PROFIBUS • PROFINET

PROFIsafe System Description

Technology and Application

PROFIsafe

Introduction

PROFIBUS and PROFINET are the only industrial communication systems providing comprehensive coverage including both factory and process automation. Both protocols are specified in the communication profile family 3 in the International Standards IEC 61158 and IEC 61784-1/-2.

One of the major events within the lifetime of the PROFIBUS & PROFINET International (PI) community was the first release of a specification for safety communication in 1999. It caused a quantum leap in possibilities in the world of automation.

The name of this technology is PROFIsafe and its logo is shown below.

Since this event, PROFIsafe has evolved to become the leading and most comprehensive safety communication technology in the world. PROFIsafe is an International Standard IEC 61784-3-3 since 2007.

It is the objective of this document to provide a thorough insight into the PROFIsafe technology and the related issues without becoming too engulfed in specific details. It is not meant to replace standards or the official specifications and guidelines mentioned below. Those are definitive and binding.

PROFIsafe is approved by both the TÜV and IFA.

Safety is a sensitive area of automation. Thus, the dissemination, implementation, and deployment of PROFIsafe technology must be treated seriously. The companies and institutions involved are obligated to conduct themselves according to the so-called "PROFIsafe Policy".

This short description is to serve as a complement to and a modest summary of the official sources.

The abbreviation "F" in this document stands for "fail-safe", "functional safety", or just "safety related".

Table of Contents

1. Safety in automation

Any active industrial process is more or less associated with the risk:

- of injuring or killing people,
- of destroying nature,
- of damaging investments.

With most processes it is quite easy to avoid risk without special requirements imposed on automation systems. However, there are typical applications associated with high risk, e.g. presses, saws, tooling machines, robots, conveying and packing systems, chemical processes, high pressure operations, offshore technology, fire and gas sensing, burners, cable cars, etc. These applications require special care and technology.

Over time the market balances out the reliability and availability of standard automation technology to a certain economic cost level. That means the failure or error rate of standard automation technology under normal circumstances is just acceptable for normal operations but not sufficient for the abovementioned high-risk applications.

The situation may be compared with a public mail system. While normal letter delivery is expected to be as affordable as possible at a certain reliability level, everybody will use special mail for important messages.

1.1 Technology change

In the past, microcontrollers, software, personal computers and communication networks influenced dramatically the standard automation technologies thus leading to cost reductions, improved flexibility and higher availability. With respect to safety, existing standards and regulations prohibited any use of those technologies. Safety automation had to be "hard-wired" and based on "relay" technology. See figure 1.

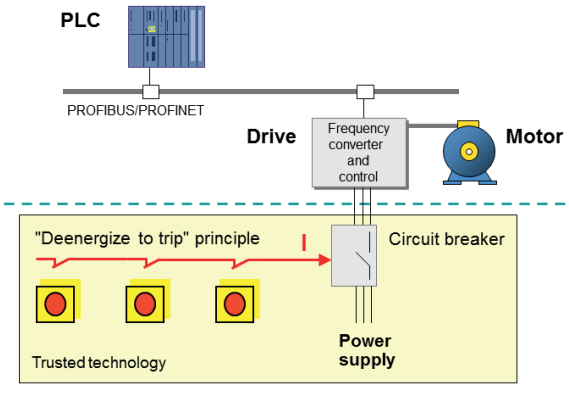

Figure 1: Classic safety with relays

This dichotomy or gap is quite comprehensible due to the fact that safety relies on trusted technology or material. Trust, in turn, is based on experience and experience needs time. But adding "classic" safety to modern automation solutions often leads to disappointing situations. For example, costs due to additional wiring and engineering, less flexibility and availability than expected and other disadvantages such as undefined stop positions of machines and tedious efforts to resume operation.

This situation has now changed dramatically. Microcontrollers and software tools have been proven in use in millions of applications and the preconditions for their use in safety applications are given since the introduction of the international standard IEC 61508.

The error detection mechanisms of many types of digital communication systems have been investigated and are well understood. Standards like IEC 62280-1 have been paving the ways.

1.2. PI achievements

That's why PI has developed the PROFIsafe technology as an additional layer on top of the existing PROFIBUS and PROFINET protocols. It reduces the residual error probability of the data transmission between a F-Host (safety controller) and a F-Device (safety device) to the level required by or better than the relevant standards.

PROFIsafe can be completely realized in software, making it easy to implement while covering the entire spectrum of safety applications utilizing PROFIBUS and PROFINET in process and factory automation. It is even approved for wireless transmission channels such as WLAN and Bluetooth. With the help of security provisions such as zones and conduits, it can be used on open Industrial Ethernet Backbones.

It covers the need for high availability and low power consumption in process automation as well as the demand for short reaction times within milliseconds in factory automation.

Modern F-Devices such as laser scanners or drives with integrated safety now can flourish as needed. The handling of their individual safety parameters (iParameters) is made easy due to iPar-Server support. This system support comprises interfaces for F-Device tools within engineering frameworks (for example the Tool Calling Interface) and iParameter storage and retrieval options (iPar-Server). It is important to note that the tool interfaces and the iPar-Server feature can also be used by any non-safety device.

The IEC 61508 standard defines special requirements such as increased electromagnetic immunity without specifying the details. A supplemental guideline "PROFIsafe Environment" fills this gap and others for the development and deployment of F-Devices and F-Hosts.

There is common agreement within PI that only F-Devices and F-Hosts in PROFIBUS and PROFINET networks that are certified according IEC 61508 are permitted. Conformity to the PROFIsafe protocol shall be tested by PI test laboratories and certified by PI office. A supplemental "PROFIsafe Test Specification" document defines the roles and tasks of assessment bodies such as TÜV and the roles and tasks of PI test laboratories.

See www.profisafe.net for actual information about PROFIsafe and www.profibus.com for general PROFIBUS and PROFINET information.

1.3. International standards

In most countries, national laws regulate how people and the environment shall be protected. In Europe for instance, the "Low Voltage Directive", the "EMC Directive", and the "Machinery Directive" are examples of such legislation. The laws in turn refer to approved International Standards.

In figure 2 you find a selection of relevant IEC and ISO standards dealing with safety and fieldbus issues and how they are related.

