PROFIsafe Environment

related to PROFIsafe V2.6.1

Guideline for PROFINET and PROFIBUS

Version 2.6 – Date: December 2015
Order No.: 2.232

File name: PROFIsafe-Environment_2232_V26_Dec15

PROFIsafe Environment

Related to PROFIsafe V2.6.1

This version 2.6 of the PROFIsafe Environment guideline has been prepared by the Profile Group 2 "PROFIsafe" within the profiles committee C3. It covers all change requests within the project database up to CR 156.

The attention of adopters is directed to the possibility that compliance with or adoption of PI (PROFIBUS&PROFINET International) specifications may require use of an invention covered by patent rights. PI shall not be responsible for identifying patents for which a license may be required by any PI specification, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. PI specifications are prospective and advisory only. Prospective users are responsible for protecting themselves against liability for infringement of patents.

NOTICE:

The information contained in this document is subject to change without notice. The material in this document details a PI specification in accordance with the license and notices set forth on this page. This document does not represent a commitment to implement any portion of this specification in any company's products.

WHILE THE INFORMATION IN THIS PUBLICATION IS BELIEVED TO BE ACCURATE, PI MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, IMPLIED WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR PARTICULAR PURPOSE OR USE.

In no event shall PI be liable for errors contained herein or for indirect, incidental, special, consequential, reliance or cover damages, including loss of profits, revenue, data or use, incurred by any user or any third party. Compliance with this specification does not absolve manufacturers of PROFIBUS or PROFINET equipment, from the requirements of safety and regulatory agencies (TÜV, BIA, UL, CSA, etc.).

PROFIBUS® and PROFINET® logos are registered trademarks. The use is restricted for members of PROFIBUS&PROFINET International. More detailed terms for the use can be found on the web page www.profibus.com/Downloads. Please select button "Presentations & logos".

In this specification the following key words (in **bold** text) will be used:

may:	indicates flexibility of choice with no implied preference.
should:	indicates flexibility of choice with a strongly preferred implementation.
shall:	indicates a mandatory requirement. Designers **shall** implement such mandatory requirements to ensure interoperability and to claim conformance with this specification.

Publisher:
PROFIBUS Nutzerorganisation e.V.
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany
Phone : +49 721 / 96 58 590
Fax: +49 721 / 96 58 589
E-mail: info@profibus.com
Web site: www.profibus.com

CONTENTS

1 Introduction

1.1 General

PROFIBUS had already been successful for many years and the reliability of microcontrollers and software development processes had been proven a million fold, when the vision of PROFIsafe was raised: communication of process data in a functional safe manner and the peaceful coexistence of safety and non-safety communication as shown in Figure 1.

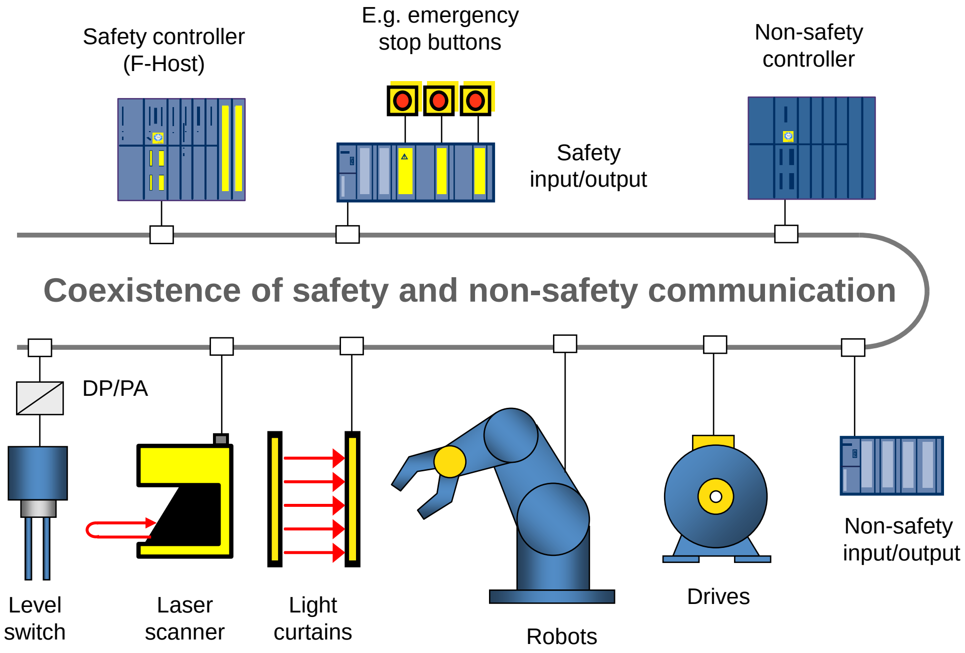


Figure 1 – PROFIsafe's vision

Ever since, a corresponding specification [1] defines so-called safety communication layers which are implemented according to IEC 61508 series usually as software parts of safety-related devices (called F-Devices/F-Slaves) or of safety-related controllers (called F-Hosts). These safety communication layers provide the necessary confidence in the transportation of messages (information) between two participants on a network in a safety-related system, or sufficient confidence of safe behaviour in the event of network errors or failures.

The PROFIsafe technology can be used mainly with PROFIBUS and PROFINET as well as with undisclosed transmission means such as backplane buses as defined in [2]. The technology is standardized in IEC 61784-3-3, which is a companion standard to the communication profile family 3 (CPF3) in IEC 61158, IEC 61784-1, and IEC 61784-2.

PROFIsafe communication layers provide functional safe transmission of messages between two safety-related devices (for example sensor to controller and controller to actuator) and thus can complement safety functions requiring functional safety up to the Safety Integrity Level 3 (SIL3) or Performance Level e (PLe).

The resulting SIL of a safety function in an automation system depends on the implementation of the PROFIsafe communication layers within the F-Host and the F-Devices/F-Slaves – implementation of a PROFIsafe communication layer in a non-safety (standard) device is not sufficient to qualify it as a safety device (see [2]).

In order to guarantee correct implementation of PROFIsafe and interoperability of F-Devices/F-Slaves with F-Hosts, PI provides a PROFIsafe test & certification specification [3], as well as a number of PI Test Labs worldwide.

Figure 2 shows the relationships between the PROFIsafe standard IEC 61784-3-3 and relevant safety and fieldbus standards in a machinery environment. A number of standards support the user of PROFIsafe during risk assessment (for example ISO 12100), during their development efforts (for example IEC 61508, IEC 62061, ISO 13849-1/2, IEC 61000-6-7), and during the deployment phase (for example IEC 62061, ISO 13849-1/2, IEC 60204-1, IEC 61000-1-2, IEC 61918, IEC 61784-5-3, IEC 62443).

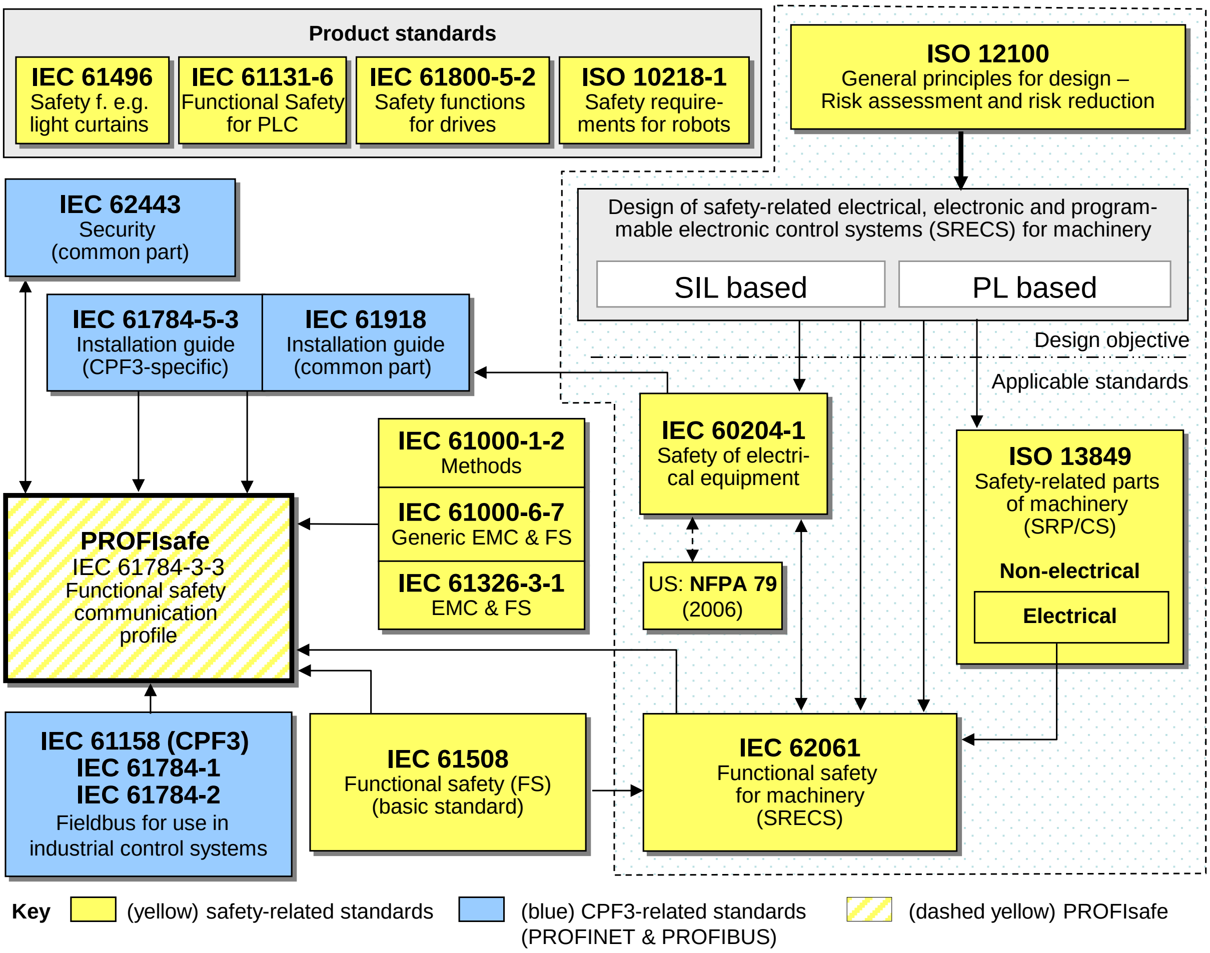

Product standards
IEC 61496
Safety f. e.g. light curtains
IEC 61131-6
Functional Safety for PLC
IEC 61800-5-2
Safety functions for drives
ISO 10218-1
Safety requirements for robots
ISO 12100
General principles for design – Risk assessment and risk reduction
IEC 62443
Security (common part)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery
SIL based
PL based
Design objective
Applicable standards
IEC 61784-5-3
Installation guide (CPF3-specific)
IEC 61918
Installation guide (common part)
IEC 61000-1-2
Methods
IEC 61000-6-7
Generic EMC & FS
IEC 61326-3-1
EMC & FS
IEC 60204-1
Safety of electrical equipment
US: NFPA 79 (2006)
ISO 13849
Safety-related parts of machinery (SRP/CS)
Non-electrical
Electrical
PROFIsafe
IEC 61784-3-3
Functional safety communication profile
IEC 61158 (CPF3)
IEC 61784-1
IEC 61784-2
Fieldbus for use in industrial control systems
IEC 61508
Functional safety (FS) (basic standard)
IEC 62061
Functional safety for machinery (SRECS)
Key
(yellow) safety-related standards
(blue) CPF3-related standards (PROFINET & PROFIBUS)
(dashed yellow) PROFIsafe

Figure 2 – Relationship of PROFIsafe with other standards (machinery)

Figure 3 shows the relationships between the PROFIsafe standard IEC 61784-3-3 and relevant safety and fieldbus standards in a process automation environment. A number of different standards support the user of PROFIsafe during their development efforts (for example IEC 61511, IEC 61326-3-2), and during the deployment phase (for example IEC 61511).

All these standards do not always align with the individual requirements of PROFIsafe and thus leave open issues such as:

- Is it possible to use the 24 V power supplies that are used for non-safety equipment for safety equipment also?
- Shall F-Devices/F-Slaves be able to withstand a significant overvoltage, for example a million volt, on the PROFIBUS or PROFINET cables?
- Which network configuration (cable length, number of devices) is required for tests?
- Is there a difference in testing of non-safety and safety modules of a remote I/O?
- Is there a difference in testing of PROFIsafe devices with SIL CL2 and SIL CL3?
- Is Power-over-Ethernet allowed for PROFIsafe devices?
- Which EMC standard to use for robots and drives, where there is no product standard?
- Which PI installation guidelines or IEC installation standards to use?
- Which PI security guidelines or IEC security standards to use?

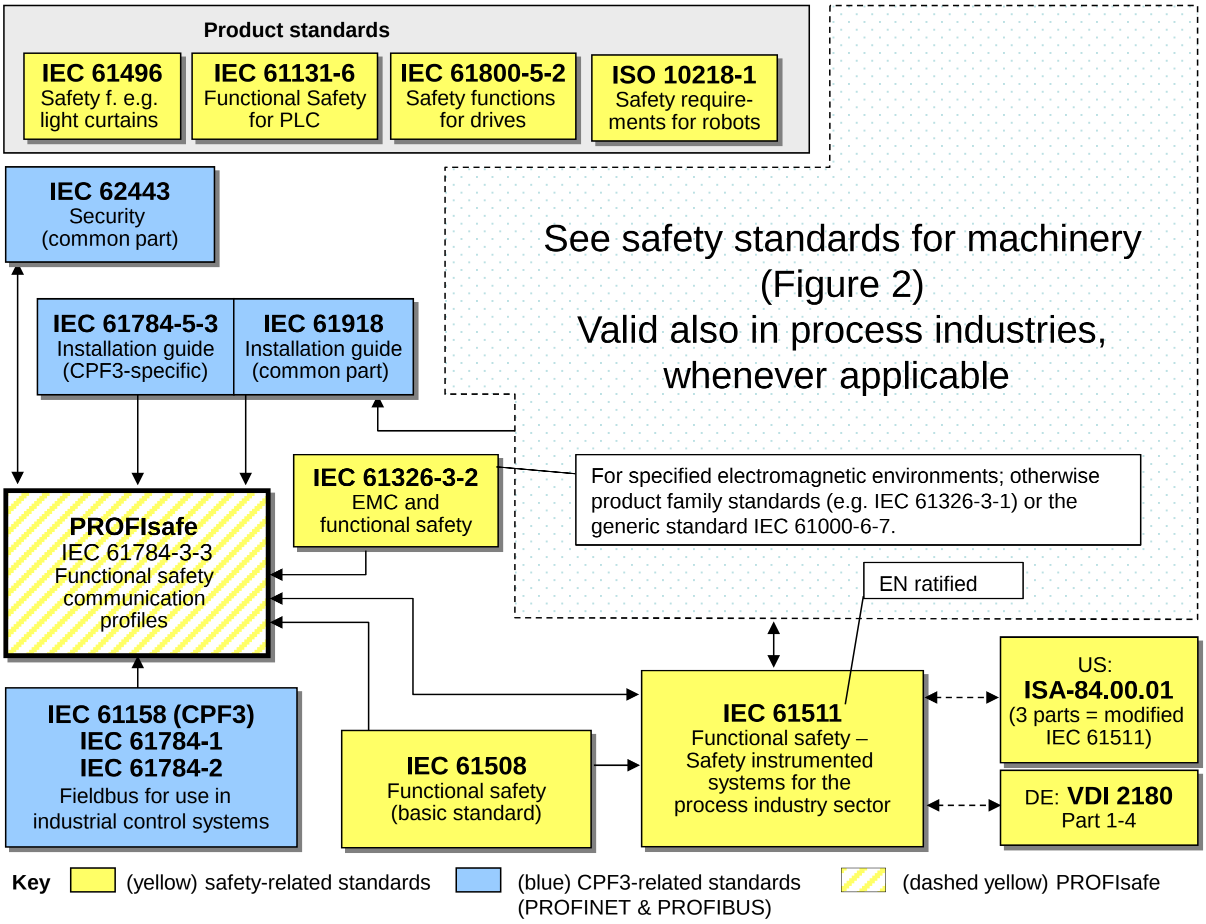

Product standards
IEC 61496 Safety f. e.g. light curtains
IEC 61131-6 Functional Safety for PLC
IEC 61800-5-2 Safety functions for drives
ISO 10218-1 Safety require-ments for robots
IEC 62443 Security (common part)
IEC 61784-5-3 Installation guide (CPF3-specific)
IEC 61918 Installation guide (common part)
See safety standards for machinery (Figure 2)
Valid also in process industries, whenever applicable
IEC 61326-3-2 EMC and functional safety
For specified electromagnetic environments; otherwise product family standards (e.g. IEC 61326-3-1) or the generic standard IEC 61000-6-7.
PROFIsafe IEC 61784-3-3 Functional safety communication profiles
EN ratified
IEC 61511 Functional safety – Safety instrumented systems for the process industry sector
US: ISA-84.00.01 (3 parts = modified IEC 61511)
DE: VDI 2180 Part 1-4
IEC 61158 (CPF3) IEC 61784-1 IEC 61784-2 Fieldbus for use in industrial control systems
IEC 61508 Functional safety (basic standard)
Key
(yellow) safety-related standards
(blue) CPF3-related standards (PROFINET & PROFIBUS)
(dashed yellow) PROFIsafe

Figure 3 – Relationship of PROFIsafe with other standards (process)

This document "PROFIsafe environment" provides answers to these and other questions within two major sections:

- for the individual PROFIsafe devices, and
- for the deployment of safety automation systems.

Many of the PROFIsafe-related automation systems worldwide are unique applications with individual topology layouts, automation software, particular requirements, and challenges.

Like with all other fieldbuses, the power and complexity of the PROFINET, PROFIBUS, PROFIsafe, and related technologies require an associated support organization (see Annex C).

1.2 Patent declaration

There are no known patents for the subjects of this document.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. PNO shall not be held responsible for identifying any or all of such patent rights.

2 Management summary - Scope of this document

IEC 61508 requires for each and every automation system with safety functions a *safety requirements specification* (SRS) defining the immunity of the safety functions against stress caused by the particular application and its environmental conditions. These stress factors include, but are not limited to, climatic changes, mechanical impacts, electrical shocks, electromagnetic interference, and cyber-attacks.

A number of international standards are available defining typical industrial automation environments and appropriate stress tests (see Figure 3) to simulate these situations. This enables companies to reduce the development efforts down to an economically reasonable value and to develop standardized non-safety products in large volumes. A similar approach has been established for safety-related products with modified stress tests.

