BS EN 61557-15:2014

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 61557-15:2014. It is identical to IEC 61557-15:2014.

The UK participation in its preparation was entrusted to Technical Committee PEL/85, Measuring equipment for electrical and electromagnetic quantities.

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

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

Published by BSI Standards Limited 2014

ISBN 978 0 580 71593 8
ICS 17.220.20; 29.080.01; 29.240.01

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2014.

Amendments/corrigenda issued since publication

Amd. No.	Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61557-15

May 2014

ICS 17.220.20; 29.080.01; 29.240.01

English Version

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 (IEC 61557-15:2014)

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
(CEI 61557-15:2014)

Elektrische Sicherheit in Niederspannungsnetzen bis AC 1 000 V und DC 1 500 V - Geräte zum Prüfen, Messen oder Überwachen von Schutzmaßnahmen - Teil 15: Anforderungen zur Funktionalen Sicherheit von Isolationsüberwachungsgeräten in IT-Systemen und von Einrichtungen zur Isolationsfehlersuche in IT-Systemen
(IEC 61557-15:2014)

This European Standard was approved by CENELEC on 2014-03-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

The text of document 85/465/FDIS, future edition 1 of IEC 61557-15, prepared by IEC/TC 85 "Measuring equipment for electrical and electromagnetic quantities" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61557-15:2014.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2014-12-19
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2017-03-19

This standard is to be used in conjunction with EN 61557-8 and EN 61557-9.

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

This standard covers the Principle Elements of the Safety Objectives for Electrical Equipment Designed for Use within Certain Voltage Limits (LVD).

Endorsement notice

The text of the International Standard IEC 61557-15:2014 was approved by CENELEC as a European Standard without any modification.

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

IEC 60300-3-1	NOTE	Harmonized as EN 60300-3-1.
IEC 60335-1:2001	NOTE	Harmonized as EN 60335-1:2002 [1)] (not modified).
IEC 60335-1:2001/A1:2004	NOTE	Harmonized as EN 60335-1:2002/A1:2004 [1)] (not modified).
IEC 60335-1:2001/A2:2006 + Corr. 08-2006	NOTE	Harmonized as EN 60335-1:2002/A2:2006 [1)] (not modified).
IEC 60364-4-41:2005	NOTE	Harmonized as HD 60364-4-41:2007 (modified).
IEC 60364-5-55:2011	NOTE	Harmonized as HD 60364-5-559:2012 (modified).
IEC 60364-7-710:2002	NOTE	Harmonized as HD 60364-7-710:2012 (modified).
IEC 60730-1:2010	NOTE	Harmonized as EN 60730-1:2011 (modified).
IEC 60812:2006	NOTE	Harmonized as EN 60812:2006 (not modified).
IEC 61010-1:2010 + Corr. 05-2011	NOTE	Harmonized as EN 61010-1:2010 (not modified).
IEC 61025	NOTE	Harmonized as EN 61025.
IEC 61078	NOTE	Harmonized as EN 61078.
IEC 61165	NOTE	Harmonized as EN 61165.
IEC 61508-7:2010	NOTE	Harmonized as EN 61508-7:2010 (not modified).
IEC 61709:1996	NOTE	Harmonized as EN 61709:1998 [2)] (not modified).
IEC 61784-3:2007	NOTE	Harmonized as EN 61784-3:2008 [3)] (not modified).
IEC 61800-5-2:2007	NOTE	Harmonized as EN 61800-5-2:2007 (not modified).
IEC/ISO 31010:2009	NOTE	Harmonized as EN 31010:2010 (not modified).
ISO 9001:2008	NOTE	Harmonized as EN ISO 9001:2008 (not modified).

[1)] Superseded by EN 60335-1:2012 (IEC 60335-1:2010, mod.)

[2)] Superseded by EN 61709:2011 (IEC 61709:2011).

[3)] Superseded by EN 61784-3:2010 (IEC 61784-3:2010).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu

Publication	Year	Title	EN/HD	Year
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	EN 61326-2-4	2013
IEC 61326-3-1 + corr. August	2008 2008	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications	EN 61326-3-1	2008
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2010
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010
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	EN 61508-5	2010

Publication	Year	Title	EN/HD	Year
IEC 61508-6	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	EN 61508-6	2010
IEC 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	EN 61557-1	-
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	EN 61557-8	-
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	EN 61557-9	2009

CONTENTS

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.

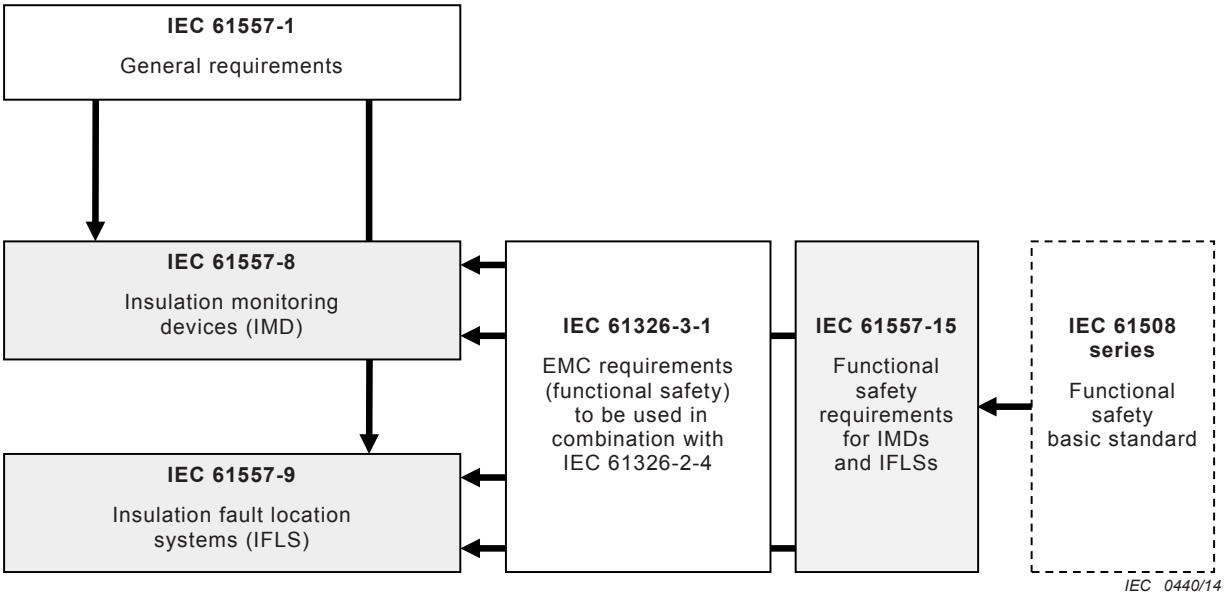


Figure 1 – Relationship between IEC 61557-15 and related standards

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.