The basic standard for functional safety is the IEC 61508 covering the functional safety of electrical equipment and the basic principles and procedures. It introduces a quantitative approach for calculating the residual probability of so-called safety functions to fail (Safety Integrity Levels - SIL). It is mainly useful for F-Device and F-Host developers. The sector standard IEC 62061 describes the specific safety aspects for machinery applications such as those found in factory automation. This standard deals with ready-to-use systems, subsystems, and elements and how to assess safety functions for certain combinations of these. ISO 13849-1 is the successor of the EN 954-1 (withdrawn in 2011) and has a similar scope. However, it introduces a slightly different calculation model (Performance Levels - PL) and covers non-electrical devices such as hydraulic valves, etc. For safety of machinery, the basic terminology and principles for design are defined in ISO 12100 as well as risk assessment and risk reduction. The IEC 60204-1 specifies general requirements and recommendations relating to the electrical equipment of machines. Some of the issues are power supply, protection against electrical shock, emergency stops, conductors and

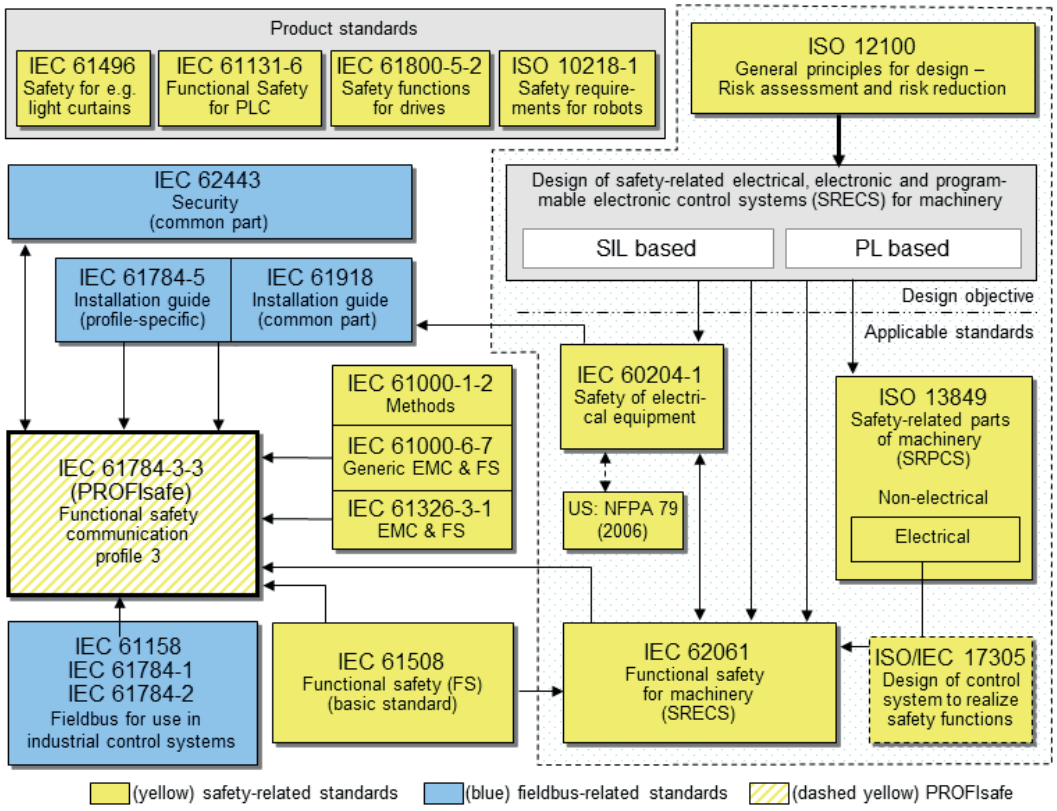

Figure 2: International fieldbus and safety standards for factory automation

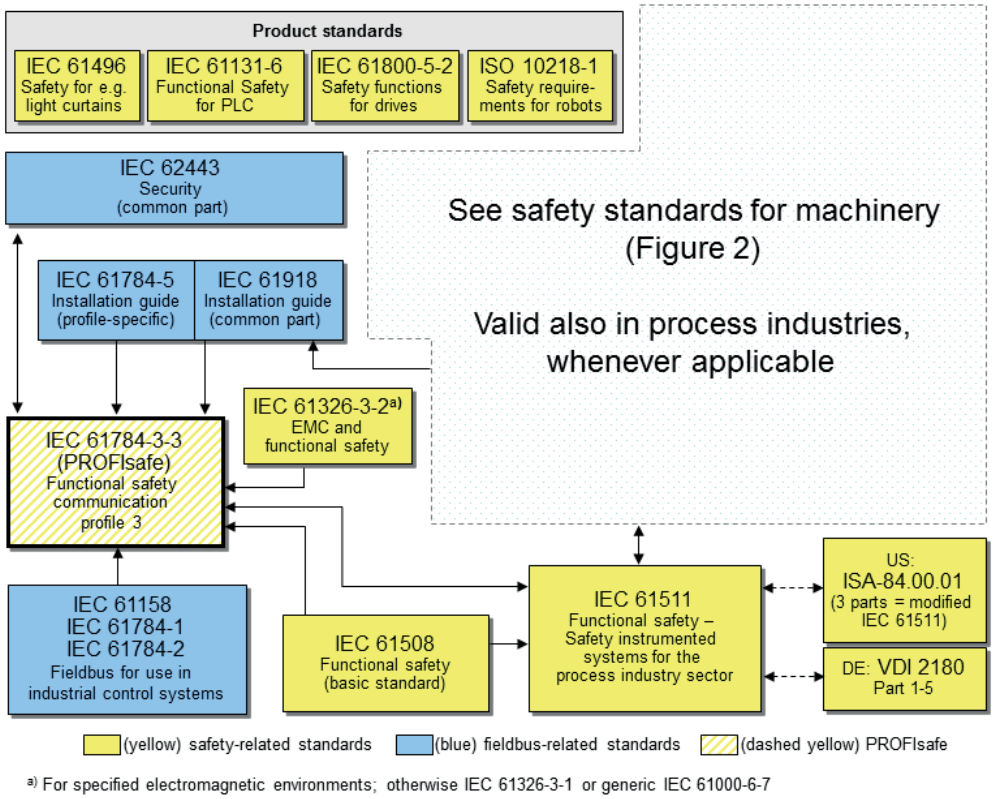

Figure 3: International fieldbus and safety standards for process automation

cables, etc. Product standards such as IEC 61496, IEC 61800-5-2, IEC 61131-6 and ISO 10218-1 for example, deal with the requirements for individual product families.