This document provides an overview of the corresponding available standards and PI specifications and guidelines as well as PROFIsafe-specific information for *developers* of PROFIsafe devices.

Users of these PROFIsafe devices are interested in information on how to deploy safety functions in automation systems, i.e. on how to plan, mount, and commission the entire equipment.

This document also provides an overview of installation and security guidelines as well as special information on how to avoid pitfalls, particularly in the field of EMC. It also reports about PI activities to gain feedback from the field via a working group of "trouble-shooters" in order to establish continuous improvement.

3 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

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

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

IEC 61000-2-5, *Electromagnetic compatibility (EMC) – Part 2-5: Environment – Description and classification of electromagnetic environments*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

IEC 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61010-2-201:2013, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 2-201: Particular requirements for control equipment*

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

IEC 61326-1:2012, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 1: General requirements*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC 479 requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety -related functions (functional safety) – General industrial applications*

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

IEC 61508 (parts 1 to 4), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

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

IEC 61784-3-3, *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3*

IEC 61784-5-3:2013, *Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3*

IEC 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

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

ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

4 Terms definitions, symbols, and abbreviated terms

4.1 Common terms and definitions

For the purposes of this document, the terms and definitions of IEC 61784-3 and IEC 61784-3-3 apply, as well as the terms and definitions of IEC 61000-6-7 (EMC) and IEC 61010-2 (electrical safety).

4.2 Additional terms and definitions

4.2.1
defined state
DS
Performance criterion for immunity tests of safety-related devices with electro-magnetic interferences at higher levels and/or longer durations

[SOURCE: IEC 61000-6-7]

4.2.2
earth
conducting mass of the Earth, whose electric potential at any point is conventionally taken as zero

[SOURCE: IEV 195-01-01]

4.2.3
electromagnetic compatibility
EMC
ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment

[SOURCE: IEV 161-01-07]

4.2.4

equipment under test

EUT

representative configuration(s), as defined by the manufacturer, used for type tests

[SOURCE: IEC 61131-2]

4.2.5

extra-low voltage

ELV

voltage on the output terminals and against ground of a system not exceeding 30 V AC, 42,2 V peak, or 60 V DC under normal conditions, and not exceeding 50 V AC, 70 V peak, or 120 V DC in case of a single fault

4.2.6

functional earthing conductor

conductor that is in electrical contact with, for example, Earth, for purposes of interference immunity improvement

[SOURCE: IEC 61131-2]

4.2.7

functional safety

FS

part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities

[SOURCE: IEC 61508-4, 3.1.9]

4.2.8

immunity (to a disturbance)

ability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance

Note 1 to entry: Not used exclusively to refer to EMC in this standard. It may also refer, for example, to vibration, humidity, etc.

[SOURCE: IEV 161-01-20]

4.2.9

nuisance trip

spurious trip with no harmful effect

Note 1 to entry: Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

[SOURCE: IEC 61784-3]

4.2.10

operator

trained person who is aware of the general hazards in an industrial environment and who is commanding and monitoring a machine or process through an HMI connected to one or more PLCs that shall not be changed in hardware, software or the application programme by this operator.

[SOURCE: IEC 61131-2, modified]

4.2.11

performance criterion

permitted defined reactions of equipment under test (EUT) during and after immunity testing

4.2.12

performance level

PL

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1]

4.2.13
protective extra-low voltage
PELV
electric system in which the voltage cannot exceed the value of *extra-low voltage* under normal conditions, and under single-fault conditions, except earth faults in other circuits

NOTE 1 to entry: protective extra-low voltage is a grounded variant of safety extra-low voltage

[SOURCE: IEV 826-12-32, modified]

4.2.14
safety extra-low voltage
SELV
electric system in which the voltage cannot exceed the value of *extra-low voltage* under normal conditions, and under single-fault conditions, including earth faults in other circuits

Note 1 to entry: a safety extra-low voltage system shall not be grounded

[SOURCE: IEV 826-12-31, modified]

4.2.15
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010.

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL*n* safety-related system" (where *n* is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to *n*.

[SOURCE: IEC 61508-4:2010]

4.2.16
type test
conformity test made on one or more items representative of the production

[SOURCE: IEV 151-16-16]

4.3 Abbreviations

AC	alternating current	
AOPD	active opto-electronic protection device	
DC	Direct Current	
DS	Defined State	[IEC 61000-6-7]
EC	European Community	
EMC	Electromagnetic Compatibility	
EN, prEN	European Norm, preliminary European Norm	
ESD	Electrostatic Discharge	
ERS	Equipment requirement specification	[IEC 61000-1-2]
ESPE	Electro sensitive Protection Equipment	
EUT	Equipment under Test	
FS	Functional Safety	
HSE	Health and Safety Executive (United Kingdom)	
IACS	Industrial Automation Control System	[IEC 62443]
IEC	International Electrotechnical Commission	

IFA	German Institute for Occupational Safety and Health ("Institut für Arbeitsschutz")	
I/O	Input / Output	
ISO	International Standards Organization	
MBP-IS	Manchester Bus Powered – Intrinsically Safe	
PELV	Protective extra-low voltage	
PI	PROFIBUS and PROFINET International (interest group)	
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
PNO	PROFIBUS Nutzerorganisation e.V. (PI support organization)	
PoE	Power over Ethernet	
RS485-IS	RS485 – Intrinsically Safety	
SELV	Safety extra-low voltage	
SIL	Safety Integrity Level	[IEC 61508]
SRS	Safety requirement specification	
SUVA	Schweizerische Unfallversicherungsanstalt	
TÜV	Technischer Überwachungsverein (Organization for global certification)	
UL	Underwriters Laboratories Inc. (Product Safety Testing and Certification Organization)	
VPN	Virtual Private Network	
WAN	Wide Area Network	

5 Motivation and objectives

5.1 General

PROFIsafe is designed to be functional safe. Any communication fault – be it caused by failure or by error – will lead to a defined safety reaction.

PI provides a test and certification specification [3] to guarantee implementation of a correct PROFIsafe protocol in F-Hosts/F-Devices/F-Slaves and their interoperability (e.g. GSD check). It also requires a report and certificate of a safety assessment body such as IFA, TÜV, SUVA, and HSE.

This is reassuring to know. However, if PROFIsafe is embedded in non-safety automation equipment with low reliability or low availability, communication may be disturbed and PROFIsafe will realize for example CRC errors or timeouts. This results in so-called nuisance trips, i.e. tripping of safety functions without a real safety demand. As a consequence, the user or operator may look for a removal of the safety equipment in order to produce/operate without interrupts. Therefore, PI highly recommends for the entire non-safety automation equipment and system to provide enough availability in such a way that PROFIsafe will not cause *nuisance trips*.

Usually, only electromagnetic interference, network traffic load, wireless drop-outs or cyber-attacks can cause PROFIsafe to trip a safety function without a demand. Thus, mainly these effects are subject of special safety-related considerations within this document.

5.2 Holistic view of safety functions

IEC 61508 introduced a life cycle model and a holistic view of safety functions. Figure 4 shows some of the impacts, which can affect the properties of safety functions such as electromagnetic interference and power supply changes.

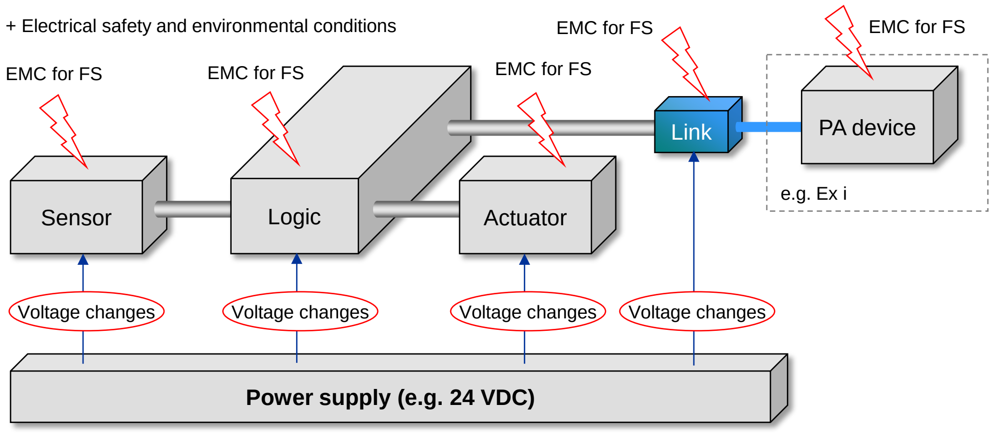


Figure 4 – Holistic view of a safety function

The safety function is implemented by a safety system, which is composed of safety subsystems (for example sensor, logic controller, actuator), connected via PROFIsafe. Safety subsystems can comprise individual safety elements (for example electro mechanic switches).

Many aspects of these components are specified in standards such as IEC, ISO, and EN. Some of them are generic or basic such as IEC 61508, which is valid for all products (TYPE A). Others are valid for an automation sector or a group (TYPE B) such as ISO 13849 (safety-for-machinery) and others are valid for particular products or product families (TYPE C).

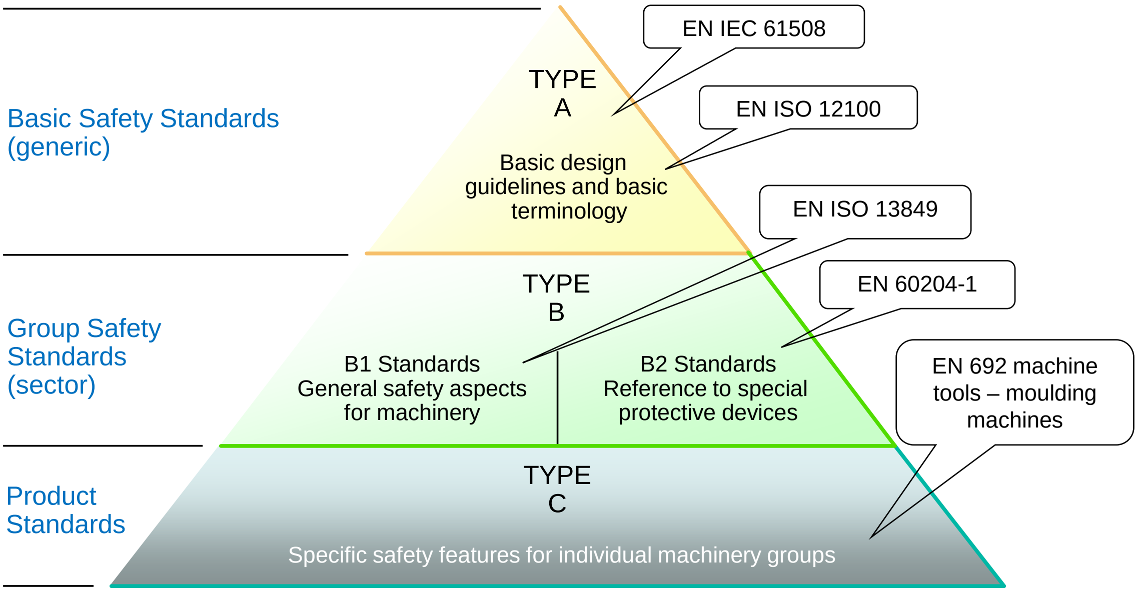

Basic Safety Standards (generic)
Group Safety Standards (sector)
Product Standards
TYPE A
Basic design guidelines and basic terminology
TYPE B
B1 Standards General safety aspects for machinery
B2 Standards Reference to special protective devices
TYPE C
Specific safety features for individual machinery groups
EN IEC 61508
EN ISO 12100
EN ISO 13849
EN 60204-1
EN 692 machine tools – moulding machines

Figure 5 – The EN standards hierarchy

Figure 5 shows as example the EN standards hierarchy. A rule exists, that more specific standards overrule more general ones. In case of functional safety this does not mean less stringent requirements. Quite contrary, product standards sometimes require higher levels and longer durations than the more general standards.

This is not a comfortable situation for a user of PROFIsafe within a certain automation system where one particular set of environmental conditions is given. It can be very time-consuming to find out which standards are relevant for a project. In the past, PI had been and now still is striving in several standards working groups to harmonize standards and facilitate their usage.

It is the purpose of this document to provide guidance on how to ensure the necessary immunity of safety devices and safety applications for typical environments of decentralized industrial automation structures. These structures can be classified into two main sections: factory automation and process automation. The section factory automation is defined by the scope of IEC 61000-6-2 and the section process automation by the scope of IEC 61326-1.

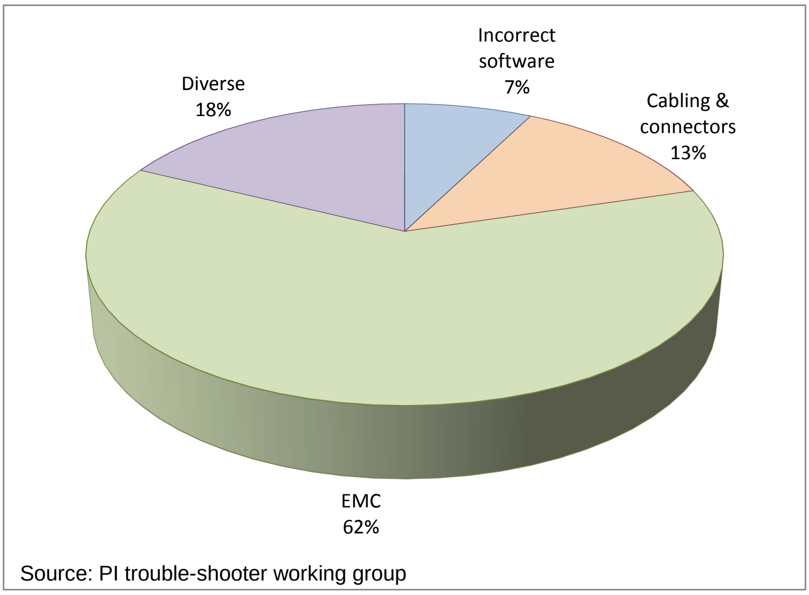
Another characteristic of decentralized industrial automation is the huge variety of configurations and the extent of machines and plants in comparison to automotive, train, or airplane electronics. Products of many different vendors are involved and the machine builders depend on the immunity of these products as they are usually not able to perform the corresponding tests. Products include but are not limited to safety controllers, safety field devices, active and passive fieldbus network components, cables, connectors, and power supplies.

5.3 Motivation

Due to this variety in products and configurations, it can be observed, that despite many international standards and individual PI specifications and guidelines, the safety applications in the field are sometimes still facing some start-up problems.

Figure 6 shows the share of problems of 72 emergency services of trouble-shooters in the years 2009 to 2011 with 226 problems in total. The problems were grouped into "incorrect software" (7 % of 226), "cabling and connectors" (13 %), "electromagnetic interferences/EMC" (62 %), and "diverse" (18 %).

Therefore, it is one of the goals of this document to provide not only information about available standards, but background information and overviews as well as feedback from the field of safety applications.



Source: PI trouble-shooter working group

Figure 6 – Typical shares of problems in trouble-shooting reports

5.4 Objectives

It is the purpose of this document to collect agreed upon guidance and constraints for the design of PROFIsafe devices and for PROFIsafe-related automation applications within normal industrial environment as defined e.g. in IEC 61000-6-2.

It is the declared objective of PI to integrate safety technology into PROFINET and PROFIBUS; that means to communicate on one cable without having an impact on the installed base of devices and systems (see Figure 1). In addition, *no separate power supply* shall be required for the safety devices.

The *electrical safety* is a precondition for a PROFINET/PROFIBUS system. Thus, for functional safety, a defined situation for using functional safe devices can only be achieved through corresponding

- compliance to the installation guidelines (cables, cable installation, shields, shield connections, grounding, power supply, etc.) including constraints for PROFIsafe operations (see [1]),

- defined requirements for the non-safety-related bus devices (conformance to IEC 61158/CPF3 through PI certification),
- defined safety requirements for the power supplies (SELV, PELV).

The overall steps required for such a network may differ regarding the different safety integrity levels (SIL). Wherever it is economically possible, the adherence to the capability for SIL3 is the aim. The steps taken must be compliant and/or conform to the existing standards. There are still cases where the standards do not yet cover the state-of-the-art, especially with respect to fieldbus operations. Here, ways and means are to be found that are based on basic standards such as IEC 61508 and proven principles and that ensure the required safety integrity or performance (IEC 61508, IEC 62061, and/or ISO 13849). These ways and means shall retain their validity for a suitable transitional period even if new standards are published in the meantime.

In the following, common objectives for the design of F-Hosts, F-Devices, and F-Slaves as well as for decentralized safety applications are defined.

Figure 7 shows the typical mix of safety functions with different safety integrity levels, for example SIL2 and SIL3. Standards specifying the stress tests for functional safety should not differentiate between safety integrity levels. Test levels and durations should be the same as much as possible. Thus, the safety devices of safety function 1 with SIL2 can be tested in the same manner as the safety devices of safety function 2 with SIL3.

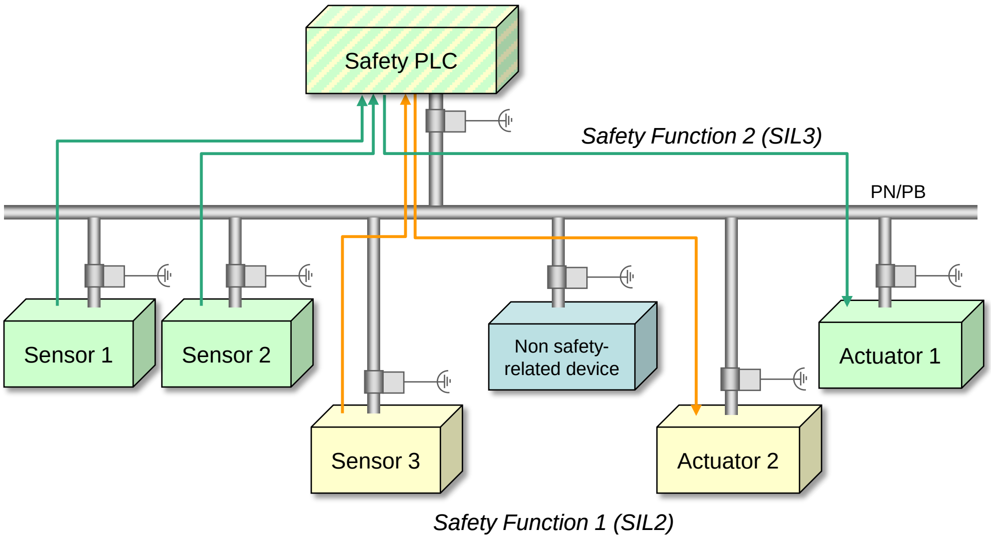


Figure 7 – Mixed safety functions within a fieldbus network

Another objective is demonstrated in Figure 8 where a variable remote I/O device is configured with non-safety-related I/O modules and safety-related (PROFIsafe) modules.