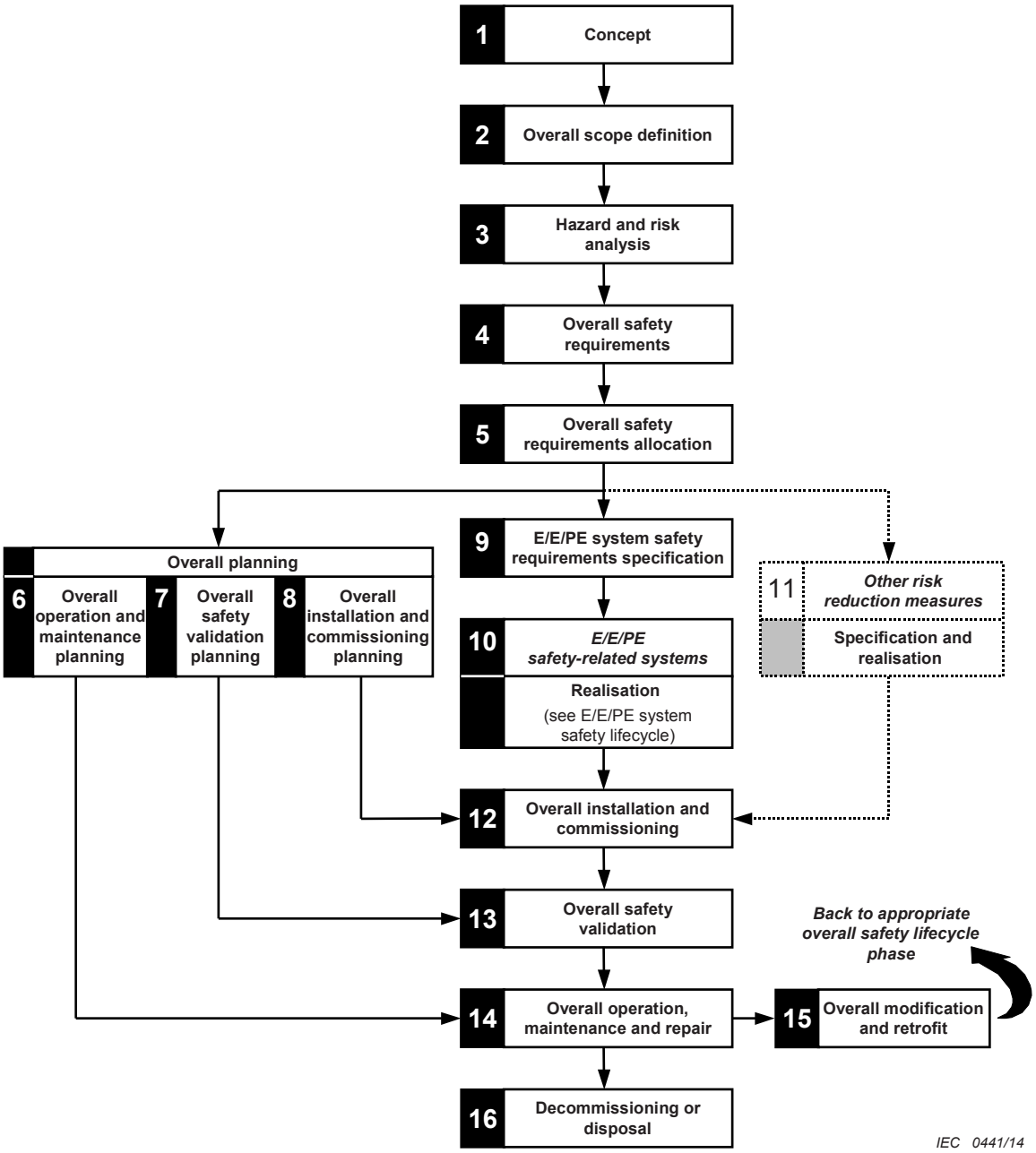


Figure 2 – Overall safety lifecycle applicable to an IT system

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.