The annex of the European "Machinery Directive" lists the machines and parts which legally require certification e.g. by a "Notified Body" (IFA, TÜV, FM-Factory Mutual, etc.). If there is a harmonized corresponding product standard (for example, IEC 61496), a declaration by the manufacturer can be sufficient.

The requirements for F-Devices and F-Hosts to provide increased electromagnetic immunity are defined within the generic IEC 61000-6-7 and in sector standard IEC 61326-3-1. Special performance criteria DS ("defined state") allow for incorrect functioning under increased electromagnetic interference conditions above the normally required levels. However, in these cases the equipment under test (EUT) shall go at least into a safe state.

The fieldbus standards are specified in IEC 61158 and IEC 61784-1. Realtime Ethernet variants such as PROFINET IO are defined in IEC 61784-2. Common parts for installation guidelines are summed up in IEC 61918, whereas profile-specific parts are collected in IEC 61784-5. Common parts for security guidelines are summed up in IEC 62443, whereas profile-specific parts are planned for a future IEC 61784-4.

In figure 3 you find a similar selection of IEC and ISO standards adapted to the requirements of process automation. Here, the sector standard IEC 61511 is considering the particular situation of long term experience ("proven-in-use") with very sensitive process instrumentation and a specified electromagnetic environment in this area. Thus, the sector standard IEC 61326-3-2 takes these EMC requirements into account.

2. Requirements fullfilled

From the very beginning, it was the intention of PROFIsafe to specify a comprehensive and efficient solution for both the safety device developer and the end user. The PROFIsafe protocol is suitable for both PROFIBUS and PROFINET networks without impacts on these existing fieldbus standards. It is possible to transmit safety messages on the existing standard bus cables in coexistence with standard messages (figure 4).

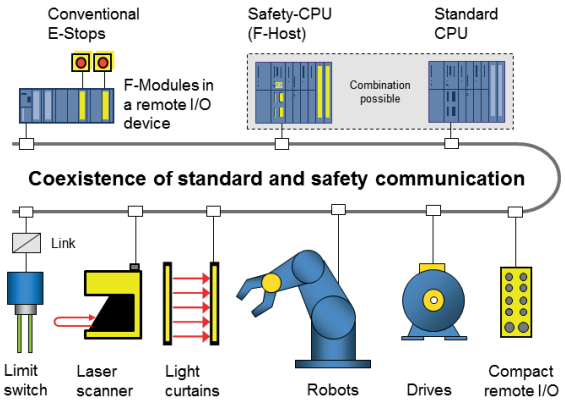

Figure 4: The "Single Channel" approach

This "Single Channel" approach also allows the use of standard PLCs with integrated but logically separated safety processing. This way media redundancy to achieve higher availability could be realized as an option. Physical separation of standard and safety communication is of course supported, too, without any drawback induced by PROFIsafe. Even in that case, users can still benefit from the common PROFIsafe technology on the separate communication networks.

The PROFIsafe protocol does not have any impact on the standard bus protocols. On the other hand, it is completely independent from the base transmission channel, and works equally well over copper wires, fiber optics, wireless communication links, or backplanes. For instance, PROFIsafe does not make any assumptions regarding transmission rates or error detection mechanisms. This is called the "Black Channel" principle (figure 5).

The PROFIsafe protocol eliminates the need for a safety assessment of individual backplane communications or other transmission paths beyond the PROFINET and PROFIBUS networks. Therefore, it secures the whole path from the location where a safety signal originates (e.g. F-Module in a remote I/O device) to the location where it is processed (F-Host) and vice versa (figure 6).

The PROFIsafe protocol can be used for safety applications up to SIL3 according to IEC 61508 / IEC 62061, or PL "e" / Category 4 according to ISO 13849.

The parameters for the PROFIsafe protocol are defined, maintained, and engineered with the standard means of PROFIBUS or PROFINET, i.e. via GSD. However, the parameters should be secured during storage, interpretation, value assignment and transfer from the configuration tool to the IO Controller or DP-Master and from there into the F-Device. There has to be the same set of PROFIsafe (protocol) parameters for all F-Devices or F-Modules in a remote I/O device to ensure uniform handling (so-called F-Parameter).