The same stress tests should be required for both the non-safety-related I/O modules and safety-related (PROFIsafe) modules, except EMC.

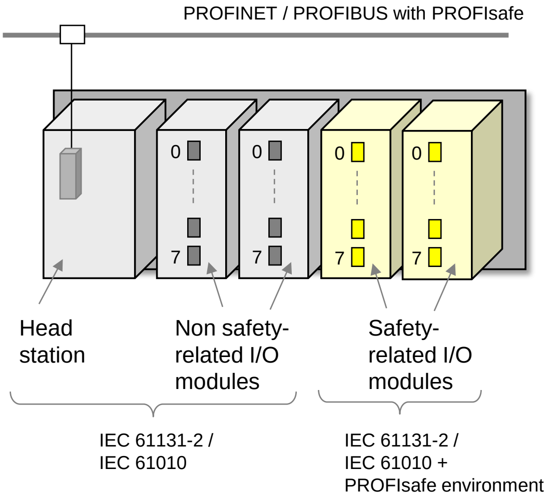

PROFINET / PROFIBUS with PROFIsafe
0
7
Head station
Non safety-related I/O modules
Safety-related I/O modules
IEC 61131-2 / IEC 61010
IEC 61131-2 / IEC 61010 + PROFIsafe environment

Figure 8 – Example of a mixed module remote I/O

No combined stress tests such as for example climatic and EMC tests at the same time should be required, unless explicitly required by a safety requirements specification (SRS).

However, it can be very important to test certain combinations of products, for example F-Devices/F-Slaves and different connectors (weight, layout) and cables from the market during mechanical stress tests.

In order to ensure correct operation of decentralized industrial automation systems PI also takes care of well-defined installation instructions, the specification of permitted cables and cable parameters as well as connectors, and the requirements for power supplies that can energize non-safety-related and safety-related devices.

This document provides guidance for developers of F-Devices and F-Slaves as well as for users/operators of PROFIsafe-related decentralized automation applications.

6 F-Device/F-Slave development

6.1 Overview

This document applies to general industrial environments such as defined in IEC 61131-2 or IEC 61000-6-2 and process automation environments such as those covered in the IEC 61326 series. Table 1 provides an overview of all the issues for the design of F-Devices/F-Slaves.

Table 1 – Overview of the issues for F-Devices/F-Slaves

Issue	Factory automation (machinery, industrial environments such as defined in IEC 61000-6-2)	Process automation (specified electromagnetic environment)	Remarks
User manual	See Clause 6.2	See Clause 6.2	
Markings and identification	See Clause 6.3	See Clause 6.3	
Test bed and operations	See Clause 6.4	See Clause 6.4 Extensions of the test bed for intrinsically safe fieldbus physics	Concepts include but are not limited to barriers, FISCO (Fieldbus Intrinsically Safe Concept), etc.
General test conditions	See Clause 6.5	See Clause 6.5 Depending on the deployment area: See classification in the IEC 60721-3 series	

Issue	Factory automation (machinery, industrial environments such as defined in IEC 61000-6-2)	Process automation (specified electromagnetic environment)	Remarks
Mechanical stress tests	See Clause 6.6, IEC 61131-2	See Clause 6.6, classifications in IEC 60721-3-1	
Electrical safety	See Clause 6.7	See Clause 6.7	
Ingress protection (IP)	See 6.7.2	See 6.7.2, type "field device" shall be ≥ IP65, other types ≥ IP20	
Insulation rating	See 6.7.3	See NOTE	
Electrical shock	See 6.7.4	See 6.7.4	
Clearance and creepage distances	See 6.7.5	See NOTE	
Flame-retardancy	See 6.7.6	See NOTE	
Electromagnetic immunity	See Clause 6.8 IEC 61000-6-7 with special requirements in IEC 61496-1	See Clause 6.8 IEC 61326-3-2	See Figure 2 and Figure 3 for selection of the appropriate standard
Easy circumvention	See Clause 6.9	See Clause 6.9	
Field verification	-	See Clause 6.10	SIL2 devices designed to achieve SIL3 via e.g. 1oo2 shall have software designed for SIL3
Product, sector and application specific requirements	See Annex B	See Annex B	
NOTE Usually no requirements; exceptions possible depending on deployment.			

6.2 User manual

The EUT shall come with a user manual that allows for proper installation, configuration, parameterization, programming, commissioning, troubleshooting, maintenance, and decommissioning. It shall consider and cover all of the appropriate issues listed in:

- IEC 61131-2, general information to be provided by the manufacturer;
- IEC 61508-2:2010, Annex D (safety manual for compliant items);
- IEC 61508-3:2010, 7.4.2.12 and Annex D (safety manual for compliant items, additional requirements for software elements);
- IEC 61784-3-3, 9.7 (safety manual or user manual for PROFIsafe F-Devices/F-Slaves).

These documents require, as far as applicable, the following items:

– Name and address of the manufacturer (brand, picture mark)

– Type designation or serial number

– Intended use

– General description of the functional safety communication system

– Instructions on planning, installation, and mounting of the safety communication system including drawings, circuit diagrams, and mounting elements

– Instructions for commissioning and operation of the safety communication system

– Instructions for preventive maintenance

– Statements on residual risks

– Instructions on the usage of non-ionizing radiation

– Nominal operating voltage(s) with indication of voltage type and frequency

- Power/current consumption
- SIL claim according IEC 61508. In case of factory automation additionally PL/Category according to ISO 13849-1
- Statements on parameterization, configuration and programming as far as required
- Advice on how to determine the safety function response times required short circuit and overvoltage protection means, as far as applicable
- Operating temperature range
- Ingress protection class (IPxy); if required, separate statements on the individual components
- Rated insulation voltages and the degree of pollution
- Required wiring and functional description of wiring blocks and connectors
- Required safety instructions
- Instructions on how to act in case of faults
- Drawings, circuit diagrams, descriptions, and illustrations required for operation, maintenance, repair, and for the check of correct functioning of the safety bus system
- Warnings with respect to typically possible missuses of the safety communication system
- Proof tests and proof test interval for the safety device

6.3 Markings and identification

The main safety components shall be marked according to IEC 61131-2 and/or relevant parts of the IEC 61010 series. These markings comprise as far as applicable:

a) Name and address of the manufacturer/vendor
b) Name of safety device
c) Any conformity marking for the country of deployment, e.g. CE or UL
d) Model name or type designation
e) Ordering Code
f) Year built
g) Ex-i approval
h) Nominal operating voltage(s) with indication of voltage type and frequency
i) Power/current consumption
j) Hardware serial number
k) Fuse for operational voltage if required
l) Unambiguous labelling of connectors and terminals
m) Ingress protection class

The indications according g) to l) can be mentioned within the user manual.

6.4 Test bed and operations

As far as feasible, all parts of a PROFIsafe based system shall be tested together. Otherwise, F-Devices/F-Slaves can be tested separately. In this case, reference systems (test beds) or simulators are defined and made available to assessment bodies. Effectiveness of all implemented safety measures as well as conformance to PROFIsafe shall be proved by the test bed software.

The test bed takes into account worst case conditions, for example shortest possible connections of devices. Signals that are required for the safety function can be emulated.

Relevant operational modes are

- cyclic data exchange of safety process values,
- with most critical transmission rates (highest/lowest speed),
- shortest possible cycle times (burden), and
- acyclic data exchange of safety parameterization data (F-Parameters and iParameters).

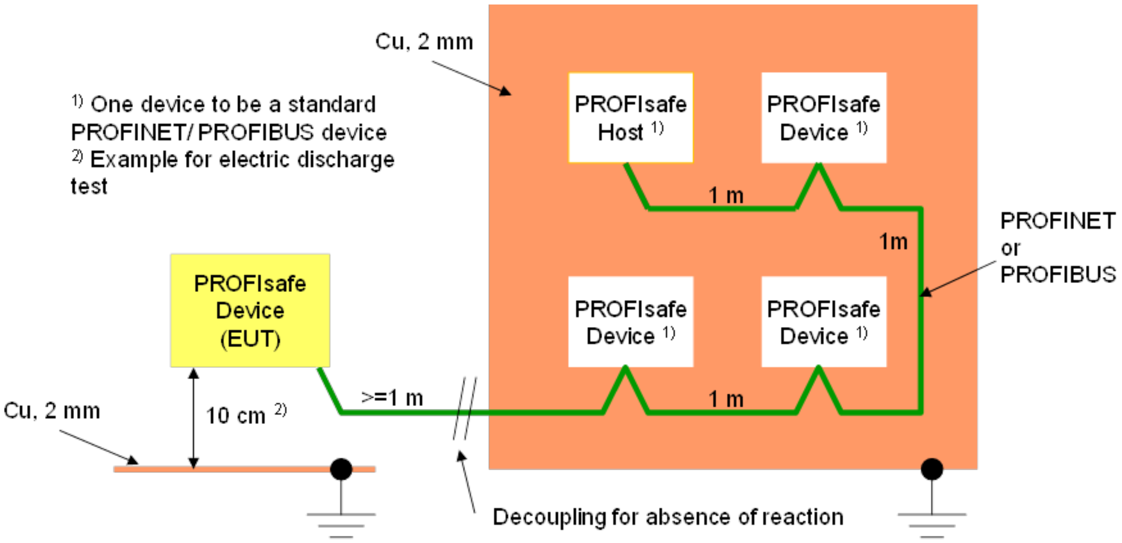


Figure 9 – PROFIsafe test bed for EMC and other testing

Figure 9 shows the PROFIsafe test bed for EMC and other testing. It achieves situations close to worst case topologies and guarantees repeatable and comparable test results as much as possible.

6.5 General test conditions

During the tests, the equipment under test (EUT) shall be operated at the test conditions outlined in the product documentation or at the conditions defined by PROFIsafe related specifications.

The tests shall ensure that the PROFIsafe based system meets the specified technical data.

6.6 Mechanical stress tests

All components of a PROFIsafe based automation system shall have a sufficient mechanical strength or means against the expected stresses, for example vibration, shock, impact, and rigidity according to IEC 61131-2 or corresponding product standard.

For components intended to be mounted on vibrating machinery, extended tests shall be applied according to the individual safety requirement specification or to an applicable product standard (long term stability without compromising functional safety such as any broken wires/connectors or broken electrolytic capacitors). F-Devices/F-Slaves shall be tested using the connectors and cables recommended in the user manual or requested by the customers. Different weights and mechanical layouts of connectors, different elasticity of cables, as well as the type of shields and shield contacts can have influence on the result of the tests.

NOTE An example of such applicable product standards is IEC 61496-1 (electro-sensitive protective equipment).

NOTE Safety devices intended for safety instrumented systems (process automation) are classified according to IEC 60721-3-2 and tested according to the IEC 60068-2 series.

6.7 Electrical safety

6.7.1 Overview of standards

General requirements for the communication ports of every PROFINET/PROFIBUS and PROFIsafe device are laid down in IEC 60364-4-41 (2005). This standard deals with extra-low voltages (SELV/PELV).

General safety information, which may be useful for all kinds of safety products and applications, can be retrieved from 6.7.4.5 and from IEC 60204-1:2009.

For "Programmable Logic Controllers" (F-Host) and fieldbus devices like remote I/O terminals (F-Devices/F-Slaves/F-Modules) the standards IEC 61131-2:2007 and IEC 61010-1:2010 apply.

For "Electro Sensitive Protective Equipment" (ESPE or AOPD such as light curtains) the standard IEC 61496-1:2012 applies.

For electrical power drives the standard IEC 61800-5-1 applies.

6.7.2 Ingress protection (IP)

All components of bus systems for the transmission of safety data shall be designed such that they withstand the normal environmental conditions of the intended use. Ingress protection shall be ≥ IP20 according to IEC 61131-2 or corresponding product standards.

Safety devices intended for safety instrumented systems (process automation) are classified according to the IEC 60721 3 series. The ingress protection for type "field device" shall be ≥ IP65, other types ≥ IP20.

6.7.3 Insulation rating

All components of bus systems for the transmission of safety data shall have insulation ratings according to the equipment classes in IEC 61131-2 or relevant parts of the IEC 61010 series.

6.7.4 Electrical shock (SELV/PELV)

6.7.4.1 High voltage considerations

Functional safety regarding PROFIsafe devices is considered on the assumption that no impermissibly high voltages occur on neither the power supply cables nor the data communication cables or only with a permissibly low probability under normal and single fault conditions.

On the other hand, these cables are hazardous to humans if touched, regardless of whether these are safety devices or not. Therefore, this shock protection approach for humans is applied to safety electronics also: it shall be able to "tolerate" the voltage that a human being is expected to tolerate and then respond safely.

All components of bus systems for the transmission of safety data shall have electrical safety according to the equipment classes in IEC 61131-2 or relevant parts of the IEC 61010 series.

6.7.4.2 SELV/PELV

SELV: Safety Extra-Low Voltage

Being specified as a SELV system includes a limitation of voltage and a protective measure against direct and indirect contact with hazardous voltages through "safe separation" implemented in the device. However, a SELV system must not be grounded (in contrast to a PELV system).

PELV: Protective Extra-Low Voltage ("Function voltage")

Protective extra low voltage is a grounded variant of SELV. Being specified as a PELV system according to IEC 60364-4-41 or IEC 61010-1 includes a limitation of voltage and a protective measure against direct and indirect contact with hazardous voltages through "safe separation" of the primary and secondary side implemented in the device.

The above mentioned isolation testing (hazardous) voltages only refer to the SELV/PELV voltages or data lines respectively.

The following items are permissible as current sources for SELV and PELV

- transformers with safe isolation,
- power sources with the same degree of safety; for example, motor generators with corresponding separated windings or Diesel units,
- electro-chemical power sources; for example, batteries, galvanic elements.

On the same level are electronic devices if, in case of normal conditions, the voltage on the output terminals and against ground is no higher than *30 V AC*, *42,4 V peak* or *60 V DC*; in case of a *single fault* no higher than *50 V AC*, *70 V peak* or *120 V DC*.

The following shall apply for power circuits for safety extra-low voltage (SELV)

- Active parts of safety extra low voltage power circuits shall not be connected to ground or with protective conductors of other power circuits. They shall be separated from active parts with higher voltage. Exposed conductive parts shall not be connected intentionally. Cables shall be installed separated from the cables of other power circuits, or special isolation steps shall be taken. See IEC 61918 and IEC 61784-5-3 for further information.

- Only special plugs, socket outlets and couplers that do not fit the plugs, socket outlets and couplers of higher voltages shall be used for SELV. They shall not have ground contact.

6.7.4.3 Device model including power supplies

Each and every PROFIsafe device (F-Host/F-Device/F-Slave/F-Module) shall be designed and built in a way that despite all possible internal voltages (including high voltages) in the worst case only SELV/PELV voltages reach the data lines and the outside.

Before a standard PROFIBUS/PROFINET or PROFIsafe device is accepted for certification in a PI test laboratory, it shall prove its general capability by a manufacturer declaration of conformity to the appropriate standards (see 6.7.1). In Europe it shall be signed with a CE mark.

PI test and certification is then performed based on the international standards IEC 61158 and IEC 61784-1/-2 (CPF3), which requires the following:

"PROFINET and PROFIBUS devices shall comply with the legal requirements of that country where they are deployed (e.g. within Europe, indicated by the CE mark). The measures for protection against electrical shocks (i.e., electrical safety) within industrial applications shall be based on IEC 61010 or IEC 61131-2 depending on a device type specified therein."

If another network device should apply a SELV or PELV voltage to the data line, the PROFIsafe device can perform its safety response unharmed.

On the other side, the functional safety systems are set up with a 24 V DC power supply (load power supply unit, batteries, etc.) providing also SELV/PELV.

Figure 10 shows the typical structure of F-Devices, where the PROFINET data lines are isolated from the transceiver via transformers. The test voltage is 1,5 kV AC, applied for 1 min according to the IEEE 802.3 rules.

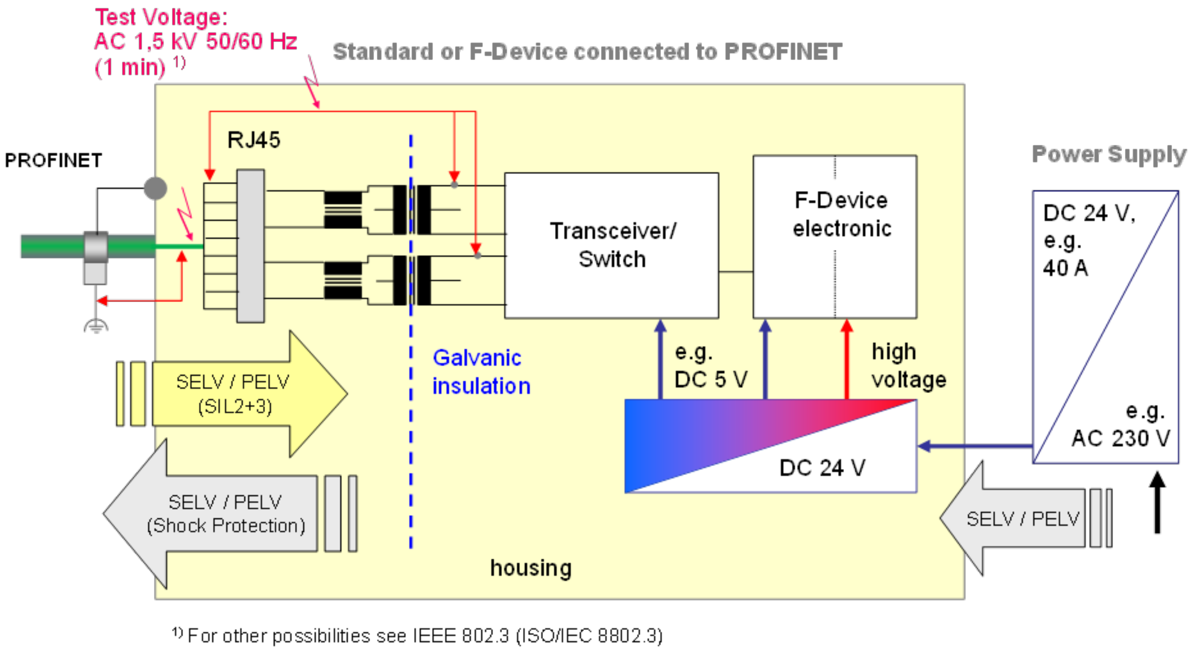


Figure 10 – Typical structure of an F-Device

Figure 11 shows the typical structure of F-Slaves, where the data lines are connected via a "Line driver" to an opto-coupler or a transformer and therefore are galvanically separated from the remaining device electronics. The "Line driver‘s" power supply is also decoupled. The test voltage is 500 V DC, applied for 1 min according to IEC 61158 (CPF3).