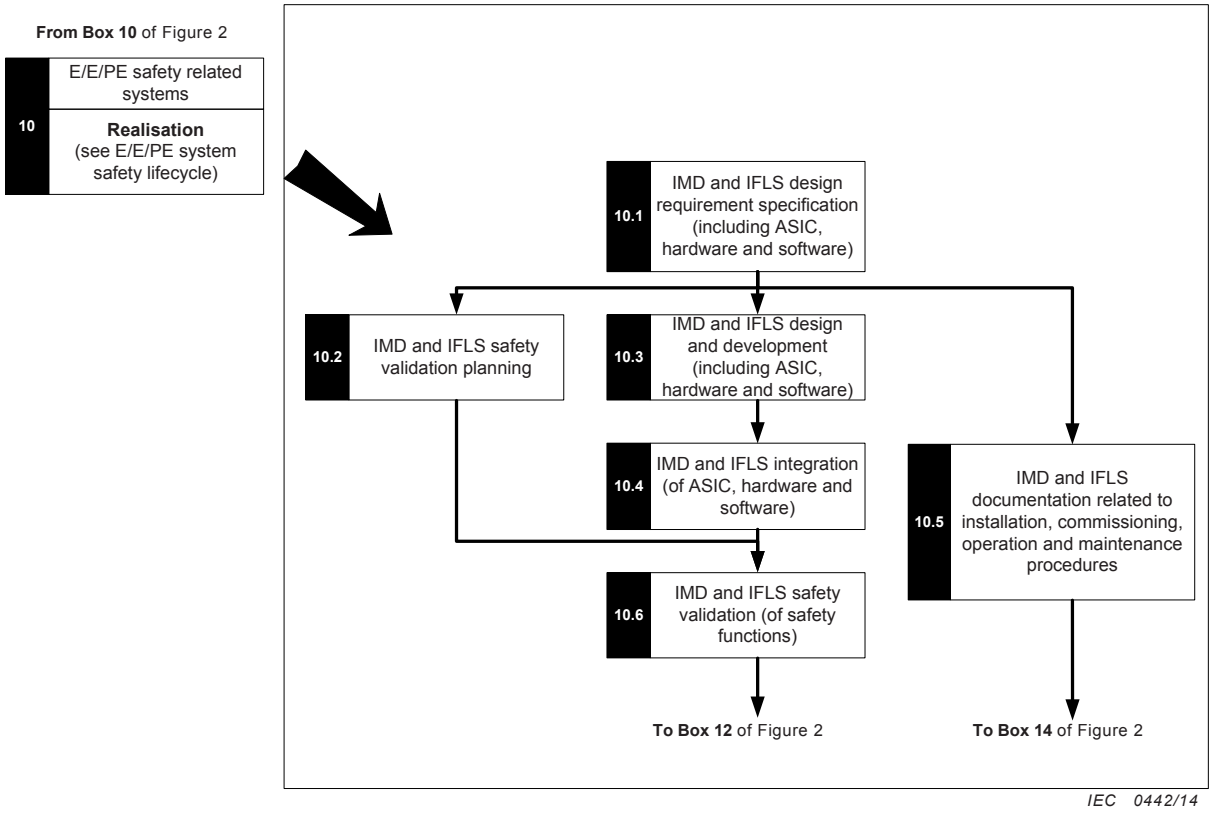


Figure 3 – IMD and IFLS safety lifecycle (in realisation phase)

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.

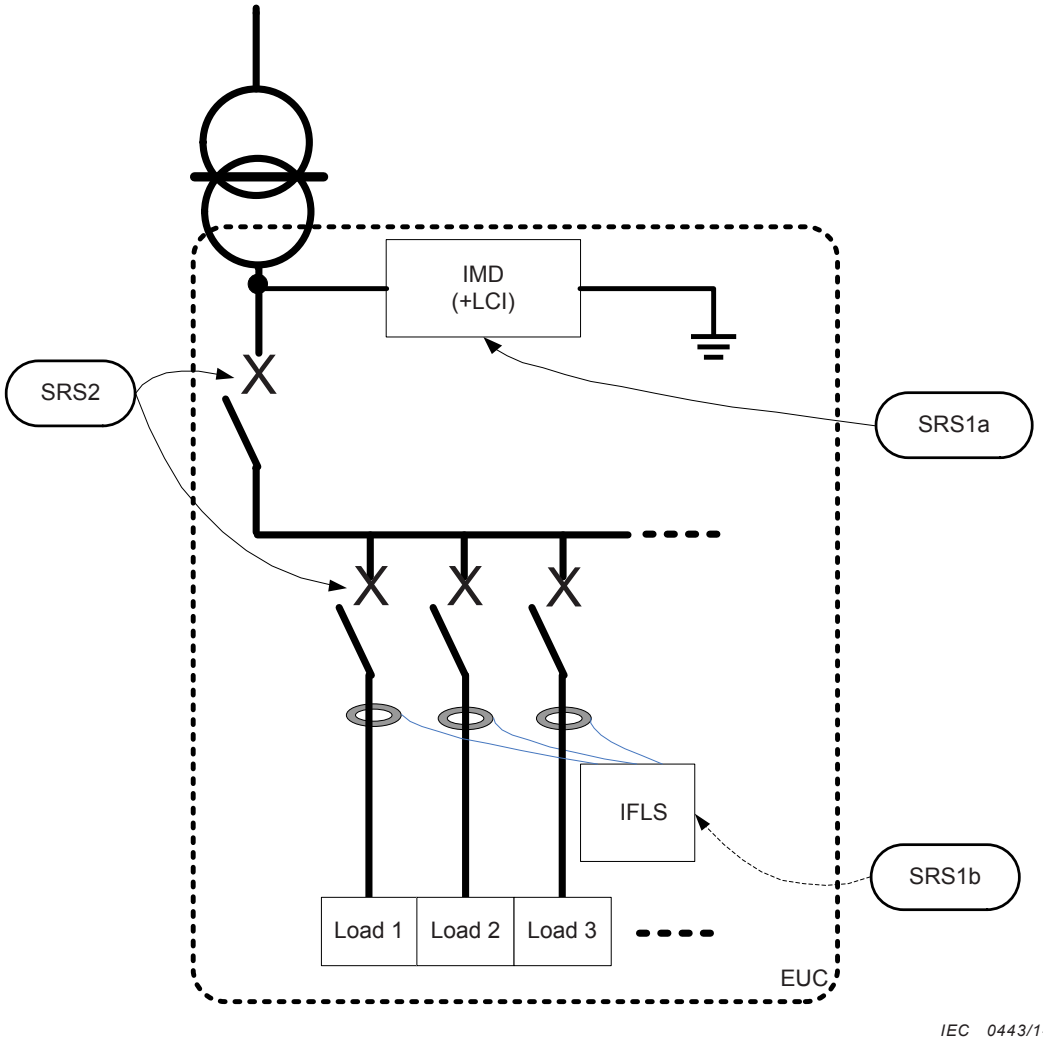


Figure A.1 – Functional elements of an IT system and their relationship to the definitions and abbreviations of the IEC 61508 series