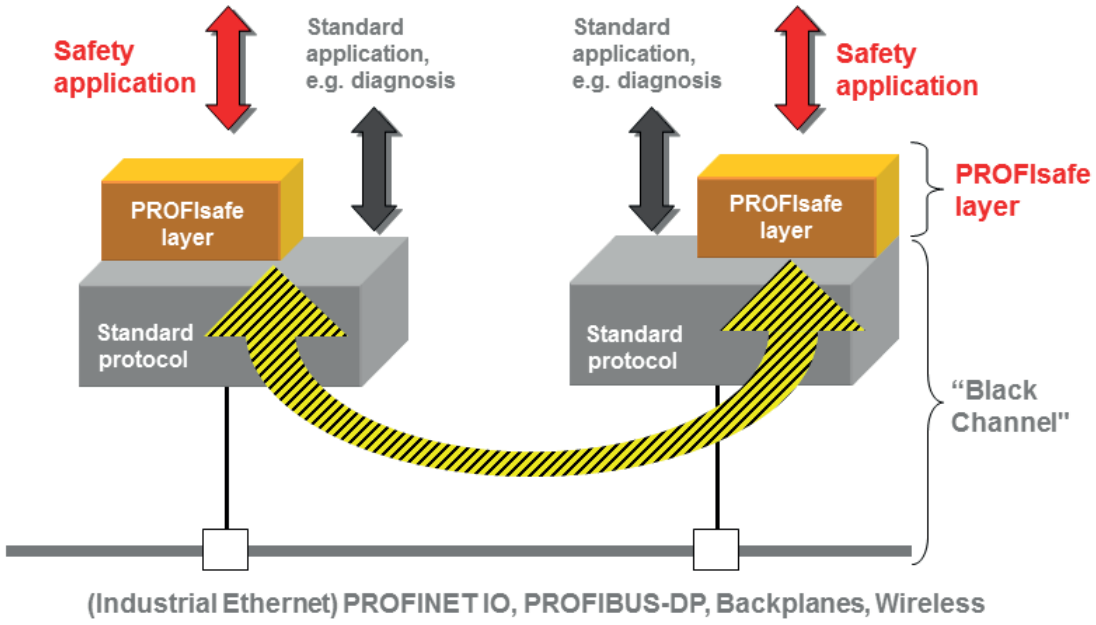

Figure 5: The "Black Channel" principle

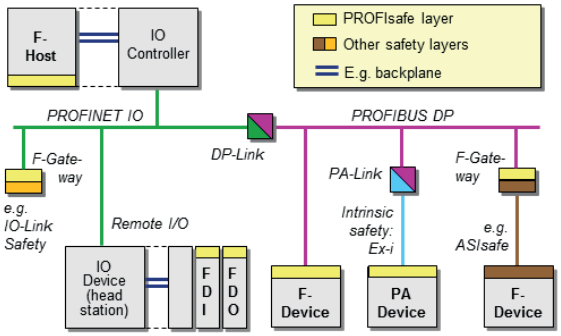

Figure 6: The complete safety communication paths

The individual safety parameters of a F-Device are technology-specific, e.g. drives with integrated safety, laser scanners, etc. Handling these iParameters via GSD would entail tremendous efforts and unnecessary dependencies. It therefore has to be possible for F-Device developers to integrate their individual configuration, parameterization and diagnostic tools (CPD tools) via appropriate interfaces into the engineering tools of system vendors. This facilitates the navigation and communication to the specific F-Device or F-Module.

For fast F-Device replacement in case of a failure, the system has to support "Save and Restore" functionality for individual safety parameters (iPar-Server) in a uniform way. Usually the F-Host or the controller that provides the basic bus start-up parameterization provides also this feature.

Supplementary documentation defines all aspects of deployment of PROFIsafe devices such as requirements for

- Installation
- Electrical safety
- Power supplies
- Electromagnetic compatibility
- Data security

Finally, strong support for developers of PROFIsafe in F-Devices or F-Modules is available in the form of PROFIsafe development kits, competence centers and test centers.

In its current version, PROFIsafe meets all of these requirements. The final concept is still straightforward and easy to understand.

Before we learn more about PROFIsafe in detail let's take a look at some preconditions and constraints.

3. "Black Channel"

Even though PROFIsafe uses the "Black Channel" principle, there are some basic features of PROFIBUS and PROFINET that were considered for its design.

3.1. Basic features

One such feature is the cyclic communication between a bus controller and its associated field devices (send and receive response principle). This polling operation will immediately detect any failed device. PROFIsafe adopted this principle.

The other feature is the 1:1 communication relationship between a bus controller and its associated field devices. PROFIsafe also adopts this principle to ensure the authenticity of messages.

3.2. Network components

A "Black Channel" may comprise several types of transparent network components such as switches, routers, links, and wireless transmission channels. For PROFIsafe, minor constraints exist in order to meet the SIL3 requirements.

Any kind of switch is permitted but only 100 can be connected in a row. The Codename space within a PROFIsafe island must be unique. Connected islands with the same Codename space must be separated by multiport routers. There are no restrictions for links such as from PROFINET to PROFIBUS and from there to the intrinsic safety version MBP-IS (figure 6).

3.3. Wireless

Wireless transmission is permitted as long as sufficient availability (no nuisance trips) and security can be guaranteed.

PROFIsafe specifies certain security requirements for wireless transmission and for wired networks that are connected to industrial Ethernet backbones or the Internet (open networks).

3.4. Data types

In general, fieldbus communication uses different data types for information transfer (see literature box on page 11). In order to reduce complexity, PROFIsafe offers a reasonable subset.

3.5. Selective tripping

PI's document "Remote IO for Factory Automation (RIO for FA)" specifies so-called qualifier bits associated to process values to indicate validity. This allows individual user reaction per process value. PROFIsafe offers an additional configurable prevention from automatic machine start.

4. PROFIsafe – the solution

It is the objective of safety communication between two partners to deliver:

- updated and correct data (data integrity),
- to the intended destination (authenticity),
- just-in-time (timeliness).

Various errors may occur when messages are transferred in complex network topologies, whether due to hardware failures, extraordinary electromagnetic interference, or other influences. A message can be lost, occur repeatedly, be inserted from somewhere else, appear delayed or in an incorrect sequence, and/or show corrupted data. In the case of safety communications, there may also be incorrect addressing: a message erroneously appears at a wrong F-Device and pretends to be a correct safety message. Different transmission rates may additionally cause bus component storage effects to occur. Out of the numerous remedies known from literature, PROFIsafe focuses on those presented in the matrix shown in figure 7.

Measure: / Error:	Monitoring Number (sign of life)	Time-out (with receipt)	Codename (for sender and receiver)	Data Consistency Check (CRC)
Data corruption				X
Unintended repetition		X		
Incorrect sequence	X			
Loss	X	X		
Unacceptable delay		X		
Insertion	X		X	
Masquerade (standard message mimics failsafe)				X
Incorrect adressing	X		X	
Out-of-sequence	X			
Loopback of messages	X			

Figure 7: Error types and safety measures

4.1. Safety measures

These safety measures include:

- The numbering of the PROFIsafe messages (sequence error detection used for "timeliness")
- A time expectation with acknowledgment (timeout error detection used for "timeliness")
- A Codename between sender and receiver ("authentication")
- Data integrity checks (CRC = cyclic redundancy check)

Using the Monitoring Number, a receiver can see whether or not it received the messages within the correct sequence. When it returns a message with the Monitoring Number only as an acknowledgment to the sender, the sender, too, will be assured. Basically, a simple "toggle bit" would have proven sufficient. However, due to the storage buffers in some bus components, e.g. switches, a 32-bit Monitoring Number was selected for PROFIsafe.

As safety systems are real-time systems, process signals must not only be delivered correctly, but also in time. In case of timeliness errors, the safety system will initiate a safe reaction, e.g. safely stop the movement of a drive. For this purpose, F-Devices utilize a watchdog timer that is restarted whenever a new PROFIsafe message with a new subsequent Monitoring Number arrives.

The 1:1 relationship between the F-Host and a F-Device facilitates the detection of misdirected message frames. Sender and receiver must simply have identification (Codename) that is unique in the network, and can be used for verifying the authenticity of a PROFIsafe message. PROFIsafe's Codename is called "F-Address".

A cyclic redundancy check (CRC) plays a key role in detecting corrupted data bits. The necessary probabilistic examination makes use of the definitions within the IEC 61508 that considers the probability of dangerous failures of entire safety functions. PROFIsafe follows this approach (figure 8).