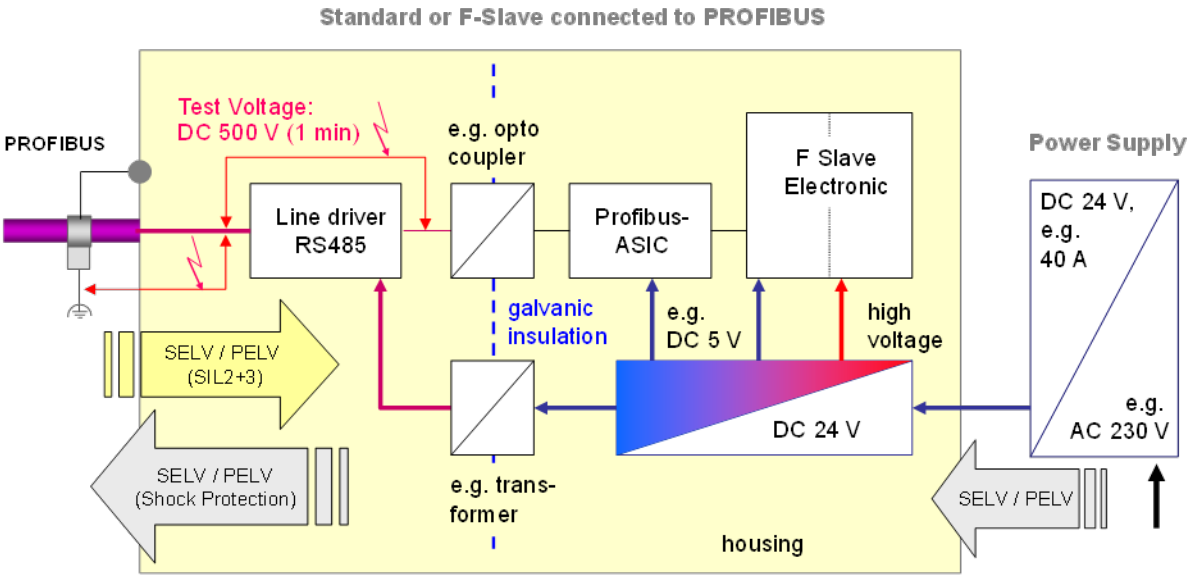


Figure 11 – Typical structure of an F-Slave

6.7.4.4 SIL3/PLe considerations (two faults)

Regarding the safety functions according to SIL3 or PLe, the behavior of the devices shall be considered if *two faults* occur that are weighted with respect to time. This is necessary if the errors are undetected. In the following, the influences of power supplies are discussed as well as the influences of higher voltages as SELV/PELV on data transfer lines.

Power supplies with double fault electrical safety

Since we are aiming for the use of one and the same 24 V power supply for all devices, the request for double fault safety would be a problem since there are no power supplies with this corresponding qualification. From the PROFIsafe perspective, the requirement does not present itself due to the following:

a) The quality and the prevalence of industrial power supplies according to IEC 61010/61131-2 with SELV/PELV are so high that such error cases are not known. The fact that such an error would jeopardize a high investment volume in a standard plant should be sufficient motivation for such high quality.

b) The failure of such a power supply beyond SELV/PELV would already jeopardize human life because when working with power supply cables, the cable ends are not contact-protected.

c) Only PROFIsafe devices with output functions would be affected. They must be able to handle their safety functions autonomously in any case, even if impermissibly high voltages occur. Here, it may be useful to increase the test voltage in 6.7.4.3 to 1500 V DC for final elements such as drives or devices with power supplies exceeding 60 V unless proven otherwise.

d) F-Hosts and PROFIsafe input/output devices shall be toughened up against overvoltages according to IEC 61508-2, table A9, i.e. they shall detect all faults caused by overvoltage and respond in a safe manner. Conformance to the safety regulations can be shown through type testing.

Voltages above SELV/PELV on data lines

Here, it is a question of whether PROFIsafe devices shall be tested for voltages above SELV/PELV levels.

From the PROFIsafe viewpoint, this requirement does not present itself due to the following:

a) If the installation guidelines are adhered to (cable types and cable installation) and certified devices are used, the occurrence of voltages higher than SELV/PELV on data lines because of second faults can be estimated as extremely unlikely (probability of cable failure multiplied with the probability of a SELV/PELV failure).

b) In this case again, humans would be in danger, because when working with data cables, the cable ends are not contact protected.

c) Only PROFIsafe devices with output functions would be affected. They shall be able to handle their safety functions autonomously in any case, even if impermissibly high voltages occur. Here, it may be useful to increase the test voltage in 6.7.4.3 to 1500 V DC for final elements such as drives or devices with power supplies exceeding 60 V unless proven otherwise.

d) F-Hosts and PROFIsafe input devices shall detect all faults caused by overvoltage and respond in a safe manner. Conformance to the safety regulations can be shown through type testing.

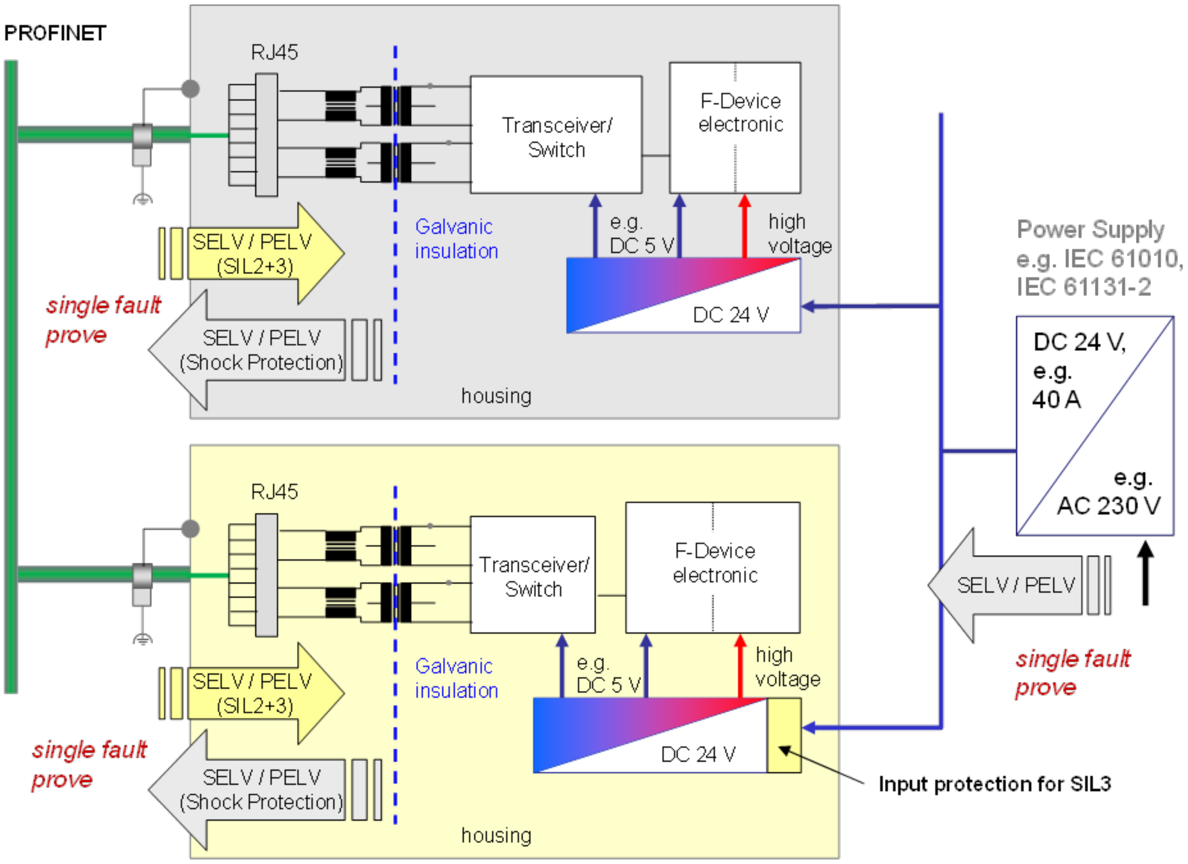


Figure 12 – SIL3/PLe considerations on overvoltages

The following conclusions regarding hazards from overvoltages for a PROFIsafe device ("safety electronic") can be drawn out of Figure 12:

a) If the main power supply fails above SELV/PELV, the PROFIsafe device in case of SIL3 shall be able to protect the "slave electronic" by special precautions (not within the scope of the PROFIsafe profile and guidelines). Thus this power supply port is 2 faults prove.

b) If the main power supply fails above SELV/PELV (2 faults), the galvanic isolation (opto-coupler, transformer) of a non-safety network device (1 fault) and the galvanic isolation of the PROFIsafe device (1 fault) must fail before the "slave electronic" will be damaged. Thus, the communication port of a PROFIsafe device is more than 2 faults prove.

6.7.4.5 Electrical safety for drives with integrated safety

The most basic safety function of drives is to safely switch off any motor induced torque or force without separation from power (STO = safe torque off). This function is used to protect against injury of personnel by unexpected motor movement (see IEC 60204-1: stop category 0 and emergency stop) but provides no protection against electrical shock.

Figure 13 shows an example for measures to ensure electrical safety for drives with integrated safety (and without integrated safety).

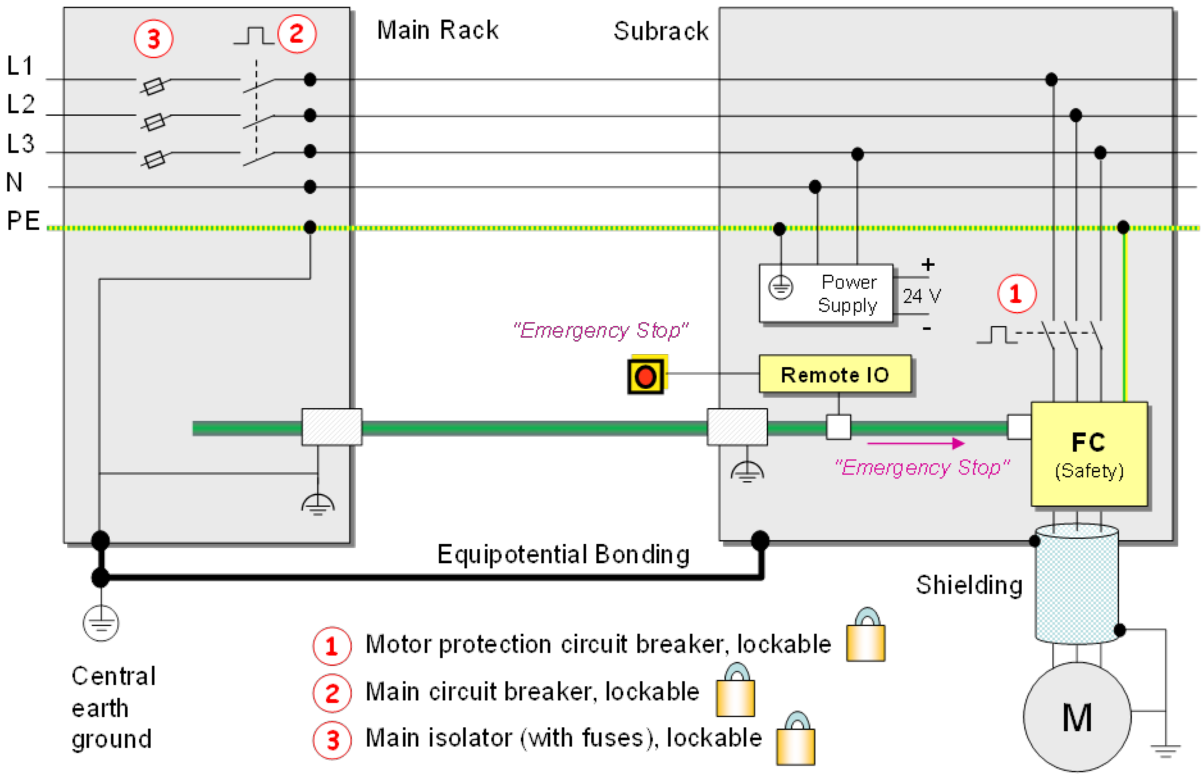


Figure 13 – Electrical safety for drives with integrated safety

In order to protect personnel from being hurt by electrical shock, motor protection circuit breakers①, main switches②, and circuit breakers/fuses ③ shall be used that all can be locked. See IEC 60204-1 for more details.

6.7.5 Clearance and creepage distances

The clearance and creepage distances shall be designed according product specific standards such as IEC 61131-2, IEC 61800-5, or relevant parts of the IEC 61010 series.

6.7.6 Flame-retardancy (thermal stress of insulation parts)

Insulating parts shall be sufficiently heat- and fire proof as specified in IEC 61131-2.

6.8 Electromagnetic immunity

6.8.1 Overview of standards

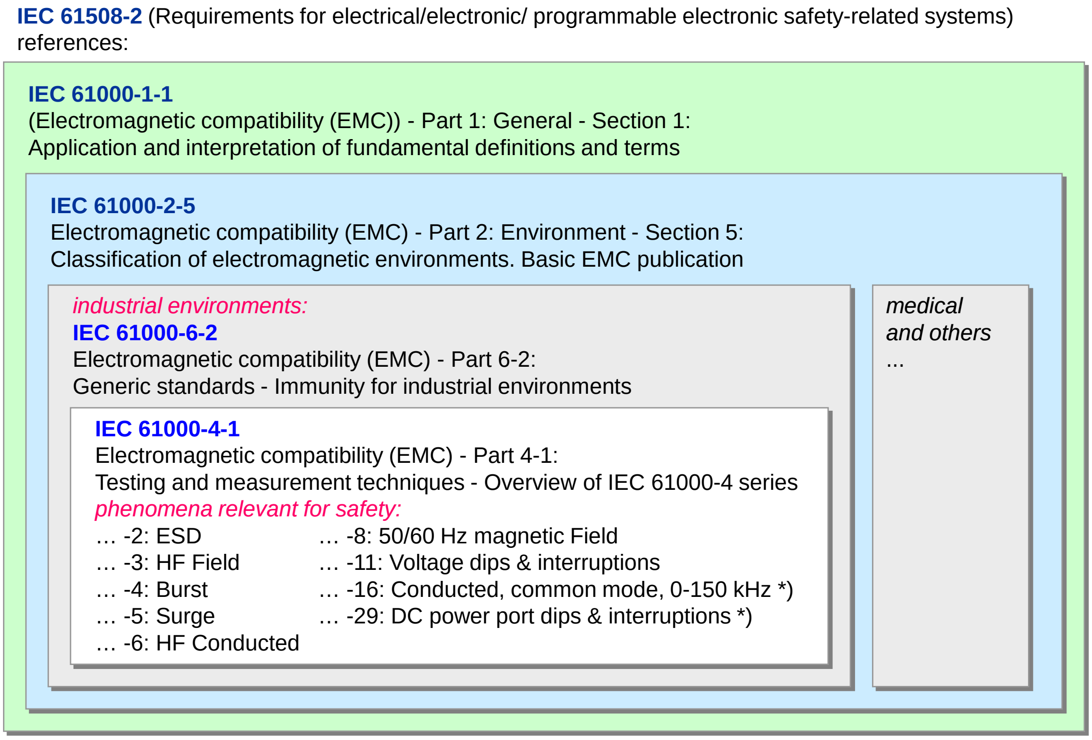
When creating the safety requirement specification (SRS), a comprehensive source for all kinds of electromagnetic phenomena is the Technical Report IEC TR 61000-2-5 standard. It should be clearly stated in the SRS, which of the assumed electromagnetic immunity levels are general values for non-safety functions (standard levels) and which electromagnetic immunity levels are required for the safety functions. It should be stated whether the specified value already includes an increased level.

NOTE IEC 61508 does not necessarily require that the proof of sufficient immunity is done by means of immunity tests. There might be other approaches to demonstrate sufficient immunity, e.g. by means of design and/or analysis.

NOTE The EMC requirements on Adjustable speed electrical power drive systems defined in IEC 61800-5-2 Ed 2.

This document provides advice how different electromagnetic immunity requirements for PROFIsafe devices should be handled within normal industrial environments as defined in IEC 61000-6-2 or IEC 61131-2 respectively for PROFINET and PROFIBUS automation equipment. Heavier industrial environments as described in IEC 61000-2-5 are not subject of this guideline. In such a case appropriate measures shall be taken to achieve the according electromagnetic immunity (e.g. extra housing, fibre optics, etc.).

Figure 14 shows the EMC standard IEC 61000-6-2 referenced by IEC 61508-2 and the corresponding hierarchy.



IEC 61508-2 (Requirements for electrical/electronic/ programmable electronic safety-related systems) references:

IEC 61000-1-1
(Electromagnetic compatibility (EMC)) - Part 1: General - Section 1:
Application and interpretation of fundamental definitions and terms

IEC 61000-2-5
Electromagnetic compatibility (EMC) - Part 2: Environment - Section 5:
Classification of electromagnetic environments. Basic EMC publication

industrial environments:
IEC 61000-6-2
Electromagnetic compatibility (EMC) - Part 6-2:
Generic standards - Immunity for industrial environments

IEC 61000-4-1
Electromagnetic compatibility (EMC) - Part 4-1:
Testing and measurement techniques - Overview of IEC 61000-4 series
phenomena relevant for safety:

… -2: ESD	… -8: 50/60 Hz magnetic Field
… -3: HF Field	… -11: Voltage dips & interruptions
… -4: Burst	… -16: Conducted, common mode, 0-150 kHz *)
… -5: Surge	… -29: DC power port dips & interruptions *)
… -6: HF Conducted	

medical
and others
…

*) not included in IEC 61000-6-2

Figure 14 – EMC standards referenced by IEC 61508 for industrial environments

For safety devices, IEC 61508-2 requires increased immunity of safety functions. The corresponding generic standard to IEC 61000-6-2 for functional safety is the IEC 61000-6-7. IEC 61000-6-7 defines an additional performance criterion DS. For safety functions, performance criterion DS is required when applying the amended test levels and durations of IEC 61000-6-7, which means the EUT can fail operating according to the specifications during and after the EMC tests. However, it shall always switch to a "defined state".