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

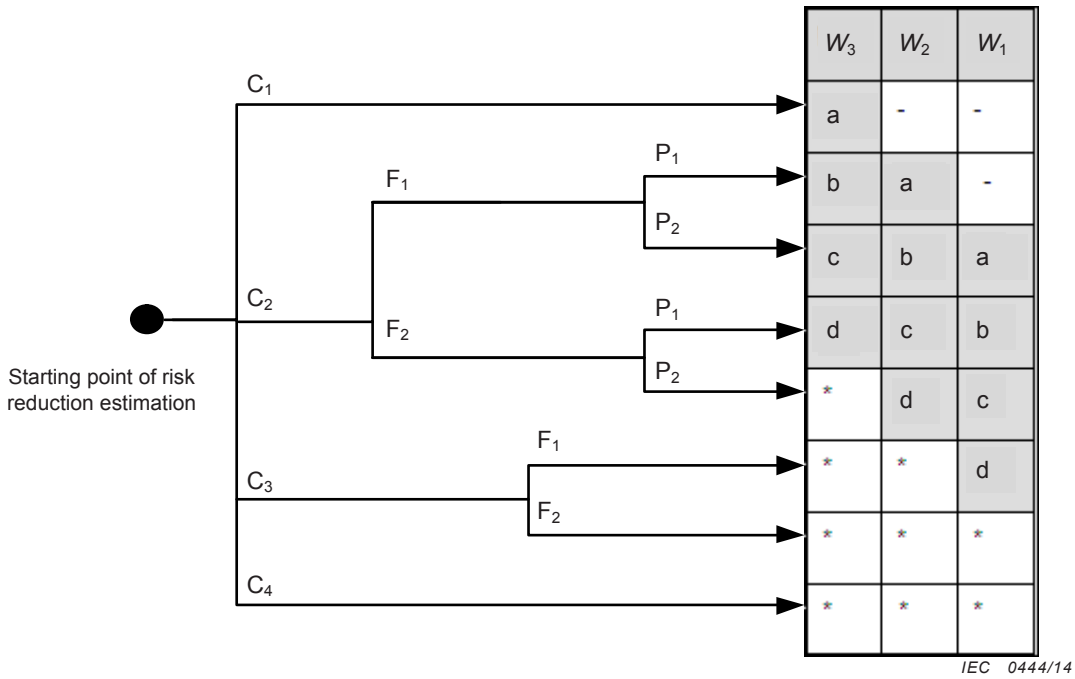
Table A.2 provides some guidance about the relevant applicable SIL level.

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.

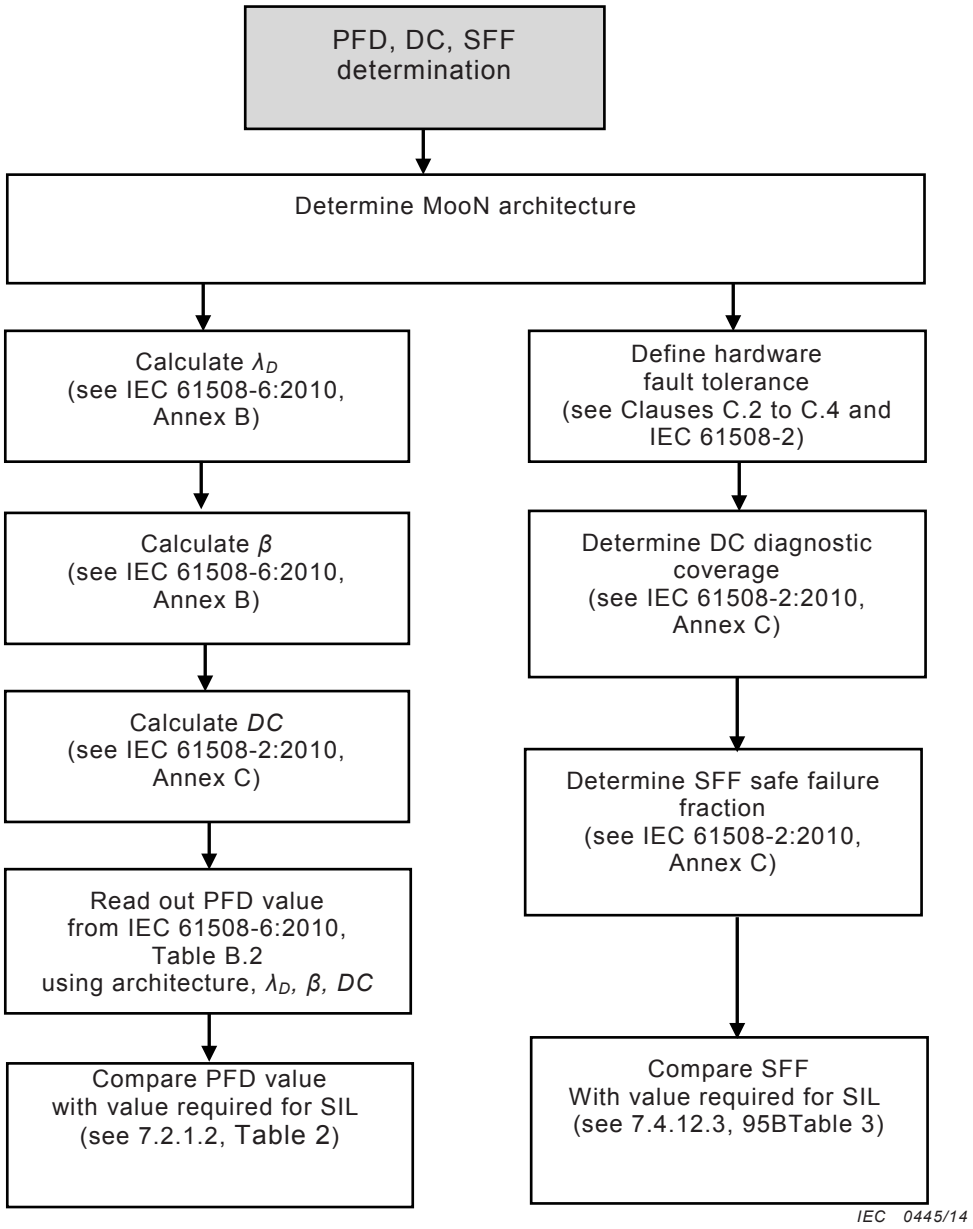


Figure B.1 – Flowchart for PFD, DC, SFF determination

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.