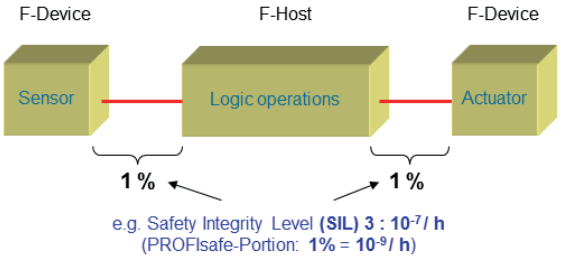

Figure 8: Safety function and SIL

According to IEC 61508, a safety circuit includes all sensors, actuators, transfer elements and logic processes that are involved in a safety function. IEC 61508 defines overall values for the probability of failures for different safety integrity levels.

For example, for SIL3 this is 10^{-7}/h. PROFIsafe uses a carefully selected 32-bit CRC generator polynomial, which ensures a probability of dangerous failures per hour of less than 10^{-9}/h. This value is guaranteed, independent of the "Black Channel" in use. Thus, even in SIL3 applications, less than 1% of the overall budget of 10^{-7}/h per safety function is consumed by PROFIsafe, leaving 99% of the budget for failures in sensors, actuators, or logic operations.

4.2. PROFIsafe formats

A PROFIsafe message that is exchanged between F-Host and its F-Device is carried within the payload of a standard PROFIBUS or PROFINET message. In case of a modular F-Device with several F-Modules, the payload consists of several PROFIsafe messages. Figure 9 shows the format of a safety protocol data unit (SPDU).

F-Input/Output data	Status / Control Byte	CRC signature
		across F-Parameter, F-I/O data, Status/Control Byte, Monitoring Number
1 to 12/13 (max. 123) bytes	1 byte	4 bytes

Figure 9: PROFIsafe SPDU format

The data unit consists of three fields. The first field contains the F-Input or F-Output data using the already-mentioned subset of data types. These data structures of a particular F-Device usually are defined via its associated GSD (General Station Description) file. Normally, factory automation and process automation place different requirements upon a safety system. One deals with short ("bit") signals that must be processed at a very high speed, the other involves longer ("floating point") process values that may take a little more time. PROFIsafe recommends using 1 up to 12/13 bytes F-Input/Output data for factory automation applications since all F-Hosts are obliged to support at least this data length. However, the measures of PROFIsafe (CRC signature) are laid-out such that data lengths up to a maximum of 123 bytes can be supported.

The second field consists of a Control Byte if the SPDU was sent by the F-Host or a Status Byte if it was sent by the F-Device. This information helps synchronizing the sender and receiver of PROFIsafe SPDUs.

The third field of a PROFIsafe SPDU is a 32 bit CRC signature.

The Monitoring Number is not transmitted within a PROFIsafe SPDU. Both sender and receiver use their own Monitoring Number generators that are synchronized via the Control Byte and Status Byte. Correct synchronization is monitored through the inclusion of the Monitoring Number values into the CRC signature calculation. The generators are based on an efficient pseudorandom number generator. Every connection uses a different seed for the generator, derived from its respective Codename ("F-Address").

4.3. PROFIsafe services

Sender and receiver of PROFIsafe SPDUs are located in layers above the "Black Channel" communication layers (figure 5). Usually, these PROFIsafe layers are realized in software ("drivers"). Their central functionality is a state machine controlling the regular cyclic processing of PROFIsafe messages and the exceptions such as start-up, power-on/off, CRC error handling, etc. Figure 10 shows how the PROFIsafe layers interact with the technology part in F-Devices and with the user program in F-Hosts.

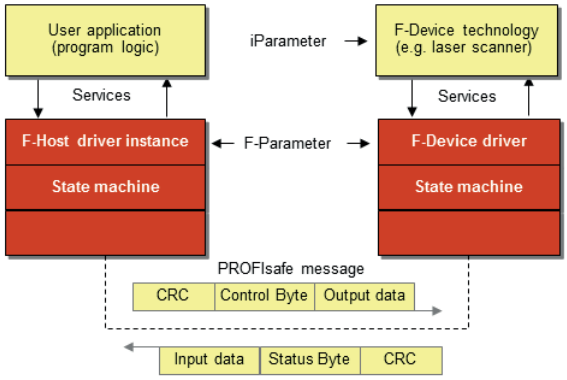

Figure 10: PROFIsafe layer structure in F-Host and F-Device

F-Host services

The main services provide exchange of F-Output and F-Input data. During start-up, or in case of errors, the actual process values are replaced by default fail-safe values (FV). These fail-safe values shall be all "0" to force the receiver into a safe state (e.g. de-energize).

For F-Devices where de-energize is not the only possible safe state such as with burner ventilators, PROFIsafe provides additional services via a flag "activate_FV" in the Control Byte. In return, a F-Device can inform the user program that it has activated its safe state via a flag "FV_activated" in the Status Byte.

PROFIsafe communication errors cause the F-Host driver to switch into a safe state. A safety function is usually not allowed to automatically switch from a safe state to normal operation without human interaction. To inform the user program that an operator intervention and acknowledgment is requested, PROFIsafe provides an additional service "OA_Req". PROFIsafe informs the F-Device about a pending request such that the F-Device can indicate it via a LED (optional). The operator acknowledgment can be passed over from the user program to the F-Host driver via a corresponding service "OA_C".

The technology-specific parameters of a F-Device are called iParameters. In case a F-Device needs different iParameters at runtime, another set of services is available. The service "iPar_EN" allows the user program to switch the F-Device into a mode during which it will accept new iParameters. The companion service "iPar_OK" indicates to the user program the readiness to resume normal safety operation.

F-Device services

The PROFIsafe services for F-Device technology include the corresponding exchange of F-Output and F-Input data, the extra possibility to activate and report fail-safe values, the indicators for the iParameter handling and for the already mentioned operator request.

Additionally, the F-Device technology is able to report F-Device faults to the F-Host driver via the flag "Device_Fault" in the Status Byte.

The duration of the demand of a F-Device for a safety reaction shall be long enough to be transmitted by the PROFIsafe communication (at least two subsequent Monitoring Numbers). A special service informs the technology about new Monitoring Numbers in order to facilitate the realization of this requirement.

