

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

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

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 utmost 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.

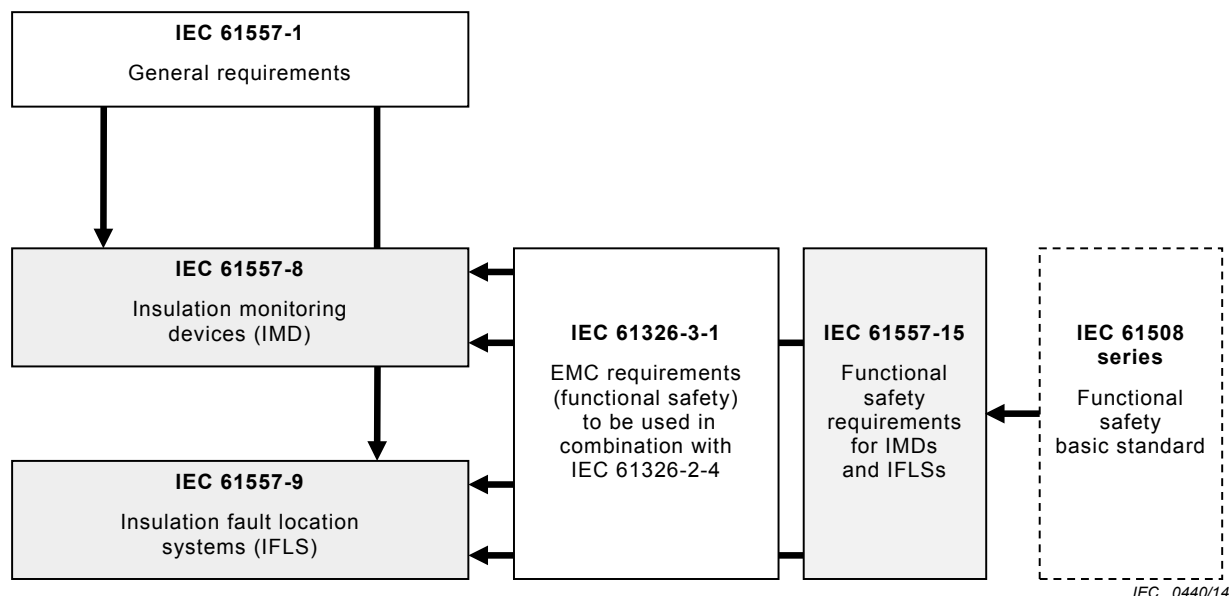


Figure 1 – Relationship between IEC 61557-15 and related standards

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*

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.

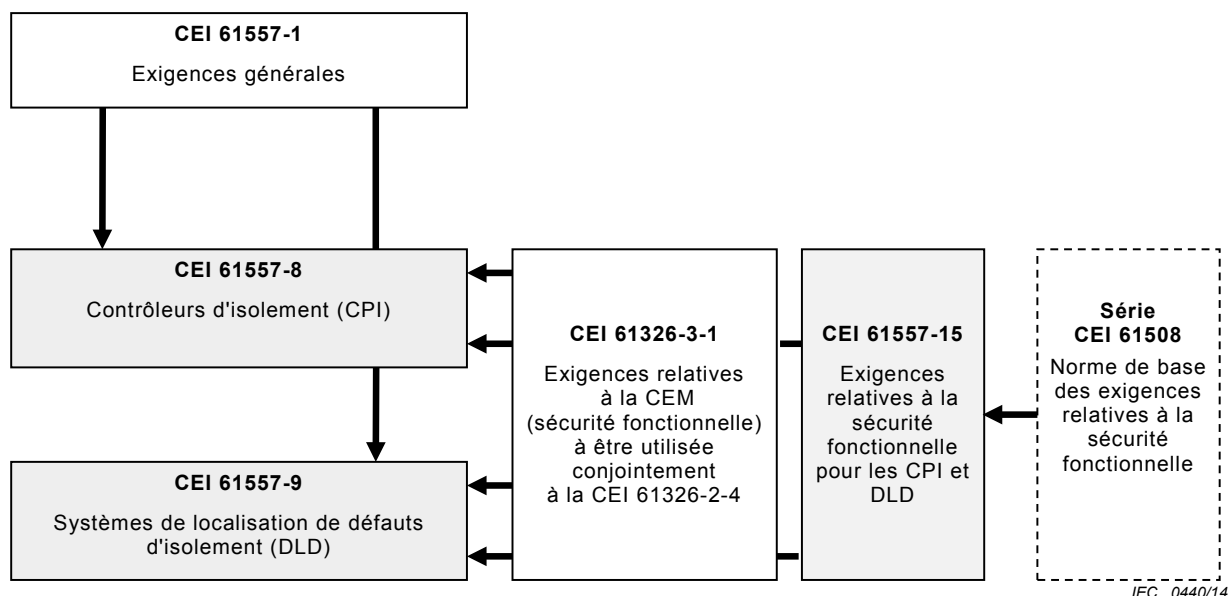


Figure 1 – Rapport entre la CEI 61557-15 et les normes apparentées

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 normative

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*