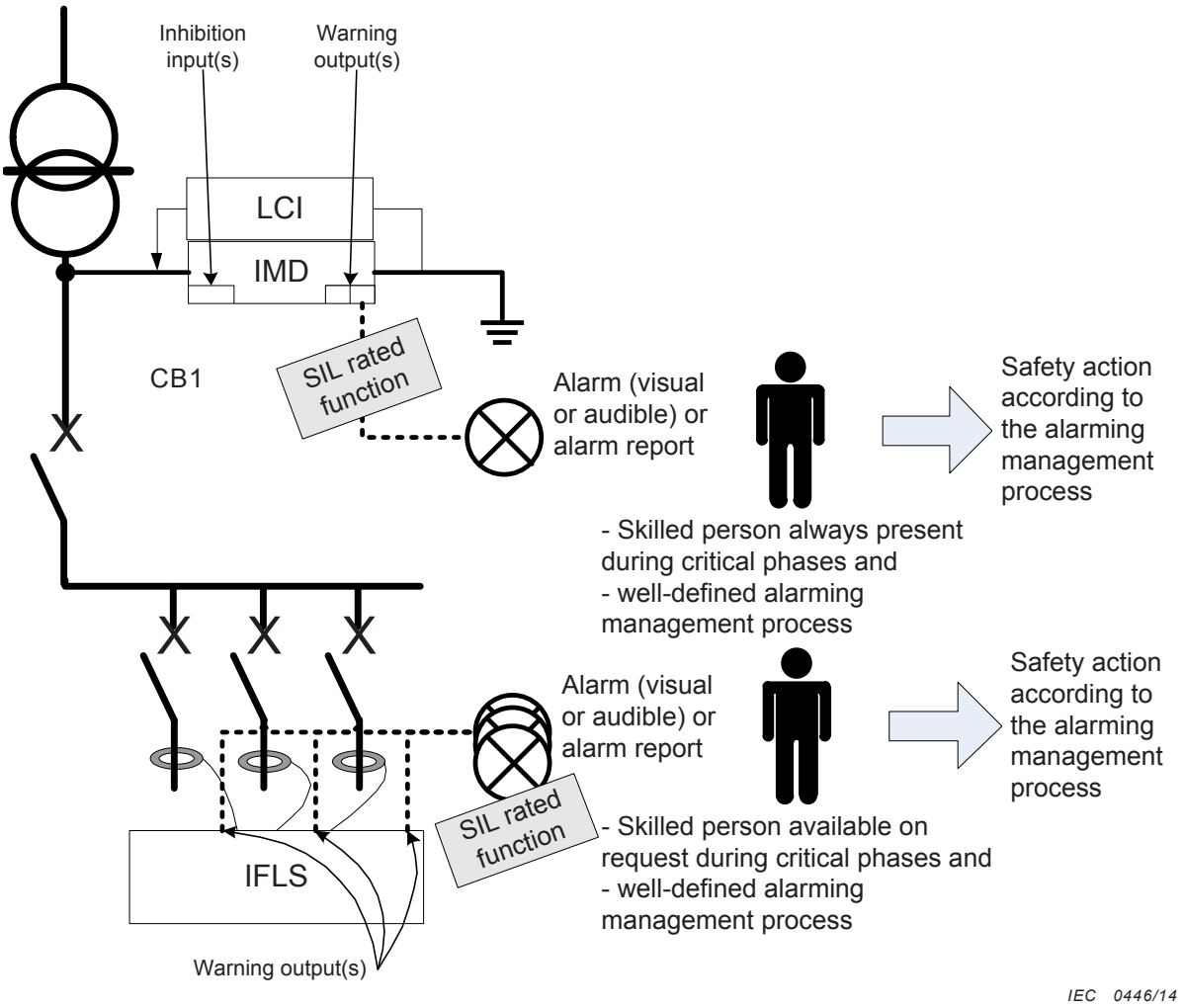


Figure F.1 – Local alarming, based on the systematic presence of one person and based on a well-defined alarming management process

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.