Figure 15 shows standards for EMC testing of functional safety equipment.

Functional safety within industrial environments:

IEC 61000-6-7

Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations

IEC 61000-4-1

Electromagnetic compatibility (EMC) - Part 4-1:
Testing and measurement techniques - Overview of IEC 61000-4 series

phenomena relevant for safety:

… -2: ESD
… -3: HF Field
… -4: Burst
… -5: Surge
… -6: HF Conducted
… -8: 50/60 Hz magnetic Field
… -11: Voltage dips & interruptions
… -16: Conducted, common mode, 0-150 kHz
… -29: DC power port dips & interruptions

Figure 15 – Standards for EMC testing of functional safety equipment

The environmental conditions within the process automation industries can be different from those of normal industrial environments and thus the specific levels and performance criteria described in IEC 61326-3-2 can be used for PA devices with functional safety.

Figure 16 illustrates the different scopes of IEC 61000-6-7 and IEC 61326-3-2. IEC 61000-6-7 (or IEC 61326-3-1) can be used for the machinery related part of an automation application (for example upstream logistics and downstream logistics); whereas IEC 61326-3-2 is related to the process automation part (mainstream) with specified electromagnetic environment, for example Ex-i.

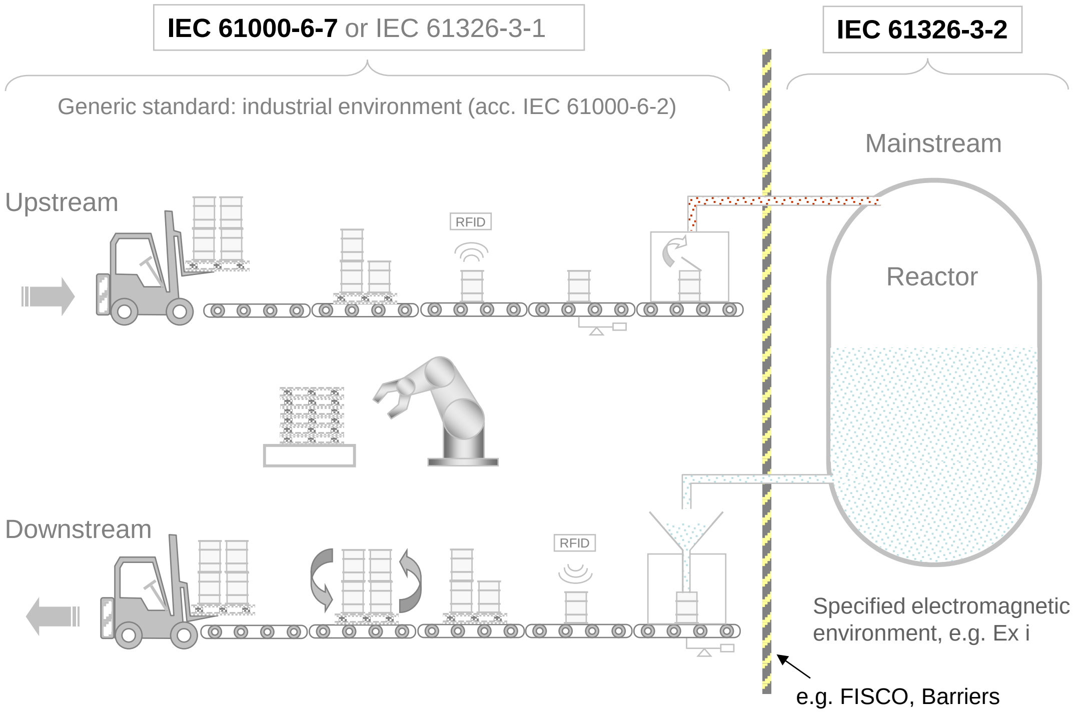

IEC 61000-6-7 or IEC 61326-3-1
IEC 61326-3-2
Generic standard: industrial environment (acc. IEC 61000-6-2)
Mainstream
Upstream
RFID
Reactor
Downstream
RFID
Specified electromagnetic environment, e.g. Ex i
e.g. FISCO, Barriers

Figure 16 – Example of application areas (up/downstream and mainstream)

For some product families, specific EMC standards exist such as IEC 61496-1 “Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests”.

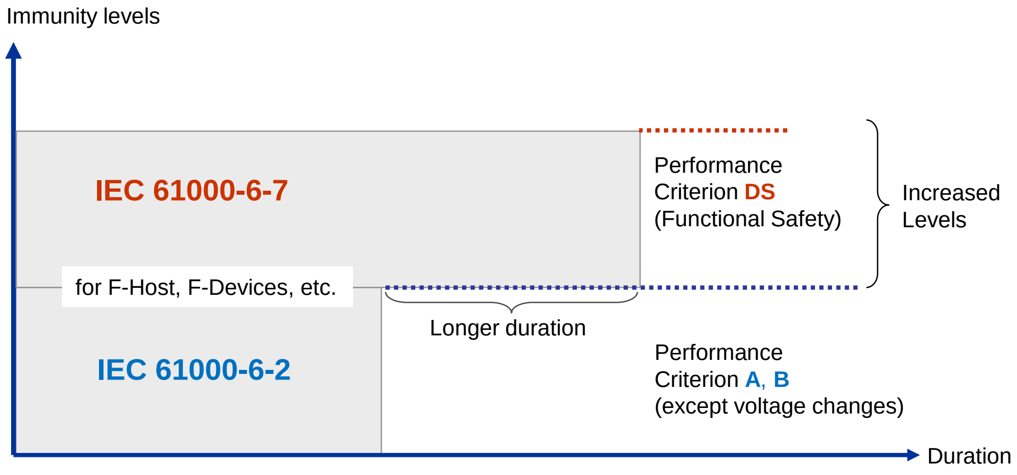

Immunity levels
IEC 61000-6-7
for F-Host, F-Devices, etc.
IEC 61000-6-2
Performance Criterion DS (Functional Safety)
Increased Levels
Longer duration
Performance Criterion A, B (except voltage changes)
Duration

Figure 17 – Increased EMC levels and duration

Annex A provides a comparison table of the test levels of several EMC standards.

6.8.2 EMC tests (phase *I* and *II*)

The EMC tests consist of two phases. In phase *I* the correct function of a safety EUT shall be tested at the test levels and durations defined in IEC 61000-6-2 for non-safety devices.

Figure 18 shows the generic concept for phase *I* and *II* testing. In phase *II* the equipment is tested with increased test levels and durations according to IEC 61000-6-7 ("increased immunity" according to IEC 61508).

This document differentiates between equipment directly exposed to the automation process such as remote input/out devices, sensors, and actuators (with or without logic solver functions) and logic solvers that are only processing data (including safety data). This document further differentiates for sensors and actuators between digital safety functions such as tripping, shut-down, stand-still, and analog safety functions such as measurement sensors or safe operating stop with drives.

For digital safety functions only performance criterion A is permitted (a motor shall not start in any case).

For analog safety functions performance criteria A or B are permitted, with a defined deviation of x % of the full scale (defined according user manual). In case of combined analog and digital safety data in one message, the tests can be performed in one step. However, the different performance criteria for analog and digital safety functions shall be observed.

Device manufacturers can specify more stringent deviations.

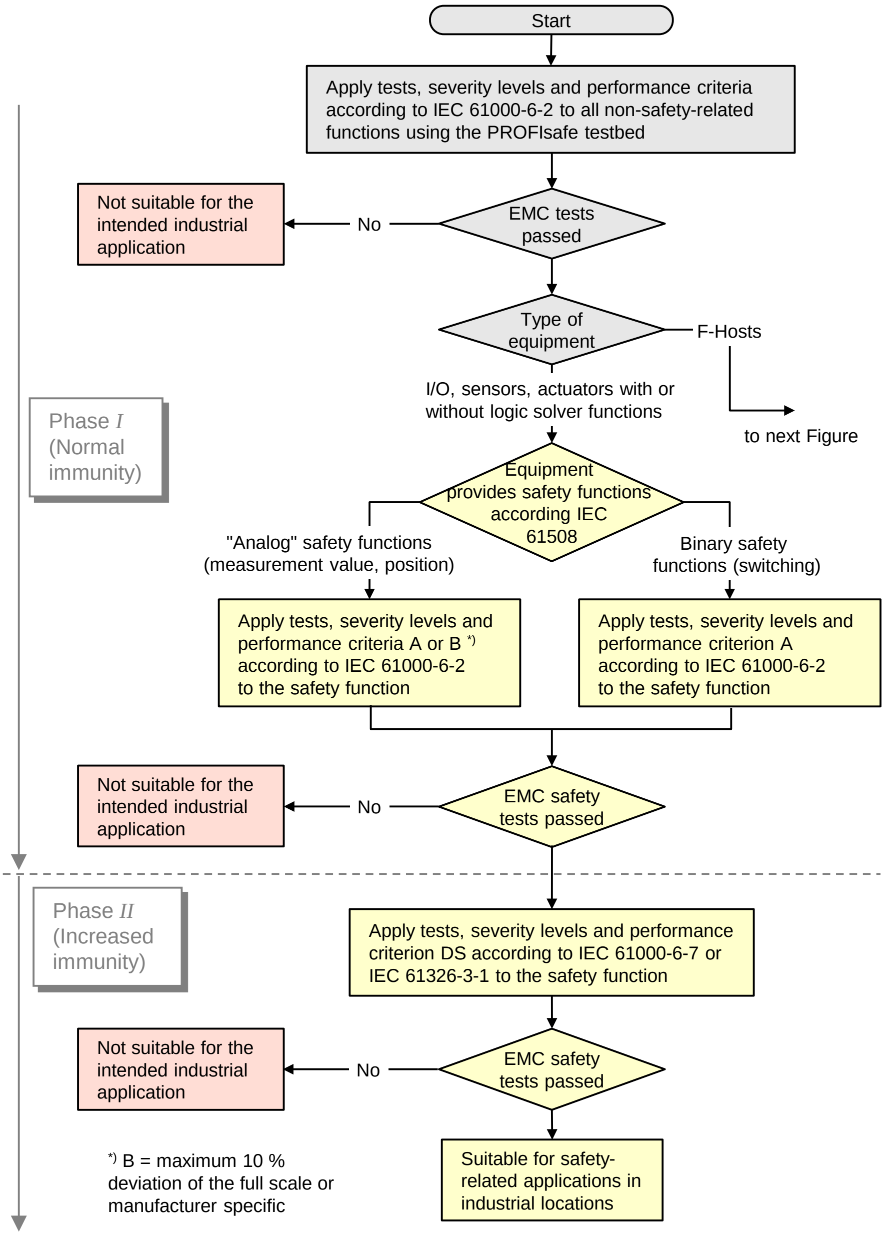

Start
Apply tests, severity levels and performance criteria according to IEC 61000-6-2 to all non-safety-related functions using the PROFIsafe testbed
EMC tests passed
No
Not suitable for the intended industrial application
Type of equipment
F-Hosts
to next Figure
I/O, sensors, actuators with or without logic solver functions
Phase I (Normal immunity)
Equipment provides safety functions according IEC 61508
"Analog" safety functions (measurement value, position)
Binary safety functions (switching)
Apply tests, severity levels and performance criteria A or B *) according to IEC 61000-6-2 to the safety function
Apply tests, severity levels and performance criterion A according to IEC 61000-6-2 to the safety function
Not suitable for the intended industrial application
No
EMC safety tests passed
Phase II (Increased immunity)
Apply tests, severity levels and performance criterion DS according to IEC 61000-6-7 or IEC 61326-3-1 to the safety function
Not suitable for the intended industrial application
No
EMC safety tests passed
*) B = maximum 10 % deviation of the full scale or manufacturer specific
Suitable for safety-related applications in industrial locations

Figure 18 – Principle concept for safety EMC testing (part 1)

Figure 19 shows the F-Host part of the generic concept for safety EMC testing. This testing shall be achieved by implementing one of two possible options:

- option 1 based on phase *I* and *II* testing; or,
- option 2 based on a proof of immunity through appropriate analytical evidence.

NOTE For example, option 2 is more suitable for safety logic solver software solutions used on general purpose industrial computer platforms, while option 1 is suitable for dedicated combinations of safety hardware and software.

Generalized performance criteria *A*, *B* and *C* as defined in IEC 61000-6-2 are not related to functional safety aspects and should therefore not be used as performance criteria in test phase *II* with increased test levels and durations.

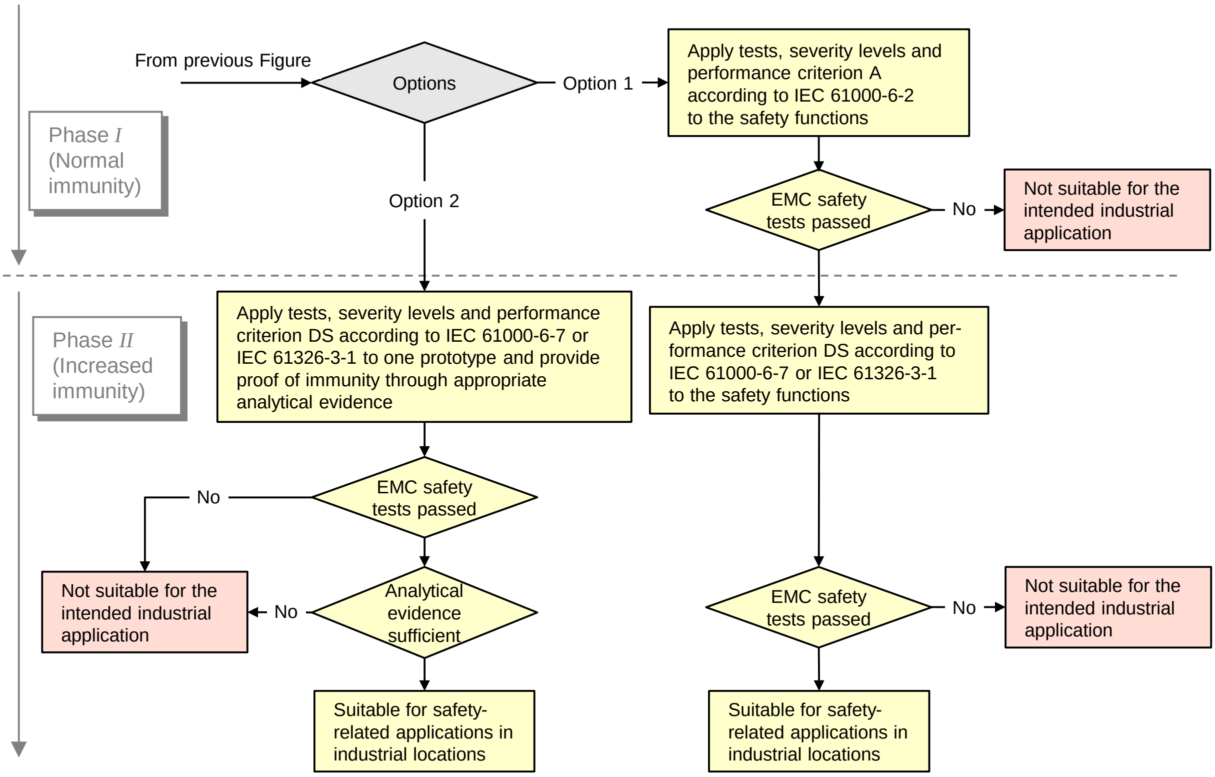

From previous Figure
Options
Option 1
Apply tests, severity levels and performance criterion A according to IEC 61000-6-2 to the safety functions
Phase *I* (Normal immunity)
Option 2
EMC safety tests passed
No
Not suitable for the intended industrial application
Phase *II* (Increased immunity)
Apply tests, severity levels and performance criterion DS according to IEC 61000-6-7 or IEC 61326-3-1 to one prototype and provide proof of immunity through appropriate analytical evidence
Apply tests, severity levels and performance criterion DS according to IEC 61000-6-7 or IEC 61326-3-1 to the safety functions
No
EMC safety tests passed
Not suitable for the intended industrial application
No
Analytical evidence sufficient
EMC safety tests passed
No
Not suitable for the intended industrial application
Suitable for safety-related applications in industrial locations
Suitable for safety-related applications in industrial locations

Figure 19 – Principle concept for safety EMC testing (part 2)

A specific performance criterion has been defined taking into account functional safety aspects. This performance criterion, DS, is defined in IEC 61000-6-7, or IEC/TS 61000-1-2 as follows:

- The functions of the equipment under test (EUT) intended for safety applications are not affected outside their specification, or
- The functions of the equipment under test (EUT) intended for safety applications may be affected temporarily or permanently if the EUT reacts to a disturbance in a way that detectable, defined state or states of the EUT are
  - maintained or,
  - achieved within a stated time.
- Also destruction of components is allowed if a defined state of the EUT is
  - maintained or,
  - achieved within a stated time.

The functions not intended for safety-related applications may be disturbed temporarily or permanently as defined in IEC 61000-6-7.

6.8.3 Mitigation

In case EMC product or sector standards for factory automation (safety for machinery) require lower test levels or shorter duration of tests than those defined in IEC 61000-6-7, the manufacturer of an EUT shall specify, how the increased immunity levels and durations of IEC 61000-6-7 (including the exception of 20 V for conducted RF) can be achieved via cabinets, optional shielding, or other auxiliary means (mitigation).

Figure 20 shows an example of how a control cabinet can be used for EMC testing. For all tests the doors of the cabinet can be closed except for the high frequency field test according to IEC 61000-4-3.

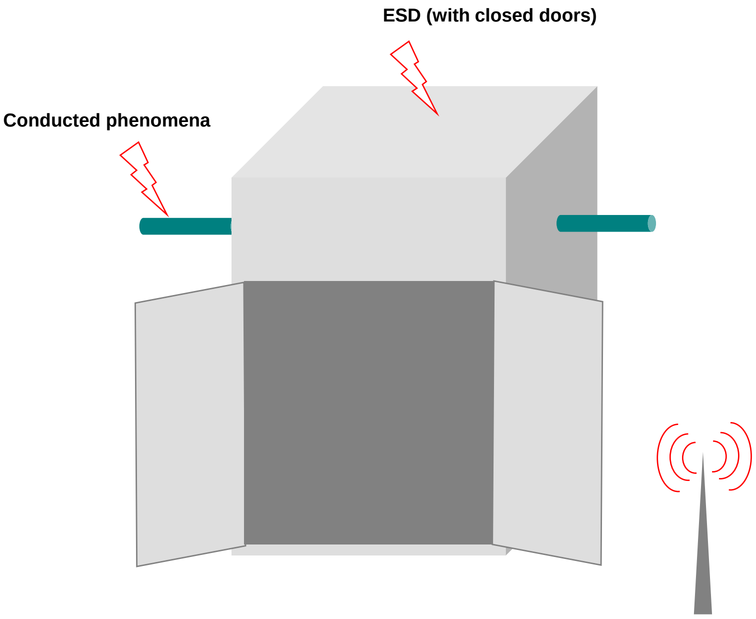


Figure 20 – EMC mitigation using a cabinet

6.8.4 Procedure model for designs

The procedure starts with the safety requirements specification (SRS) according to IEC 61508, which includes the EMC requirements for functional safety either by referencing a generic standard such as IEC 61000-6-7, or sector specific standards such as IEC 61326-3-2, or product specific standards such as IEC 61496-1. If none of these are matching the environmental conditions of the products deployment, IEC 61000-2-5 can be helpful to define phenomena and levels/durations for testing. IEC 61000-1-2 recommends an equipment requirement specification (ERS) for the detailed EMC test planning.