Diagnostic information from the PROFIsafe layer may be passed over to the technology part via a special service.

Last but not least the technology is able to pass over the F-Parameters to the PROFIsafe layer. The F-Device receives these F-Parameters together with all the other parameters during startup. What is the purpose of these F-Parameters?

F-Parameter

The F-Parameters provide the PROFIsafe layer information to adjust its behavior to particular customer needs and to double-check the correctness of assignments. The most important F-Parameters are:

- F_S/D_Address (short: "F-Address")
- F_WD_Time
- F_SIL
- F_iPar_CRC
- F_Par_CRC

The "F_Address" is a unique connection identification for F-Devices/F-Modules within one PROFIsafe island and corresponds to the Codename. The F-Device technology compares this "F-Address" with the locally assigned value of a micro switch or otherwise entered information to ensure the authenticity of the connection.

The F_WD_Time specifies a number of milliseconds for a watchdog timer. This timer monitors the reception of the next valid PROFIsafe SPDU.

F_SIL indicates the SIL expected by the user for the particular F_Device. It is compared with the locally stored manufacturer information.

F_iPar_CRC is a signature across all the iParameters within the technology of the F-Device.

Finally, the F_Par_CRC is a signature across all the F-Parameters. It is used to ensure correct delivery of the F-Parameters.

5. How to implement?

First of all, it should be made sure, that all the necessary and helpful literature for the work that is available from PI has been obtained (see Literature box on Page 11). Use the denoted or a later version. A previous version V1.30 of the PROFIsafe specification has been withdrawn.

Next, it is recommended to study at least the basic safety standard IEC 61508 or get some consultancy on what needs to be established in your development processes and in your organization to achieve the necessary safety for your device. As a general rule, it is not possible to turn a standard device into a safety device just by implementing the PROFIsafe protocol. This is due to the fact that PROFIsafe protects against transmission errors on the Black Channel, but not against errors occurring within the F-Devices itself. The architecture of the F-Device safety technology together with the protocol and the manner in which both are implemented define the final SIL of the device.

5.1. Safety classes

Even though PROFIsafe is suitable for safety functions up to SIL3, it may not be necessary to design and develop the F-Device also for SIL3. The required safety class depends on the final customer application and on how the safety functions are defined. It may be possible through redundancy or other measures to achieve higher safety integrity levels with F-Devices of an even lower safety class (see Chapter 9.6. "PA-Devices").

5.2. F-Device

In addition to the possibility of implementing the PROFIsafe specification from scratch, development kits are available on the market. See the product finder on the PI website for further information. The advantage of using a development kit is obvious: pre-certified driver software, additional valuable information and tools, and support.

For the PROFIBUS and PROFINET interface, you can use any of the available ASICs and layer stacks and adapt the PROFIsafe driver software.

Securing the GSD

For every device on PROFIBUS or PROFINET, a General Station Description (GSD file) is necessary. After defining the common part of the GSD for a F-Device, the coding of the F-Parameters is necessary. This section of the F-Parameters must be protected by a special CRC signature "F_ParamDescCRC" against data corruption on storage media. A configuration tool can check the data integrity of the F-Parameter description section utilizing this special signature, which is also a part of the GSD file.

Securing configurations

The GSD file also contains descriptions for the F-Input and/or F-Output data structures. In order to secure this part of the GSD file, another CRC signature "F_IO_StructureDescCRC" is used.

iParameter

According to the many different safety device technologies there is a huge variety of individual safety parameters (iParameter).

The amount of iParameters ranges from a few bytes for a F-Module up to several tens of kBytes for a laser scanner. For most of the safety devices, special parameterization and diagnostic software tools (CPD-Tool) already exist: therefore it does not make sense to handle iParameters via the GSD. PROFIsafe therefore recommends using a new mechanism, the so-called Universal-Parameter-Server (iPar-Server). It is the responsibility of F-Host manufacturers to provide this capability, whether it is realized within

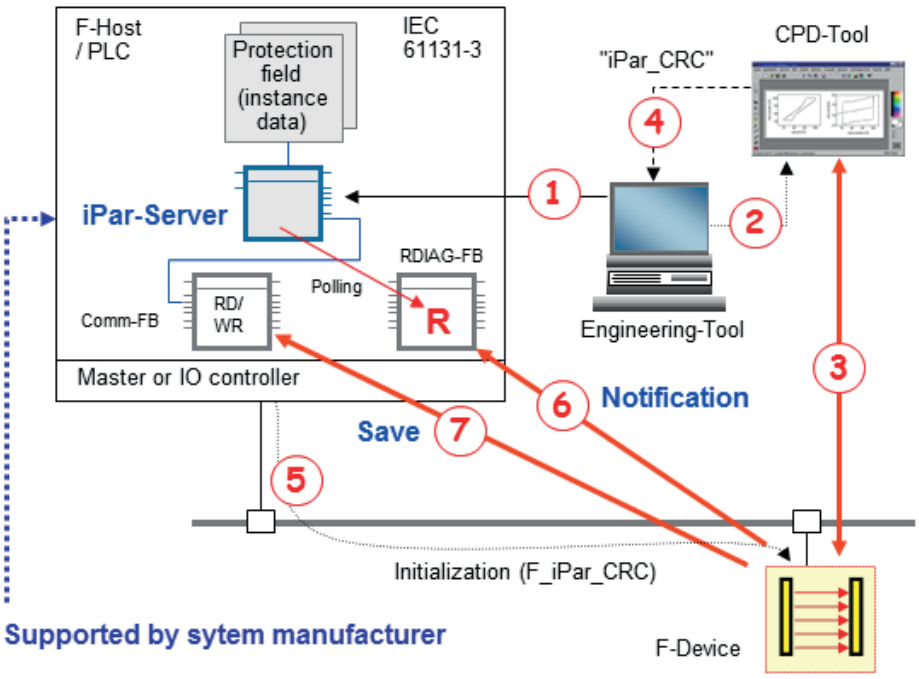

Figure 11: The iPar-Server concept

the non-safety part of F-Host acting as the fieldbus parameterization master or within a controlled subsystem such as a non-safety PLC or an industrial computer on the same network.