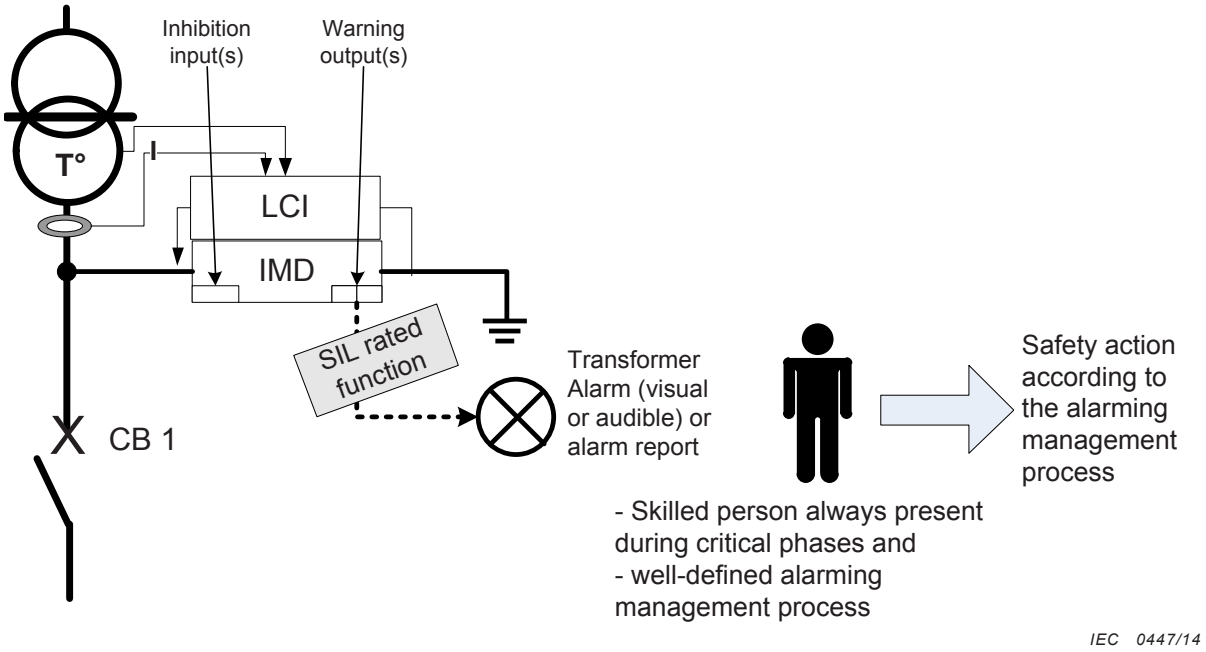


Figure F.2 – Local transformer monitoring warning, based on the systematic presence of a skilled person, and based on a well-defined alarming management process

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.

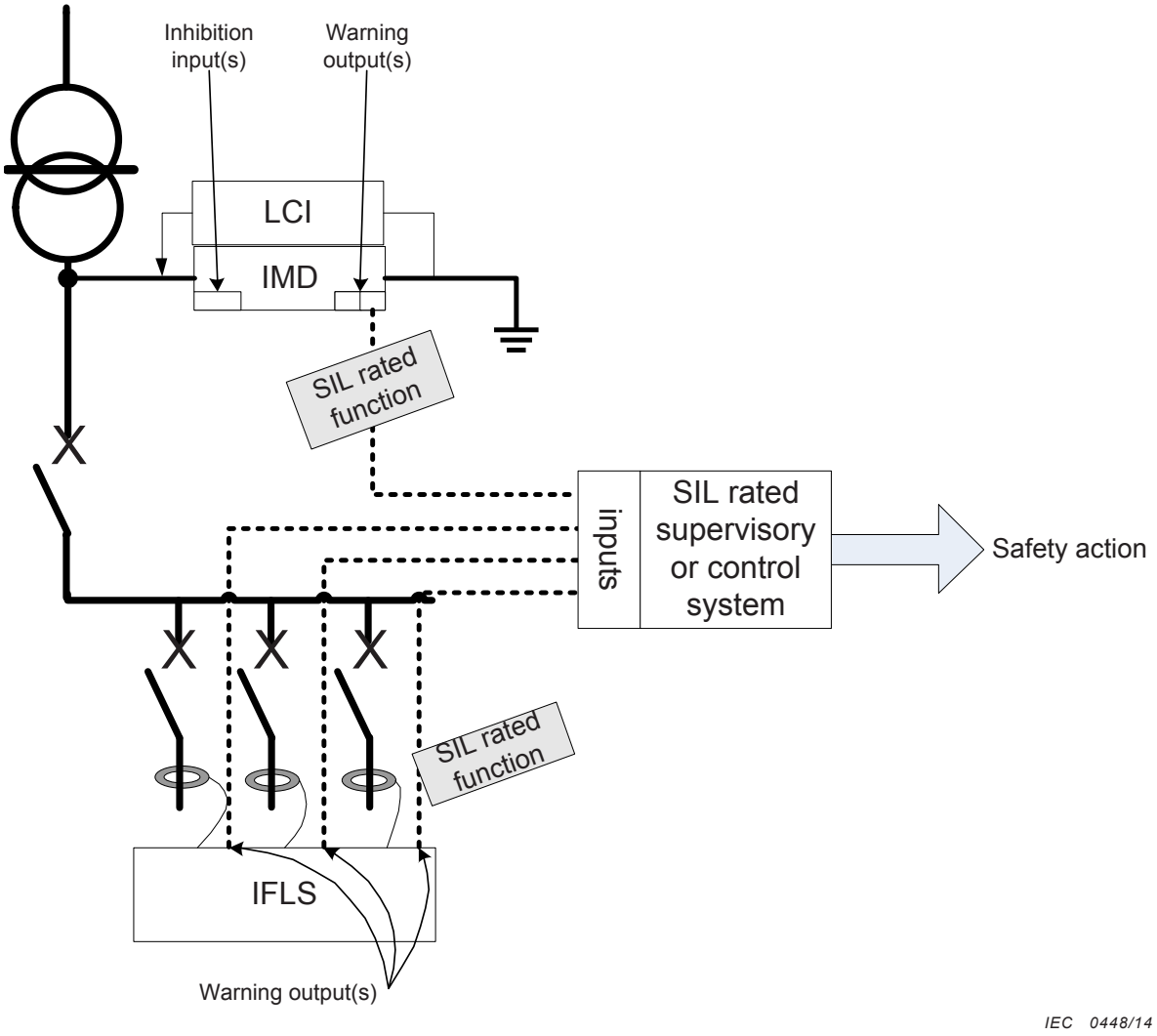


Figure F.3 – Alarming and processing of the remote insulation warning and/or the remote location warning in a supervisory control system

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.

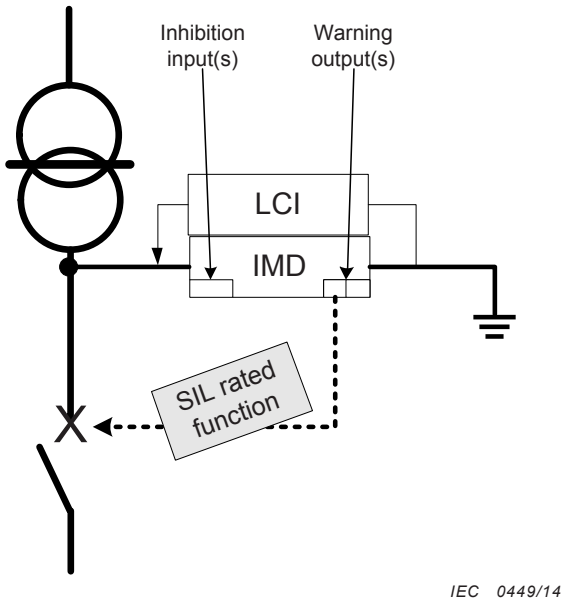


Figure F.4 – Disconnection of the complete IT system in case of insulation fault detection