6.9 Easy circumvention

All components of the automation system in use for the transmission of PROFIsafe data shall provide measures against easy circumvention of safety functions, for example password protection of separate engineering software.

6.10 Field verification (process automation devices)

Special procedures are required for field devices in process automation that are intended for use in safety instrumented systems as laid down in the IEC 61511 series. Additionally to the error and failure aspects associated with software and electronics known with safety devices for factory automation or machinery, these process automation devices are exposed to the media they are expected to measure and/or to control (Figure 21).

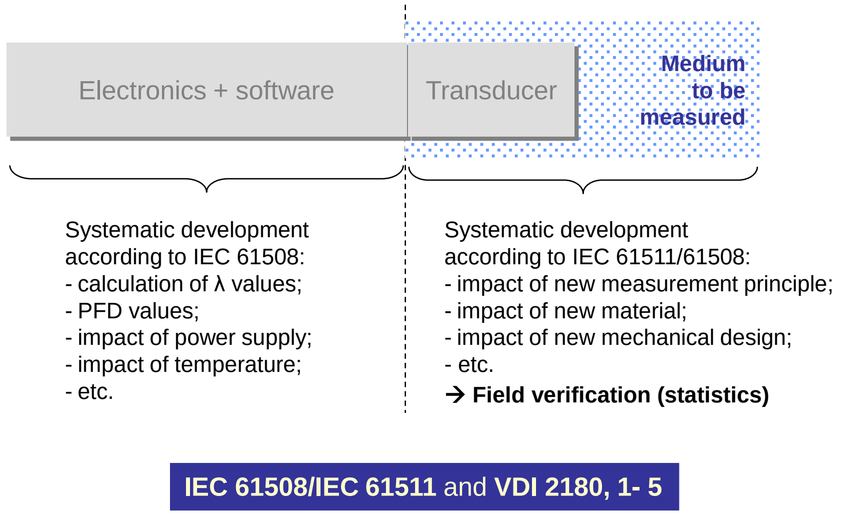

Electronics + software
Transducer
Medium to be measured
Systematic development according to IEC 61508:
- calculation of λ values;
- PFD values;
- impact of power supply;
- impact of temperature;
- etc.
Systematic development according to IEC 61511/61508:
- impact of new measurement principle;
- impact of new material;
- impact of new mechanical design;
- etc.
→ Field verification (statistics)
IEC 61508/IEC 61511 and VDI 2180, 1- 5

Figure 21 – Justification for field verification with process automation devices

Case 1: For devices with a new or changed type of transducer (see Figure 21) and, developed according to IEC 61508 and, assessed by a competent body, it is highly recommended to establish a period of field verification (experience). This verification shall comprise at least 10 devices within several different applications and last for at least six months in continuous operation.

NOTE Instructions on possible procedures can be found in IEC 61508-7 or within consortia in [55].

Manufacturers need to arrange for this field verification with their customers to obtain problem reports with the help of forms agreed upon by the competent body (see IEC 60300-3-2). These reports for the particular safety device will be delivered to the competent body, which in turn will confirm the successful field verification.

Case 2: For safety devices with "proven-in-use" transducers assessed entirely according to IEC 61508, it is possible to omit this field verification.

7 Deployment related guidance and recommendations

7.1 Installations

7.1.1 Guidelines

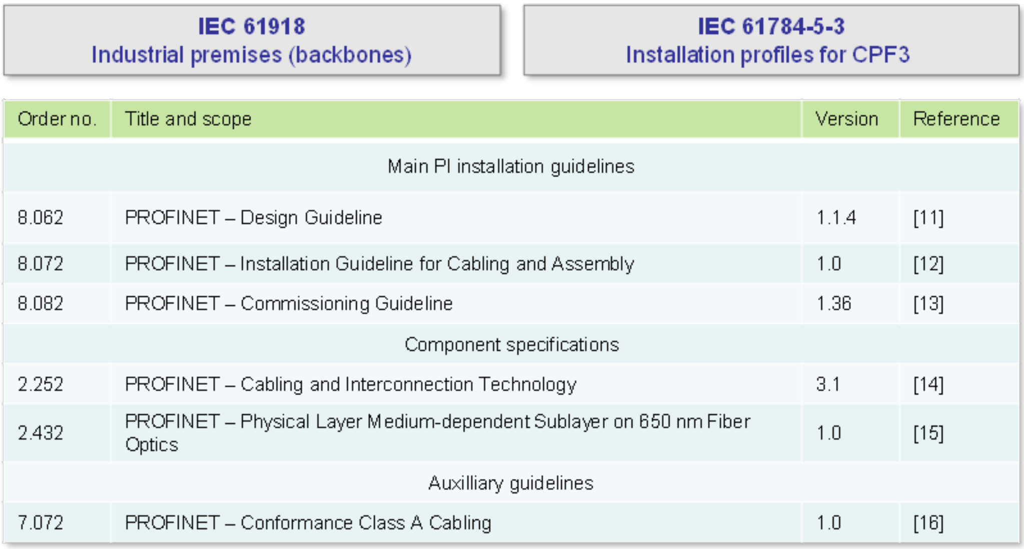
Figure 22 shows the available PROFINET guidelines related to installation that shall be considered for PROFIsafe automation applications.

The main PROFINET installation guidelines are [11] for planning, [12] for assembly, and [13] for commissioning. PROFIsafe highly recommends the usage of these guidelines to achieve the necessary availability preconditions as stated in 5.1.

The component specifications [14] and [15] can be helpful for the manufacturer and user to make decisions on connectors and cables for mechanical stress tests and guidance for the deployment of products (see **Error! Reference source not found.**).

The auxiliary PI guideline [16] defines the usability of ISO/IEC 11801 (generic cabling) and ISO/IEC 24702 (cabling between automation islands) for PROFINET networks.

For PROFIsafe networks on PROFINET it is not permitted to use *Conformance Class A* devices and network cabling transitions according to ISO/IEC 24702.



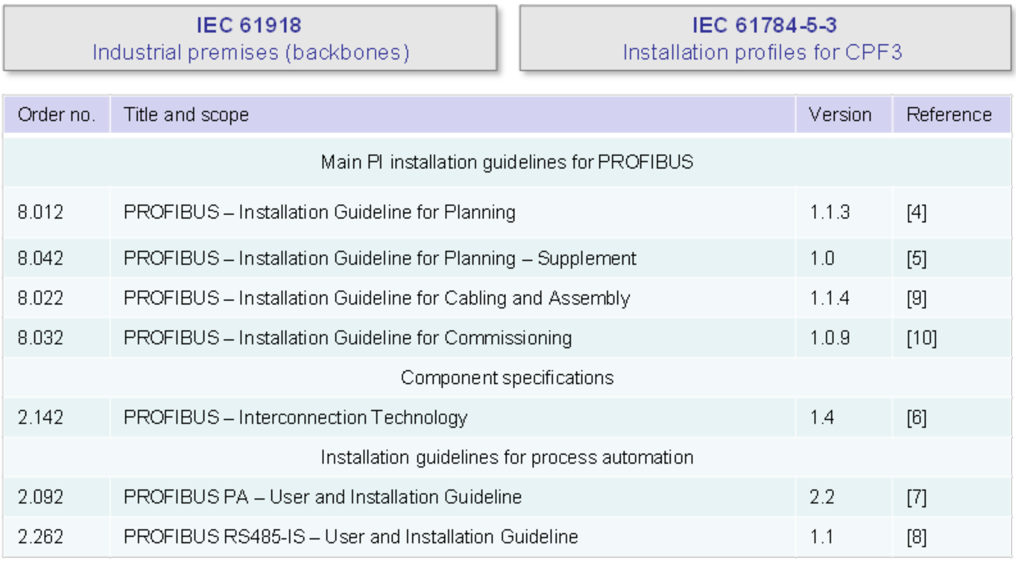
IEC 61918
Industrial premises (backbones)

IEC 61784-5-3
Installation profiles for CPF3

Order no.	Title and scope	Version	Reference
	Main PI installation guidelines		
8.062	PROFINET – Design Guideline	1.1.4	[11]
8.072	PROFINET – Installation Guideline for Cabling and Assembly	1.0	[12]
8.082	PROFINET – Commissioning Guideline	1.36	[13]
	Component specifications		
2.252	PROFINET – Cabling and Interconnection Technology	3.1	[14]
2.432	PROFINET – Physical Layer Medium-dependent Sublayer on 650 nm Fiber Optics	1.0	[15]
	Auxilliary guidelines		
7.072	PROFINET – Conformance Class A Cabling	1.0	[16]

Figure 22 – Relevant installation guidelines for PROFINET

Figure 23 shows the available PROFIBUS guidelines related to installation that shall be considered for PROFIsafe automation applications.



IEC 61918
Industrial premises (backbones)

IEC 61784-5-3
Installation profiles for CPF3

Order no.	Title and scope	Version	Reference
	Main PI installation guidelines for PROFIBUS		
8.012	PROFIBUS – Installation Guideline for Planning	1.1.3	[4]
8.042	PROFIBUS – Installation Guideline for Planning – Supplement	1.0	[5]
8.022	PROFIBUS – Installation Guideline for Cabling and Assembly	1.1.4	[9]
8.032	PROFIBUS – Installation Guideline for Commissioning	1.0.9	[10]
	Component specifications		
2.142	PROFIBUS – Interconnection Technology	1.4	[6]
	Installation guidelines for process automation		
2.092	PROFIBUS PA – User and Installation Guideline	2.2	[7]
2.262	PROFIBUS RS485-IS – User and Installation Guideline	1.1	[8]

Figure 23 – Relevant installation guidelines for PROFIBUS

The main PROFIBUS installation guidelines are [4] and [5] for planning, [9] for assembly, and [10] for commissioning. PROFIsafe highly recommends the usage of these guidelines to achieve the necessary availability preconditions as stated in 5.1.

The component specification [6] can be helpful for the manufacturer and user to make decisions on connectors and cables for mechanical stress tests and guidance for the deployment of products (see **Error! Reference source not found.**).

Especially for PROFIBUS PA are the user and installation guideline [7] and for the RS485-IS variant the user and installation guideline [8]. The PROFIsafe specification [1] describes the network crossing between PROFINET/PROFIBUS and PROFIBUS PA (MBP-IS or RS485-IS).

7.1.2 Active network components

Active network components such as repeater, router, switches, wireless access points, security gates, etc. shall be approved for industrial environment at least according IEC 61131-2. It is highly recommended to use active network components that can be configured via GSD and that provide diagnosis capabilities.

7.1.3 Topology constraints

Identical PROFIsafe applications (e.g. series machines) consisting of F-Hosts and F-Devices with the same node addresses within a PROFINET-based network can be connected via two-port routers according to [1].

PROFIsafe communication shall not be operated on RS485 transmission technology based PROFIBUS networks with spurs or branch lines.

7.1.4 Wireless

PROFIsafe is functional safe even across wireless networks. However, as stated in 5.1, sufficient availability shall be planned and established (at least 60 % reserve in electric field strength). Wherever possible, leaky-wave antennas should be used.

7.1.5 Cabling and wiring

7.1.5.1 General

For the planning of projects the different cable types (power, signal, communication, etc.) to be considered should be classified and the appropriate specifications and rules should be assigned (bending radius, shielding type, field of application, minimum distances to other categories, etc.).

7.1.5.2 Information about NFPA 79 drain wire (not safety-related)

NFPA 79 [52] requests:

"Where shielding is used around conductors in single or multi-conductor cables, a foil shield shall be permitted for non-flexing applications. A continuous drain wire shall be provided for foil shield types. A braided shield shall be used where subject to longitudinal flexing. Torsional flexing applications (e.g. robot arm) shall require shields designed specifically for their use. The shields and drain wire shall be covered with an outer jacket that is suitable for the environment. In all cases the shield shall provide a continuous conduction surface in the presence of bending and flexing."

There are PROFINET and PROFIBUS cable types with foil shields. However, they provide an additional braided shield that allows omitting the drain wire. In case of doubt, a more flexible and robust cable type should be used.

7.1.5.3 Hybrid cables (power and signal lines)

According to IEC 61508-2:2010, Tables A.16 it is *mandatory* for SIL1 to SIL4 to use separate cables for information lines and electrical energy lines. However, a NOTE associated with this requirement states that this separation is not "necessary for low power energy lines, which are designed for energising components of the E/E/PES and carrying information from or to these components".

Thus, for PROFIsafe systems the following applies:

- PROFIsafe communication is permitted on PROFIBUS PA transmission systems (MBP-IS = Manchester Bus Powered – Intrinsically Safe)
- PROFIsafe communication is permitted on PROFINET transmission systems using hybrid connectors and copper cables: a four-wire shielded information line part and a separate four-wire 24 VDC energy line part as specified in [11]. A device manufacturer shall ensure that no electromagnetic disturbances will be injected in these energy lines, e.g. through switching relays in output modules. Devices currently in the field with hybrid technology comprise for example wireless access points.
- PROFIsafe communication on PROFINET transmission systems using PoE (Power-over-Ethernet according IEEE 802.3af) based on modulation can be used for F-Devices (see Figure 24) if the SEL/PELV requirements are fulfilled.

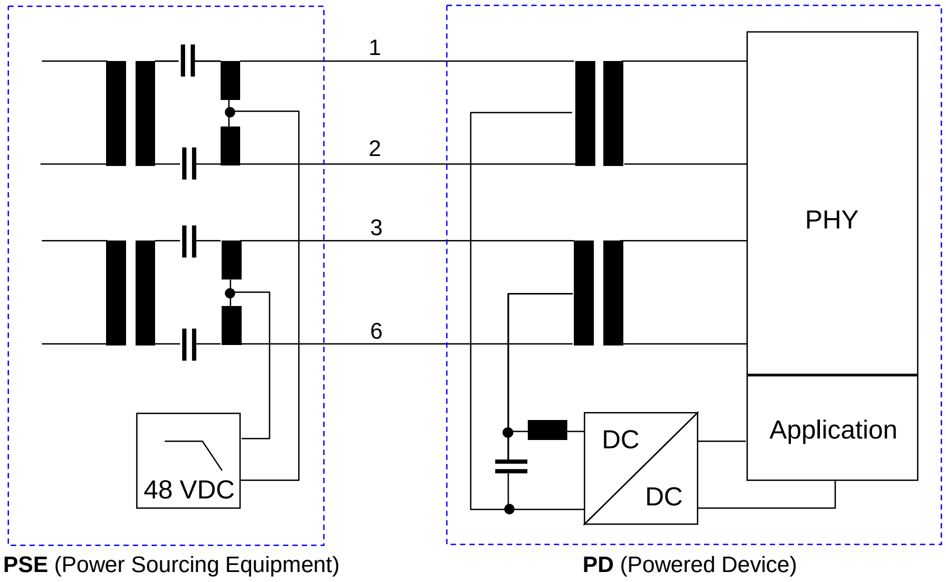


Figure 24 – Power-over-Ethernet

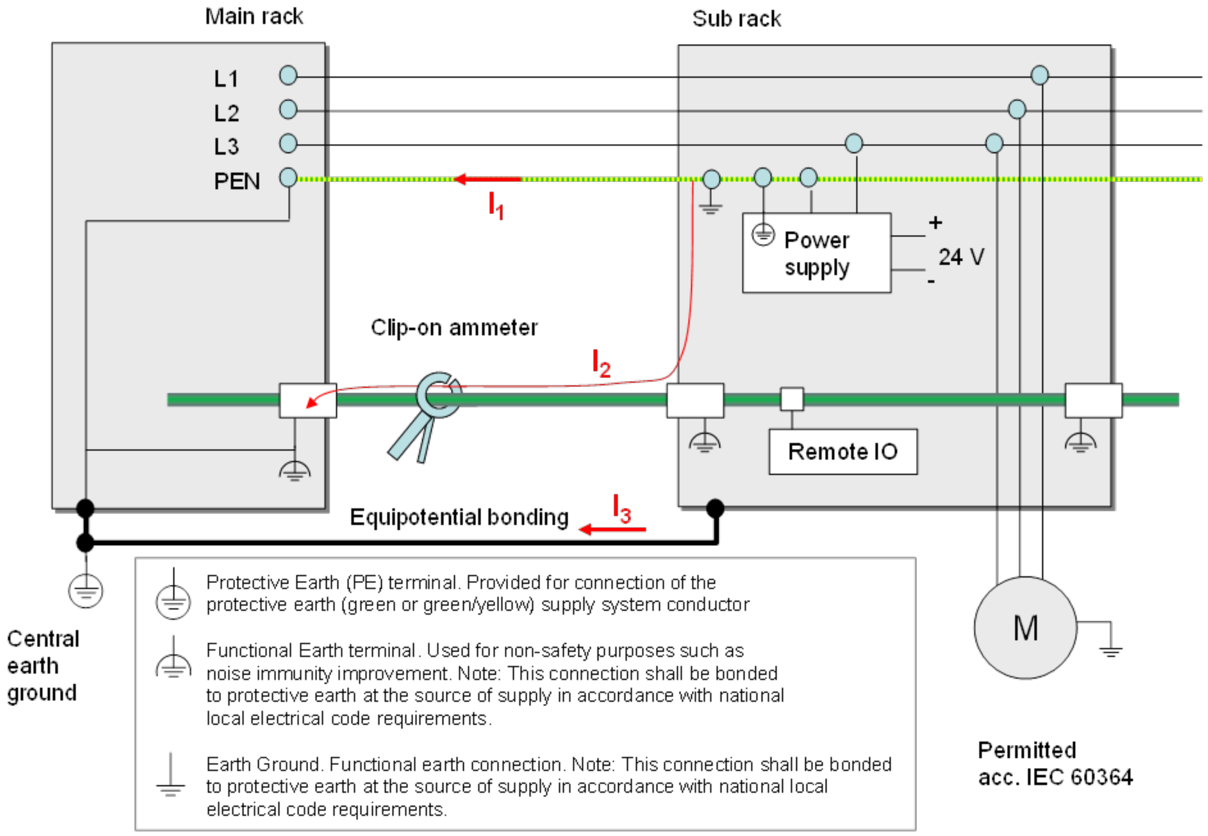
7.1.6 Power supply networks (TN-C, TN-S) (not safety-related)

A major source of electromagnetic interference is based on the wiring of power lines between decentralized automation systems communicating via fieldbus. So far it was common practice and permitted by standards to use a combined PE (protection earth) and N (neutral lead) conductor between main racks and sub racks. This kind of grounding is also called a TN-C power network. This method is acceptable if no extended fieldbus networks are involved and the currents within the power lines L1, L2, L3 are balanced out (Figure 25).