Figure 11 demonstrates the principal steps of the iPar-Server mechanism by an example. Together with the network configuration and F-Parameterization of a F-Device, an associated iPar-Server function is instantiated (1). The F-Device is able to switch into the data exchange mode while using a safe state (FV). An associated CPD tool can be launched via an appropriate interface (2) such as TCI (Tool Calling Interface) or FDT (Field Device Tool) from the engineering tool, propagating at least the node address of the configured device. Parameterization, commissioning, testing, etc., can be executed with the help of the CPD tool (3). After finalization, the iPar_CRC signature is calculated and displayed in hexadecimal form for (at least) copying and pasting of this value into the "F_iPar_CRC" entry field of the configuration part of the engineering tool (4). A restart of the F-Device is necessary to transfer the "F_iPar_CRC" parameter into the F-Device (5). After final verification and release, the F-Device is enabled to initiate an upload notification (6) to its iPar-Server instance. It thereby utilizes the standard diagnosis mechanism. The iPar-Server polls the diagnosis information (e.g. RDIAG FB) to interpret the request (R) and to establish the upload process (7), storing the iParameters as instance data within the iPar-Server host using acyclic services (Read Record).

After the replacement of a defective F-Device, the new F-Device receives its F-Parameters, including the "F_iPar_CRC", at start-up. As iParameters are normally missing in a replacement or a non-retentive F-Device, it recognizes a difference between the "F_iPar_CRC" and its stored iParameters and initiates a download notification (6) to its iPar-Server instance, again using the standard diagnosis mechanism. The iPar-Server polls the diagnosis information to interpret the request (R) and to establish the download process (Write Record). Through this transfer the F-Device is enabled to provide the original functionality without further engineering or CPD tools.

PROFIdrive

The IEC 61800-5-2 defines some safety features for drives with integrated safety. These features comprise a group of stopping functions:

- Safe torque off (de-energize)
- Safe stop 1
- Safe stop 2
- Safe operating stop

And a group of other safety subfunctions:

- Safely limited acceleration
- Safely limited speed
- Safely limited torque / force
- Safely limited (absolute) position
- Safely limited increment
- Safe direction
- Safely limited motor temperature

Figure 12 illustrates how electro mechanics are replaced by electronic safety stops and monitoring subfunctions. One major objective is to mainly monitor the operations of the drive control and to de-energize only in case of failures. The working group PROFIdrive within PI is specifying parts of these subfunctions in a special amendment to their PROFIdrive specification (see Literature box).

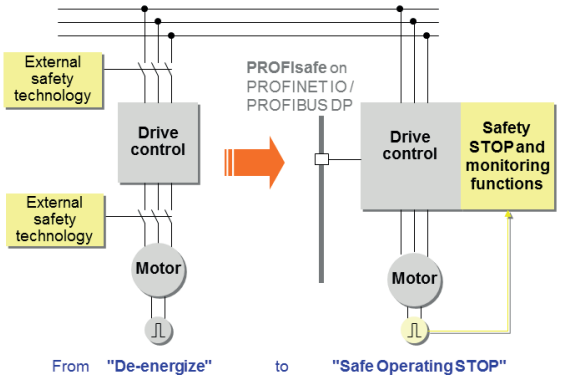

Figure 12: Drives with integrated safety STOP and monitoring subfunctions

PA Devices

F-Devices for process automation follow the sector standard IEC 61511, which takes into account the particular aspect of "proven-in-use". Under certain conditions, a PA-Device may achieve a better SIL if it is considered to be proven-in-use. PA Devices usually follow the design models of IEC 61804. The Electronic Device Description (EDD) plays an important role here. Therefore, the PI Working Group "PA Devices" also specified, within a separate amendment to their PA Device specification, how to use the PROFIsafe platform for their devices and parameterization methodologies (see Literature box).

I&M functions

Since 2005, I&M functions are mandatory for all PROFIBUS and PROFINET devices providing acyclic services. I&M stands for Identification and Maintenance and allows retrieving information about the device's manufacturer code, its catalog and serial number, and its hardware and software

versions in a standardized manner. Via the manufacturer code and additional information on the PI website, the user can be directed to the most current product information on the manufacturer's website. See the Profile Guideline (Literature box).

Diagnosis

One of the major advantages of PROFIBUS and PROFINET is the possibility for devices to report diagnostics information to the operator in exceptional situations such as failures or errors. Good diagnostics information helps in reducing down times of facilities and thus costs. The concepts not only cover how to code the information but also how to provide foreign language support and how to provide HELP information on what to do in a particular situation. See the corresponding Profile Guideline (Literature box).

Literature box

- PROFIsafe Policy V1.5; Order No. 2.282
- PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, V2.6.1; Order No. 3.192
- PROFIsafe – Environmental Requirements, V2.6; Order No. 2.232
- PROFIsafe – Test Specification for F-Slaves, F-Devices, and F-Hosts, V2.2; Order No. 2.242
- PROFIsafe for PA-Devices, V1.0.1; Order No. 3.042
- PROFIdrive on PROFIsafe, V3.00.4; Order No. 3.272
- Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD, V5.1; Order No. 2.122
- GSDML Specification for PROFINET IO, V2.3.2; Order No. 2.352
- Profile Guideline, Part 1: Identification & Maintenance Functions, V2.0; Order No. 3.502
- Profile Guideline, Part 2: Data Types, Programming Languages, and Platforms, V1.0; Order No. 3.512
- Profile Guideline, Part 3: Diagnosis, Alarms and Time Stamping, V1.0; Order No. 3.522
- Profile Guideline, Part 4: Universal Parameter Server, V1.0.1; Order No. 3.532
- Diagnosis for PROFINET IO, V1.1; Order No. 7.142
- Rapid way to PROFIBUS DP; Order No. 4.072
- Industrial Communications with PROFINET; Order No. 4.182

5.3. F-Host

Depending on the strategy of system manufacturers, different kinds of architectures for F-Hosts with PROFIsafe communication are possible: stand-alone F-CPUs or integrated but logically separated safety processing within standard CPUs.

Possible structures

Safety processing itself can be realized in many different ways also: for example via hardware redundancy and discrepancy checking or via "software redundancy" or via "safeguarding" or by using already existing diverse hardware platforms. Development kits are available.

Conformance classes

In order to ensure that all F-Devices will be supported by all the PROFIsafe F-Hosts on the market, PROFIsafe specifies conformance classes for F-Hosts. PROFIsafe F-Hosts shall meet the requirements of these conformance classes as a precondition for PI certification (figure 13).

