI 61557-8 et à la CEI 61557-15 DLD conforme à la CEI 61557-9 et à la CEI 61557-15

A.3 Exemple de graphique de risque

Le graphique de risque de la Figure A. est fondé sur les données fournies en exemple dans le Tableau A.4. Pour la détermination du niveau SIL des CPI ou DLD, il convient d'utiliser comme hypothèse les risques spécifiés de l'application correspondante.