Modern drive electronics and power supplies are using high frequency switching technology, which causes unbalanced (injected high frequency) currents flowing through the combined PEN conductor of the system (I_1). The low impedance shielding of a fieldbus cable in parallel to the PEN conductor (I_2) will take over these high frequency currents and thus perturb the transmission of messages.

Modern facility layouts already provide a so-called equipotential bonding such that the grounding system can take over these currents (I_3).

It is highly recommended to use separate PE and N conductors ("5 conductors") in order to avoid fieldbus communication errors and possible retries, which will affect the efficiency and probably the availability of the entire system.



Protective Earth (PE) terminal. Provided for connection of the protective earth (green or green/yellow) supply system conductor

Functional Earth terminal. Used for non-safety purposes such as noise immunity improvement. Note: This connection shall be bonded to protective earth at the source of supply in accordance with national local electrical code requirements.

Earth Ground. Functional earth connection. Note: This connection shall be bonded to protective earth at the source of supply in accordance with national local electrical code requirements.

Figure 25 – Four conductor power network (TN-C)

Figure 26 shows an example of a 5-conductor power network. The corresponding types of power networks are called TN-S.

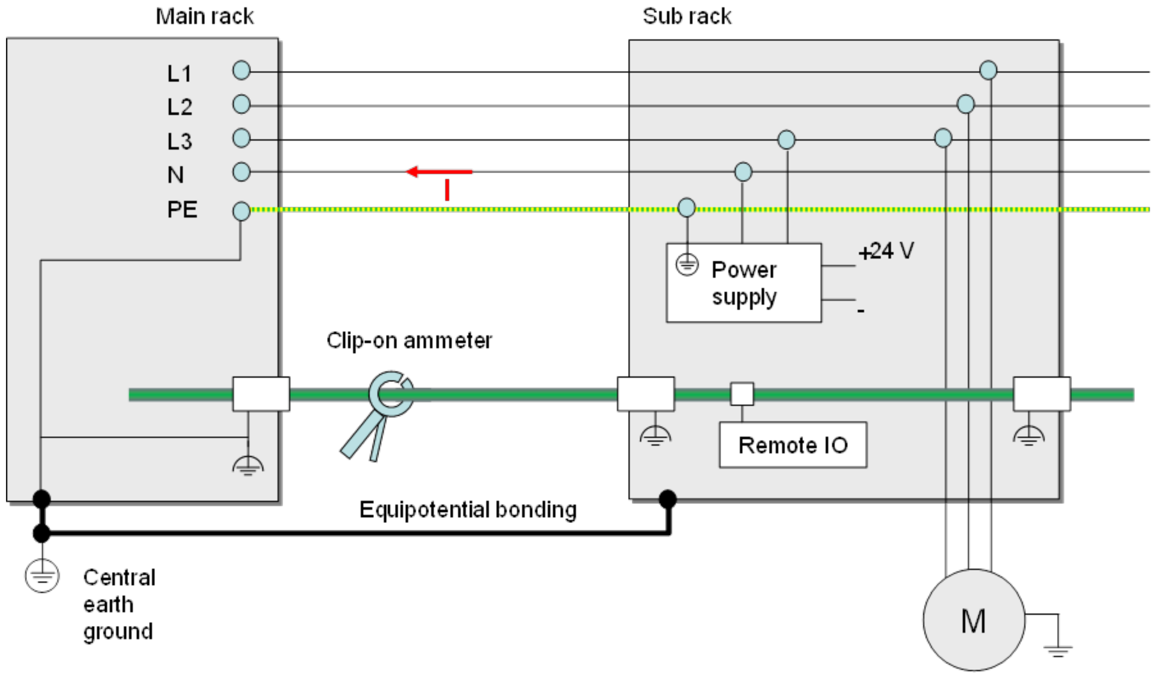


Figure 26 – Five conductor power network (TN-S)

More complete information about the design of power networks in respect to electromagnetic interference can be retrieved from [18] and [57].

7.1.7 Shielding and grounding (earthing) (not safety-related)

7.1.7.1 Basic effects

Two basic methods exist to protect data transmission wires. One is shielding, which keeps electromagnetic fields away from the sensitive high speed transmission signals. The other is twisting of the symmetrical signal wires, thus compensating the positive and negative induced voltages. Figure 27 demonstrates the effects of twisting and shielding of cables.

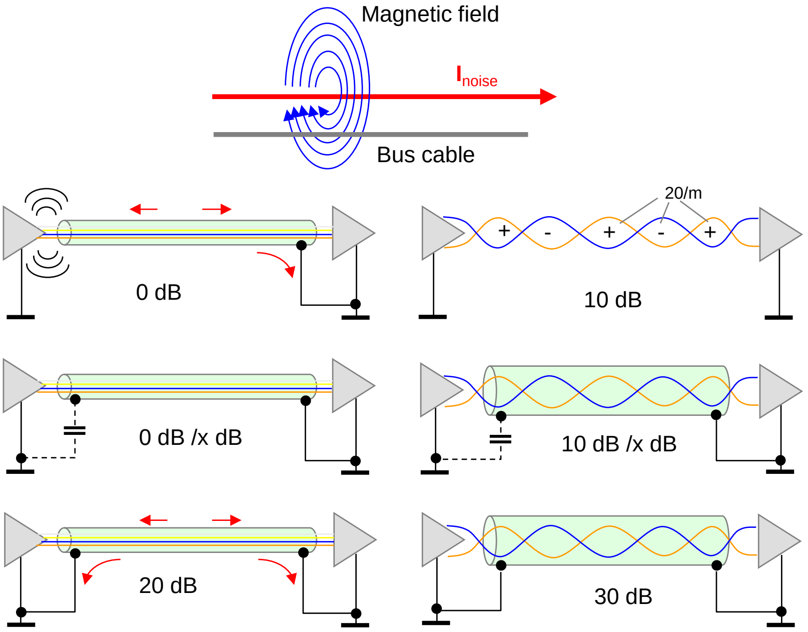


Figure 27 – Effect of shielding and twisting of cables

Correct shielding provides an attenuation of the interfered voltage of around 20 dB. Twisted pair wires with 20 twists per m are providing attenuation of around 10 dB. A combination of twisting and correct shielding leads to 30 dB attenuation. These values for shielding attenuation should be considered typical values only.

7.1.7.2 Single-ended versus double-ended grounding

In Figure 27 the noisy current (I_{noise}) on the power wire and its corresponding magnetic field is interfering with a shielded communication cable. Grounding the shield on one end causes the other (open) end to become a sending antenna. There is no doubt for high speed digital transmissions that a low impedance connection between shield and the equipment chassis "at both ends" is required in order for the shield to be effective, i.e. to compensate the interfering magnetic field [62]. This is also valid for electrical fields.

However, this two-ended grounding only achieves its purpose, if there is no difference be-tween the potentials on both ends. In order to establish equal potential, it is highly recommended to use sufficient equipotential bonding within the facility (Figure 26). If this is not possible, the use of optical fibre transmission is recommended.

In case of the transmission of analog signals such as in process industries, a capacitor with sufficient low impedance within the frequency range of the interference may be used (Figure 27). Usually in this case noise loops are the primary source of interference.

7.1.7.3 IP20

Components with an ingress protection of IP20 usually are located inside an enclosure/rack. Even in case of low shield transfer impedance across a connector housing to the chassis it is recommended to ground the shield at the entrance of the enclosure in order to keep the interior of the enclosure/rack free from noise.

7.1.7.4 IP65 or higher

Components with an ingress protection of IP65 or higher are usually mounted directly at the machine. If this grounding is not sufficient, additional measures has to be taken to provide sufficient grounding. In this case low shield transfer impedance across a connector housing to the chassis is required (e.g. M12 connector).

7.1.8 High frequency currents with power drives

Figure 28 demonstrates the problem of high frequency currents with variable speed power drives.

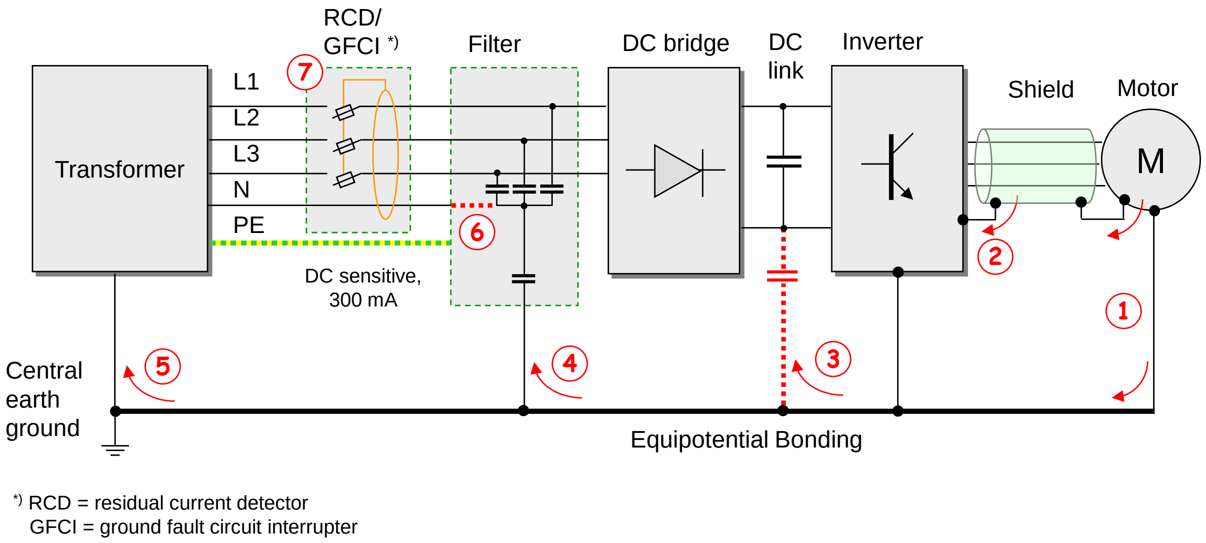


Figure 28 – High frequency currents with power drives

More and more industrial automation systems are using variable speed drives. Due to the inverter function and its switching operation parasitic high frequency currents are emerging on the cables to the motor and on the motor housing. According to Kirchhof's law these currents are looking for the shortest way to close the loop to the source of these currents, the DC link. See currents ①② in Figure 28. Since there is no path ③ to the DC link available in nowadays drives, the next possibility can be a filter at the entrance of the drives ④. Without such a filter the parasitic current is flowing across the equipotential bonding back to the grounded transformer ⑤ (central earth ground).

Normally ground fault circuit interrupters ⑦ for the protection of humans (30 mA) cannot be used with drives due to the unbalanced and high frequency current situation. In order to fulfil the requirements of fire protection (300 mA) DC sensitive ground fault circuit interrupters can be used. A connection of the neutral lead (N) with the central point in the filter ⑥ could improve the situation.

It is within the drive manufacturer's responsibility to specify the correct planning and installation of drives with integrated safety.

7.2 Network traffic (load)

The PI planning and installation guidelines are dealing already with this very important issue. It is highly recommended for PROFIsafe automation networks to check the network traffic (load) before production. Even if the traffic caused by control functions (IO controllers) has enough reserves, other network participants, for example HMI client-server permanent push operations could overload the network and cause timeouts of PROFIsafe communications (nuisance trips).

7.3 Security

7.3.1 General

Security has become more and more important in recent years. Up-to-now, it is common sense within standards and within the PI community to keep security and functional safety separate in PROFIsafe devices.

In contrast to functional safety, where countermeasures against errors and failures shall guarantee a tolerated residual error probability or rate for certain safety devices or safety functions, security deals with countermeasures against cyber or other human-driven attacks.

7.3.2 Standards and guidelines

Figure 29 shows an overview of the documents within the IEC 62443 series and their current status (End of 2014). Four parts are already available.

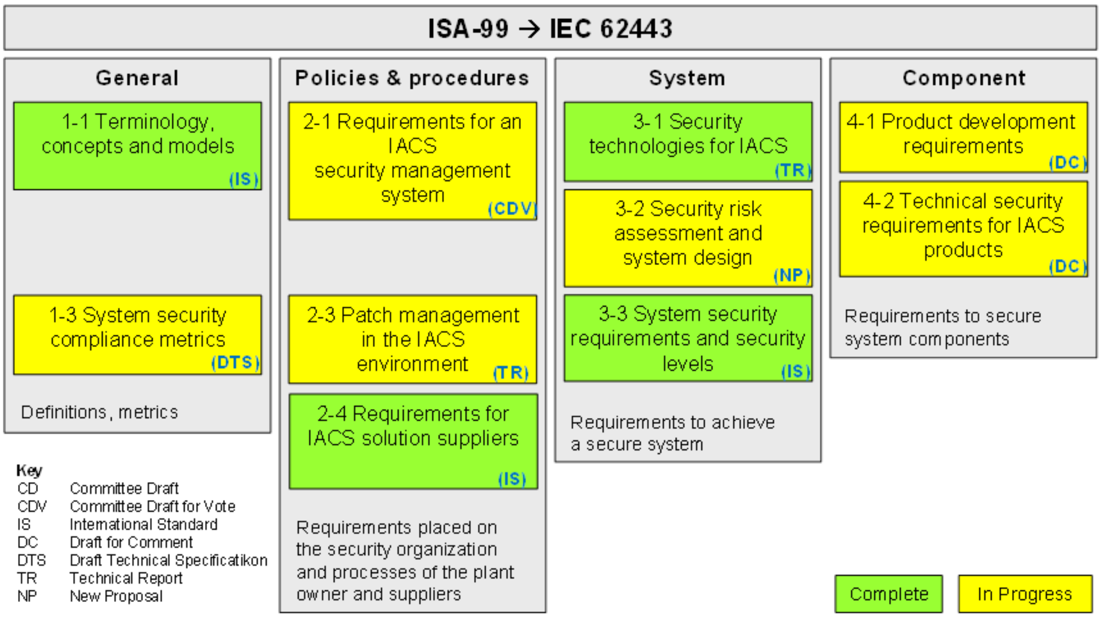

ISA-99 → IEC 62443
General
1-1 Terminology, concepts and models (IS)
1-3 System security compliance metrics (DTS)
Definitions, metrics
Policies & procedures
2-1 Requirements for an IACS security management system (CDV)
2-3 Patch management in the IACS environment (TR)
2-4 Requirements for IACS solution suppliers (IS)
Requirements placed on the security organization and processes of the plant owner and suppliers
System
3-1 Security technologies for IACS (TR)
3-2 Security risk assessment and system design (NP)
3-3 System security requirements and security levels (IS)
Requirements to achieve a secure system
Component
4-1 Product development requirements (DC)
4-2 Technical security requirements for IACS products (DC)
Requirements to secure system components
Key
CD Committee Draft
CDV Committee Draft for Vote
IS International Standard
DC Draft for Comment
DTS Draft Technical Specificatikon
TR Technical Report
NP New Proposal
Complete
In Progress

Figure 29 – Status of the IEC 62443 parts

IEC/TS 62443-1-1:2009 is a technical specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series [27].

IEC 62443-2-1:2010 defines the elements necessary to establish a cyber-security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IEC/TS 62443-1-1. The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

IEC/TR 62443-3-1:2009 provides a current assessment of various cybersecurity tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cybersecurity technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments, relative to the expected threats and known cyber vulnerabilities, and, most important, the preliminary recommendations and guidance for using these cybersecurity technology products and/or countermeasures.

IEC 62443-3-3:2013 provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C (control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.

7.3.3 Concepts for PROFINET and PROFIBUS

The basic concept for achieving appropriate security for PROFINET-based automation solutions relies on controlling the necessary accesses to the individual PROFINET domains [17]. This is accomplished by segmentation of the network and establishment of defined "zones" and by control of communication links ("conduits") between the segments and zones (cell security concept as shown in Figure 30). Together with the use of different technologies and methods, this results in the implementation of a defence-in-depth approach.

Because different solutions and technologies may be used depending on the specific requirements and these may be applied in any combination and in connection with segments, the result will be an integrated security concept.

In conjunction with the "Net load test" used during the certification process to verify the robustness of PROFINET devices under real-world network load conditions, a solution concept is now available that can be customized to meet the requirements of the production conditions in each case.

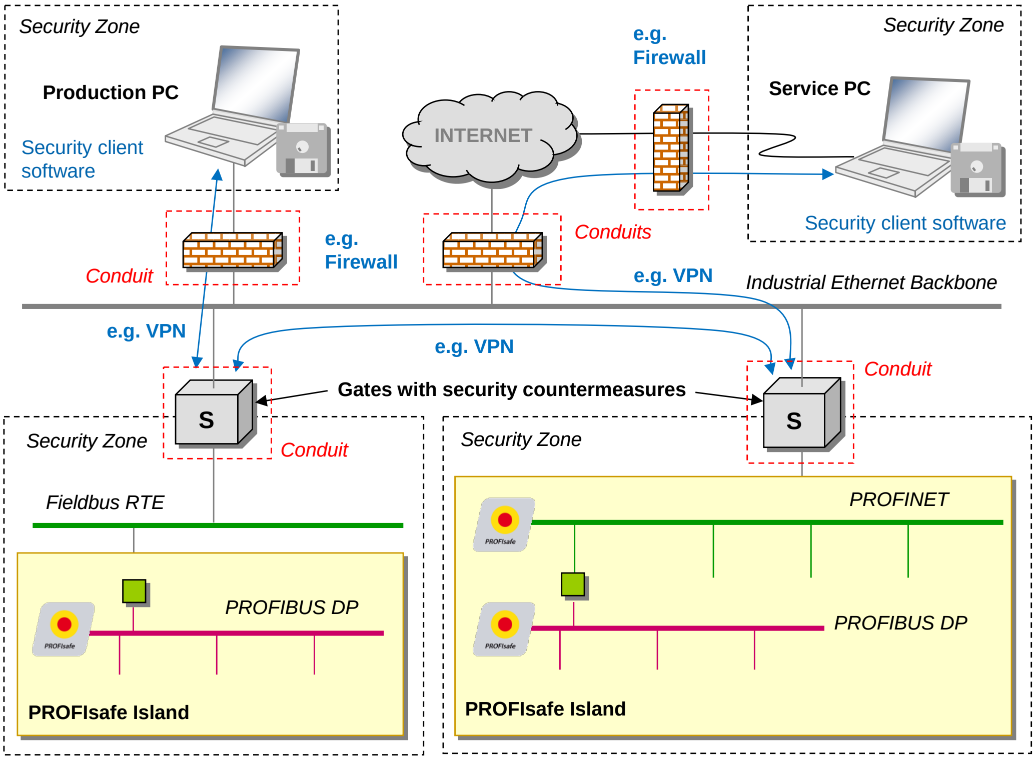


Figure 30 – Zones and conduits concept for PROFIsafe

NOTE: TC 44 considers that security threats identified by the machine manufacturer related to accessible interfaces of electrical devices should be recorded in the documentation accompanying the machine. A risk analysis of the security threats to the machine should be taken by the user who can then take measures to avoid them at the system level. This information should be taken into consideration by TC 44 convenors and will be conveyed to TC 65. This requirement can be fulfilled by the Conduit.