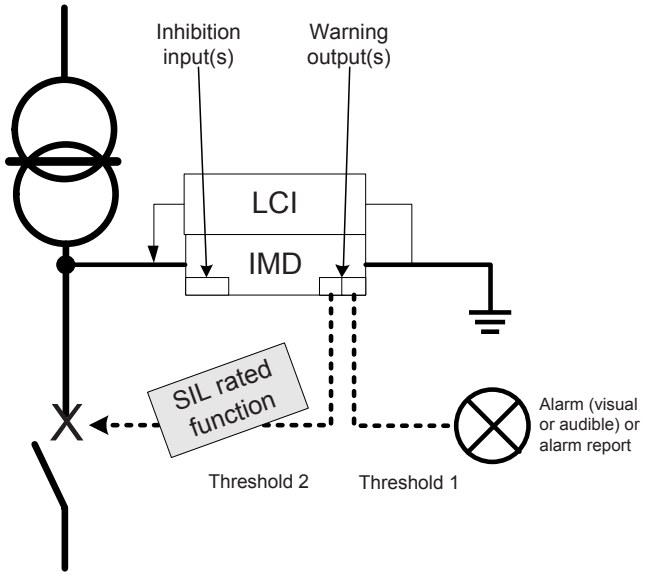


Figure F.5 – Threshold 1 warning information and threshold 2 disconnection of the complete IT system in case of an insulation fault detection

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.

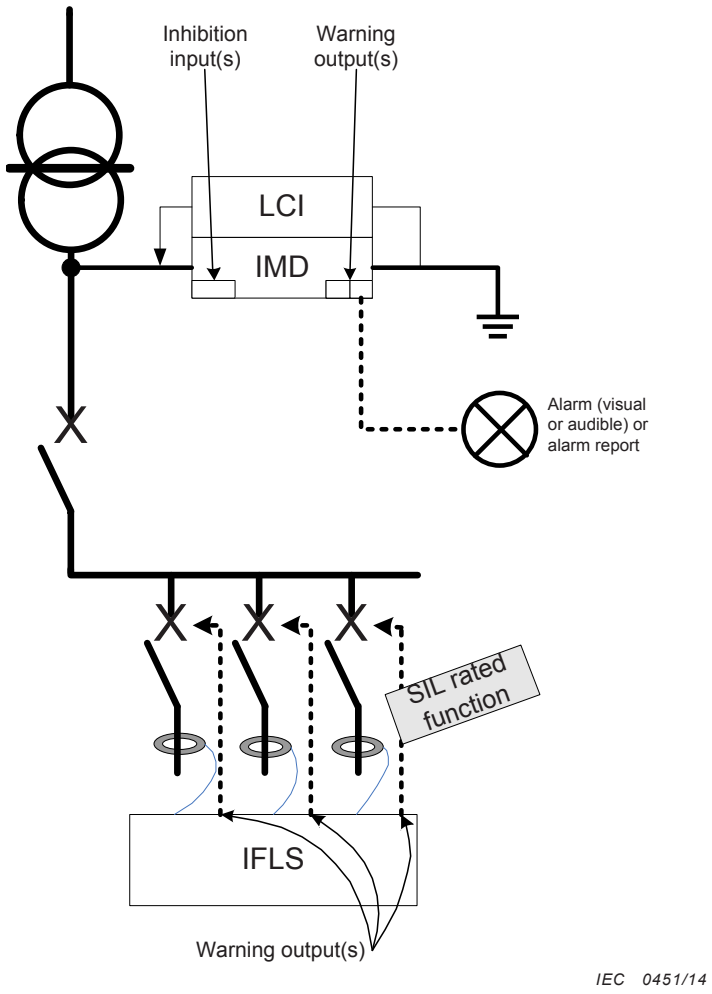


Figure F.6 – Automatic disconnection of a faulty feeder via direct signal from the IFLS

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).

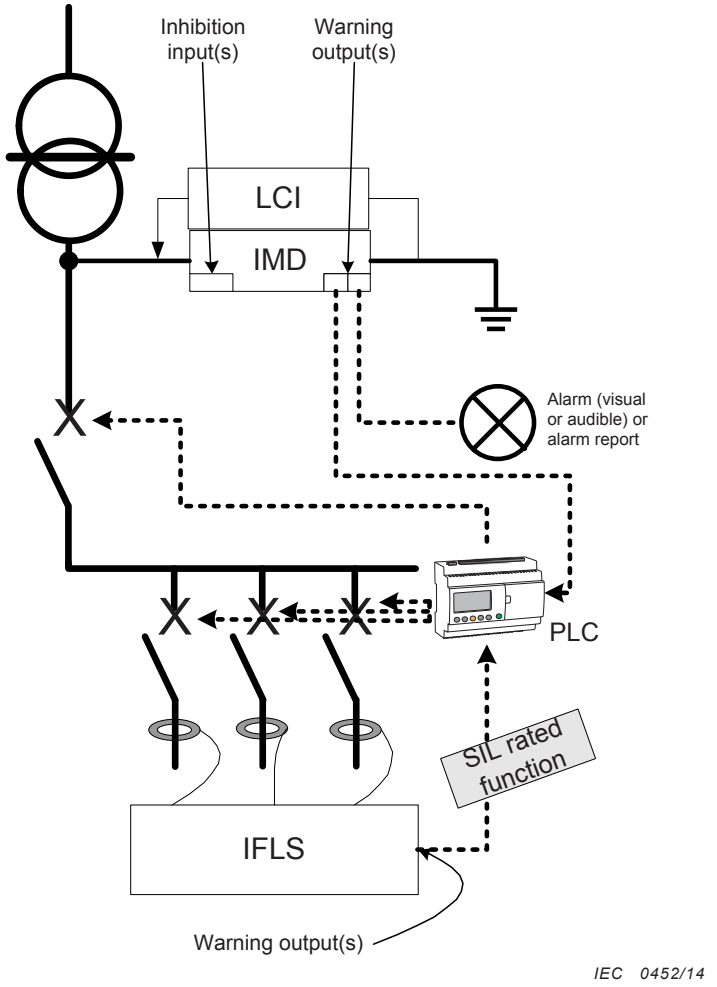


Figure F.7 – Automatic disconnection of a faulty feeder via a PLC

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.

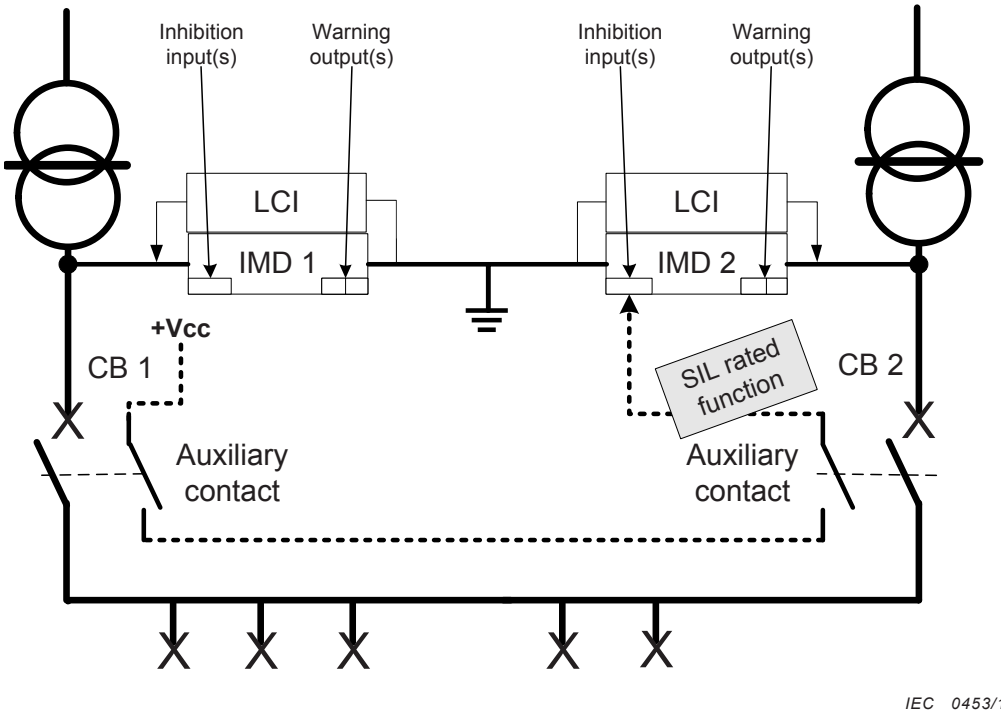


Figure F.8 – Management of multiple source systems (two incomers or of one incomer plus generator)

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.

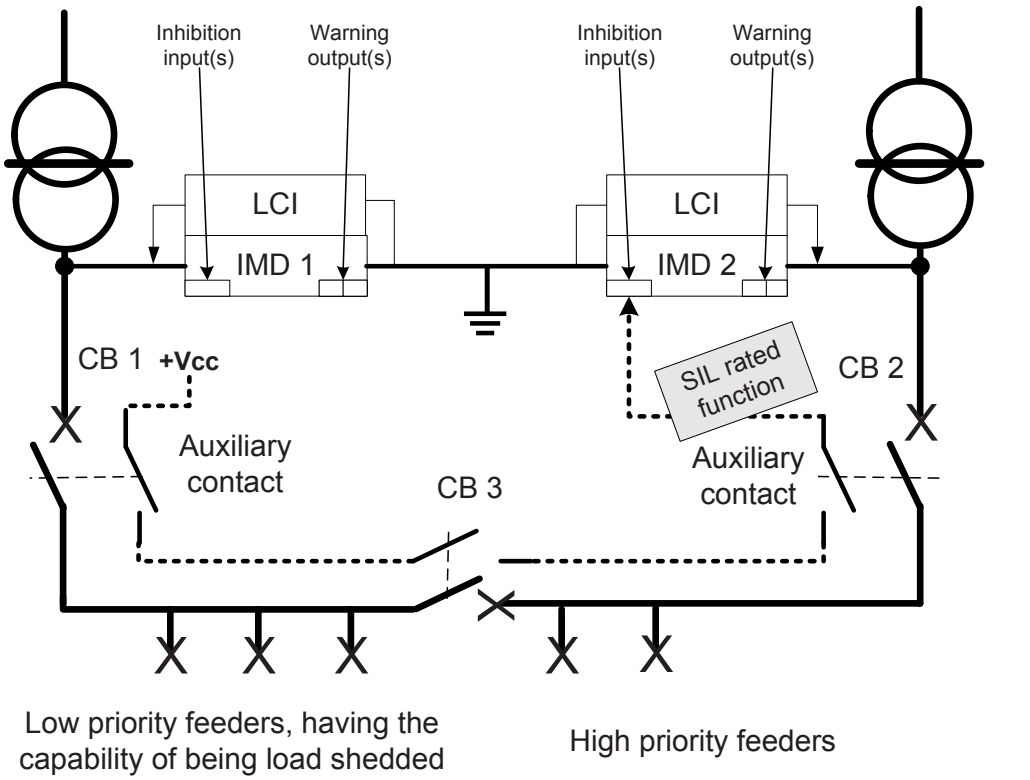


Figure F.9 – Management of multiple source system (two incomers or of one incomer plus generator, with a load shedder)

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*

———————

This page deliberately left blank

British Standards Institution (BSI)

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

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

About us

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

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

Information on standards

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

Buying standards

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

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

Subscriptions

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

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

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

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

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

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

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

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

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

Copyright

Useful Contacts:

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

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

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

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

bsi.

...making excellence a habit.™