8 International specifics

8.1 General

As a rule, the international safety standards are accepted (ratified) globally. However, since safety technology in automation is relevant to work safety and the concomitant insurance risks in a country, recognition of the rules pointed out here is still a sovereign right! The national "Notified Bodies" (similar to IFA) decide on the recognition of certificates.

8.2 Europe

The previous chapter also applies to the different countries of Europe. However the national "Notified Bodies" in Europe cooperate closely, e.g.:

IFA	Institut für Arbeitsschutz – Institute for Occupational Safety and Health in Germany
HSE	Health & Safety Executive in the UK
SUVA	Schweizerische Unfallversicherungsanstalt (swiss accident insurance company in Switzerland)

In addition to IFA, other "Notified Bodies" are approved, for example, TÜV. However, "double assessment" is not required by law. The recognition of TÜV certificates that are based on the EN standards is customary.

8.3 USA

8.3.1 Market acceptance of certificates

An assessment report is not sufficient for market acceptance because of the insurance risk. The following should be noted:

- Legal requirements (such as OSHA),
- UL requirements,
- NFPA (for example, NFPA 79),
- Labor union requirements,
- etc.

8.3.2 UL508/508C (not safety-related)

In the US, UL508 is generally applied to PROFINET and PROFIBUS devices (not only to safety devices). In this case, it is a question of the fire hazards that a facility may present. The requirements for a communication interface (communication port) are considered as having been met if the device is listed as "Class 2“. For this, the power supplied to the device must be no more than 100 VA or the PROFIsafe device has additional means inside to limit the power. Short circuits shall be limited by a fuse.

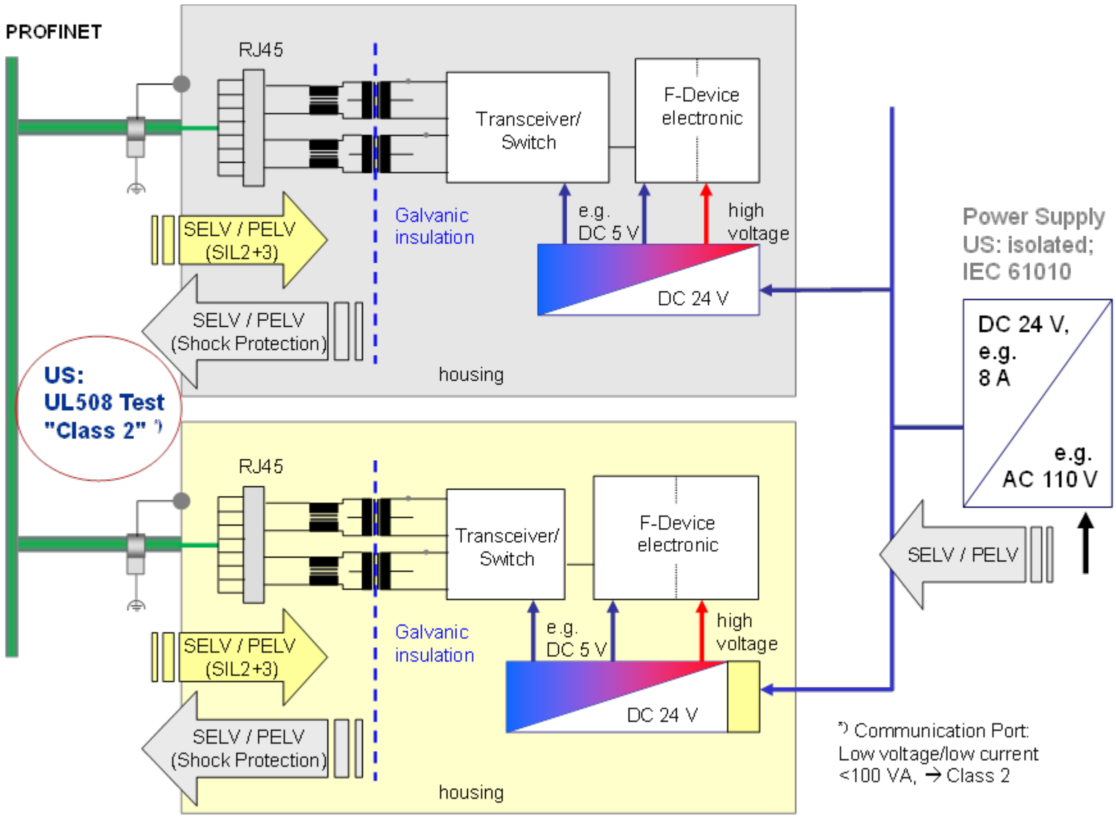


Figure 31 – UL508C considerations

Further recommendations:

Worldwide expectation is that typical computer equipment is touch-safe and that computer data communications circuits are not hazardous. Typical computer equipment provides no safety isolation between the internal logic circuits, data communication circuits and operator accessible parts (keyboard, mouse, touch panel, etc.). Any equipment that interconnects with commercial/consumer IT (Information Technology) equipment should not violate the presumed safety of the IT equipment.

As an example, Figure 31 shows the communication and power supply port conditions. The communication port shall be rated "class 2" and the 24 V DC power supply shall have a current limitation of 8 A.

8.4 Asia

In China, PROFINET and PROFIBUS are nationally recognized (GB/T). The PROFIsafe technology according to [1] will be nationally recognized in 2015.

Annex A
(informative)

Comparison of immunity levels in several IEC standards

Table A.1 provides a comparison of immunity levels in several IEC standards.

NOTE The content of this Annex A does not provide an exhaustive list.

Table A.1 – Comparison of immunity levels

Phenomenon	**Basic standard (IEC 61000-)**	**IEC 61000-6-2 Ind. app. generic**	**PC**	**IEC 61326-1 Industrial location**	**PC**	**IEC 61326-3-1 Industrial location**	**PC**	**IEC 61000-6-7 Ind. app. generic**	**PC**	**NOTES**
ESD	4-2	4/8 kV	B	4/8 kV	B	6/8 kV (x3)	FS	6/8 kV (x3)	DS	(x3) = No. of discharges (SIL3)
Radiated RF	4-3									
80 MHz - 1 GHz 1,4 GHz - 2 GHz 2 GHz - 2,7 GHz	(Enclosure)	10 V/m 3 V/m 1 V/m	A	10 V/m 3 V/m 1 V/m	A	**20 V/m** 10 V/m 3 V/m	FS	**20 V/m** 10 V/m 3 V/m	DS	
Burst	4-4									
AC Power		2 kV	B	2 kV	B	3 kV (x5)	FS	**4 kV** (x5)	DS	(x5) = Duration of test (SIL3)
DC Power		2 kV	B	2 kV	B	3 kV (x5)	FS	**2 kV** (x5)	DS	
I/O Signal + FE		1 kV	B	1 kV	B	2 kV (x5)	FS	2 kV (x5)	DS	
I/O Signal + PS		––	––	2 kV	B	3 kV (x5)	FS	**4 kV** (x5)	DS	
Surge	4-5									
AC Power		1 kV/2 kV	B	1 kV/2 kV	B	2 kV/4 kV (x3)	FS	2 kV/4 kV (x3)	DS	(x3) = Number of pulses (SIL3)
DC Power		**0,5 kV**	B	1 kV/2 kV	B	1 kV/ 2 kV (x3)	FS	1 kV/2 kV (x3)	DS	
I/O Signal		1 kV	B	1 kV	B	2 kV (x3)	FS	2 kV (x3)	DS	
I/O Signal + PS		––	––	1 kV/2 kV	B	2 kV/ 4 kV (x3)	FS	2 kV/4 kV (x3)	DS	
Conducted RF	4-6									
AC Power		**10 V**	A	3 V	A	10 V	FS	**20 V**	DS	
DC Power		**10 V**	A	3 V	A	10 V	FS	**20 V**	DS	
I/O Signal		**10 V**	A	3 V	A	10 V	FS	**20 V**	DS	
I/O Signal + PS		––	––	3 V	A	10 V	FS	**20 V**	DS	
Magnetic field	4-8									
50/60 Hz	(Enclosure)	30 A/m	A	30 A/m	A	30 A/m	FS	30 A/m	DS	If applicable
Voltage dips	4-11									
1 cycle 10/12 cycles 25/30 cycles	(AC Power)	0 % 40 % 70 %	B C C	0 % 40 % 70 %	B C C	0 % 40 % 70 %	FS FS FS	0 % 40 % 70 %	DS DS DS	
Voltage interr.	4-11									
250/300 cycles	(AC Power)	0%	C	0%	C	0%	FS	0%	DS	

Phenomenon	**Basic standard (IEC 61000-)**	**IEC 61000-6-2 Ind. app. generic**	**PC**	**IEC 61326-1 Industrial location**	**PC**	**IEC 61326-3-1 Industrial location**	**PC**	**IEC 61000-6-7 Ind. app. generic**	**PC**	**NOTES**
Common mode	4-16	––	––	––	––	Not required for FSCP based devices, see NOTE		Not required for FSCP based devices, see NOTE		Installation shall follow IEC 61918, IEC 60204-1, and FSCP specific if available
Voltage dips	4-29									
DC Power		––	––	––	––	40 % (10 ms)	FS	40 % (10 ms)	DS	
DC Power		––	––	––	––	40 % (10 ms)	FS	**70 % (10 ms)**	DS	
Voltage interr.	4-29									
DC Power		––	––	––	––	0 % (20 ms)	FS	0 % (20 ms)	DS	

Annex B
(informative)

Product, sector and application specific requirements

B.1 General

This Annex provides an overview of the requirements of product, sector and application specific requirements relevant for safety devices using PROFIsafe.

NOTE The content of this Annex B does not provide an exhaustive list.

B.2 Sensors (safety for machinery)

IEC 61496-1 requires some more stringent EMC tests for a large group of sensors such as light curtains (electro-sensitive protective equipment). It covers data interface issues such as PROFIsafe, which shall be observed for the design of the devices and for testing.

B.3 Low-voltage switchgear and controlgear devices

requirements for these devices are specified in IEC 60947-5-1 [19].

B.4 Burner management systems (BMS)

Devices intended for use in burner management systems shall be validated according to the relevant standards for the region/country.

NOTE In CENELEC countries, EN 13611 [45] and EN 14459 [46] will apply. Additionally, EN 298 [43] will be observed if relevant.

In the USA, parts of NFPA 85 [53] & NFPA 86 [54] appendices, ANSI/ISA-84.00.01-2004 Parts 1-3 ([47], [48], [49], ISA-TR84.00.02-2002 [50], ISA-dTR84.00.05 [51] will apply.

B.5 Pressure equipment directive (PED)

Devices shall be validated according to the relevant standards.

NOTE In countries of the European Union, devices within the scope of the Pressure Equipment Directive (97/23/EC) will be validated according to EN 764-7 [44] or other relevant harmonised standards within the PED.

Annex C
(informative)

PROFIsafe support

Support for PROFIsafe and the provision of related information, such as

- training classes for "Certified PROFIsafe Designers";
- PI Test Laboratories for PROFIsafe;
- connections to test laboratories for the conformance of cables and connectors with PI specifications;
- connections to "trouble-shooters" for automation systems with PROFINET, PROFIBUS, and PROFIsafe;
- connections to companies for commissioning (measurement) tools;

can be obtained from the following organization:

PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Str. 7
76131 Karlsruhe
GERMANY

Phone: +49 721 96 58 590
Fax: +49 721 96 58 589
E-mail: info@profibus.com
URL:www.profibus.com or
URL:www.profisafe.net

Bibliography

[1] PI Specification, *PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO*, V2.6.1, August 2014; PNO order No. 3.192

[2] PI Guideline, *PROFIsafe Policy*, V1.5, July 2011; PNO order No. 2.282

[3] PI Specification, *PROFIsafe – Test & Certification*, V2.2, September 2014; PNO order No. 2.242

[4] PI Guideline, *PROFIBUS – Installation Guideline for Planning,* V1.0, August 2009; PNO order No. 8.012

[5] PI Guideline, *PROFIBUS – Installation Guideline for Planning – Supplement,* V1.0, August 2009; PNO order No. 8.042

[6] PI Guideline, *PROFIBUS – Interconnection Technology,* V1.4, January 2007; PNO order No. 2.142

[7] PI Guideline, *PROFIBUS PA – User and Installation Guideline,* V2.2, February 2003; PNO order No. 2.092

[8] PI Guideline, *PROFIBUS RS485-IS – User and Installation Guideline,* V1.1, June 2003; PNO order No. 2.262

[9] PI Guideline, *PROFIBUS – Installation Guideline for Cabling and Assembly,* V1.0.6, May 2006; PNO order No. 8.022

[10] PI Guideline, *PROFIBUS – Installation Guideline for Commissioning,* V1.0.2, November 2006; PNO order No. 8.032

[11] PI Guideline, *PROFINET – Design Guideline,* V1.14, December 2014; PNO order No. 8.062

[12] PI Guideline, *PROFINET – Installation Guideline for Cabling and Assembly*, V1.0, January 2009; PNO order No. 8.072

[13] PI Guideline, *PROFINET – Commissioning Guideline*, V1.36, December 2014; PNO order No. 8.082

[14] PI Guideline, *PROFINET – Cabling and Interconnection Technology,* V3.1, March 2014; PNO order No. 2.252

[15] PI Guideline, *PROFINET – Physical Layer Medium-dependent Sublayer on 650 nm Fiber Optics,* V1.0, January 2008; PNO order No. 2.432

[16] PI Guideline, *PROFINET – Conformance Class A Cabling,* V1.0, July 2008; PNO order No. 7.072

[17] PI Guideline, *PROFINET – Security Guideline,* V2.0, November 2013; PNO order No. 7.002

[18] IEC 60364-4-44:2007, *Electrical installations of buildings – Part 4-4: Protection for safety – Protection against voltage disturbances and electromagnetic disturbances*

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

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

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

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

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

[24] IEC 61000-4-11, *Electromagnetic compatibility (EMC) – Part 4 11: Testing and measurement techniques – Voltage dips, short interruptions, and voltage variations immunity test*

[25] IEC 61000-4-16, *Electromagnetic compatibility (EMC) – Part 4 16: Testing and measurement techniques – Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz*

[26] IEC 61000-4-29, *Electromagnetic compatibility (EMC) – Part 4 29: Testing and measurement techniques – Voltage dips, short interruptions, and voltage variations on d.c. input power port immunity test*

[27] IEC 62443-1-1, *Security for Industrial Automation and Control Systems – Part 1-1: Terminology, concepts and models*

[28] IEC/TS 62443-1-3, *Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics*

[29] IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

[30] IEC/TR 62443-2-3, *Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment*

[31] IEC 62443-2-4, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*

[32] IEC/TR 62443-3-1, *Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*

[33] [33] Draft IEC 62443-3-2, Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design

[34] IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

[35] IEC 62443-4-1, *Industrial communication networks – Security for industrial and control systems – Part: 4-1: Product development requirements*

[36] IEC 62443-4-2, *Industrial communication networks – Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

[37] IEC 61496-1:2012, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

[38] IEC 61131-6, *Programmable controllers – Part 6: Functional safety*

[39] IEC 61800-5-1:2007, *Adjustable speed electrical power drive systems - Part 5-1: Safety Requirements – Electrical, thermal and energy*

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

[41] ISO 10218-1, *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*

[42] ISO 12100, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

[43] EN 298, *Automatic gas burner control systems for gas burners and gas burning appliances with or without fans*

[44] EN 764-7, *Pressure equipment – Part 7: Safety systems for unfired pressure equipment*

[45] EN 13611, *Safety and control devices for gas burners and gas burning appliances – General requirements*

[46] EN 14459, *Control functions in electronic systems for gas burners and gas burning appliances – Methods for classification and assessment*

[47] ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*

[48] ANSI/ISA-84.00.01-2004 Part 2 (IEC 61511-2 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative*

[49] ANSI/ISA-84.00.01-2004 Part 3 (IEC 61511-3 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative*

[50] ISA-TR84.00.02-2002 – Parts 1-5, *Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques Package*

[51] ISA-dTR84.00.05 (May 2009), *Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)*

[52] NFPA 79 (2015), *Electrical Standard for Industrial Machinery*

[53] NFPA 85 (2015), *Boiler and Combustion Systems Hazards Code*

[54] NFPA 86 (2015), *Standard for Ovens and Furnaces*

[55] NAMUR recommendation NE 130, *Proven-in-use devices for safety instrumented systems*, 2009.

[56] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*

[57] Kohling, A. (Hrsg.), *EMV von Gebäuden, Anlagen und Geräten*, 1998, VDE-Verlag, ISBN 3-8007-2261-5

[58] Mark I. Montrose, *EMC and the printed circuit board: design, theory, and layout made simple*, 1998, Wiley-IEEE Press, ISBN 978-0-7803-4703-8

[59] Paul Clayton, *Introduction to Electromagnetic Compatibility*, 2nd edition, 2006, ISBN 0-471-75500-1

[60] Tim Williams, *EMC for Product Designers*, 4th edition, 2007, ISBN 0-750-68170-5

[61] Peter Wilson, *The Circuit Designer's Companion*, 3rd edition, 2012, ISBN 0-080-97138-5

[62] www.sigcon.com, *archive topic: cable shield grounding*

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 96 58 590 ● Fax +49 721 96 58 589
E-mail info@profibus.com
ww.profibus.com ● www.profinet.com