6. Conformity & certification

Several products of different types from various vendors communicate within a PROFIsafe island. The products must be implemented conforming to the PROFIsafe specification to ensure that this communication works correctly. Usually the conformance is documented through a certificate from the PI Certification Office based on the test report of one of the accredited PI test laboratories.

6.1. The PROFIsafe tests

The PROFIsafe protocol mechanisms are based on finite state machines. It was possible to mathematically prove that PROFIsafe works correctly, even in cases where more than two independent errors or failures occur. This was achieved by systematically generating all possible cases for "test-to-pass" and "test-to-fail" situations. They have been extracted as test cases for a fully automated PROFIsafe layer tester, which is used to check the PROFIsafe conformance of F-Devices and F-Hosts. It is part of a three-step-procedure within the overall safety certification process according to IEC 61508 by assessment bodies (figure 13).

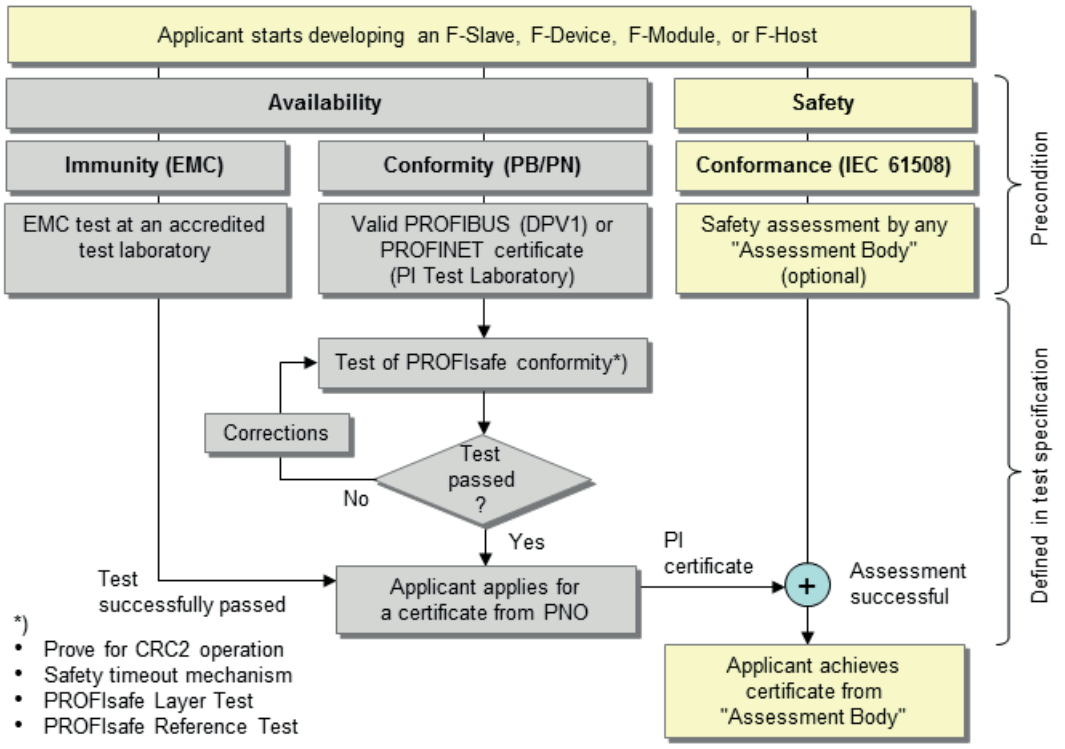

Figure 13: Test and certification procedures

6.2. Safety assessment

It is important to note that the PI Test Laboratories perform the approved PROFIsafe layer tests on behalf of assessment bodies such as, for example:

- TÜV (worldwide)
- IFA (Germany)
- SP (Sweden)
- SUVA (Switzerland)
- HSE (United Kingdom)
- FM, UL (USA)

These are the only ones to be responsible for the safety assessments according to IEC 61508.

The mandatory safety manual of each F-Device shall provide information about the SIL_{CL} (claim limit), Cat, PL, and the PFH_d (probability of dangerous failure per hour).

PROFIsafe provides a specification for test and certification. Currently, four PI test laboratories are accredited for PROFIsafe testing worldwide (see www.profibus.com/test-labs).

7. PROFIsafe deployment

The guideline "PROFIsafe - Environmental Guidelines" (see Literature box) deals with all environmental aspects of the PROFIsafe communication protocols. It answers questions such as:

- Do I need to protect my F-Device against very high voltages coming across the PROFIBUS /PROFINET cable from an unknown other source?
- Is it safe to use the same 24V power supply that I use for the standard devices in my network?
- How do I test my F-Devices for the "increased immunity" that is required by IEC 61508?
- What are the installation rules?
- What are the security requirements?

The following sections quickly summarize this guideline.

7.1. Electrical safety

The fieldbus standards IEC 61158 and IEC 61784-1 / -2 require for all devices within the network "to comply with the legal requirements of that country where they are deployed" (for example, as indicated by the CE mark). The measures for protection against electrical shocks (i.e. electrical

safety) within industrial applications shall be based on the IEC 61010 series depending on device type specified therein. These measures are called PELV (Protected Extra Low Voltage) and limit the permitted voltages in case of one failure to ranges that are not dangerous for humans.

Due to this normally legal requirement, it is possible to limit the protection effort within a F-Device or a F-Host.

7.2. Power supplies

It is possible to use the same 24V power supplies for standard and F-Devices / F-Hosts. In both cases the power supplies shall provide PELV due to legal requirements.

7.3. Increased immunity

For each safety application, the corresponding SRS (Safety Requirements Specification) shall define electromagnetic immunity limits (see IEC 61000-1-1) which are required to achieve electromagnetic compatibility. These limits should be derived taking into account both the electromagnetic phenomena (see IEC 61000-2-5) and the required safety integrity levels.

For general industrial applications the generic IEC 61000-6-7 or IEC 61326-3-1 respectively defines immunity requirements for equipment performing or intended to perform safety related functions.

Product standards such as IEC 61496-1 (e.g. laser scanners) may define increased immunity requirements for some phenomena.

The environmental conditions within the process industries can be different from those of general industrial environments. Thus the specific requirements and performance criteria described in IEC 61326-3-2 can be used for PA Devices.

For PROFIsafe a particular EMC test bed is defined.

7.4. High availability

The objective of *safety* is to maintain *safety functions* in order to prevent personnel from being injured, e.g. by de-energizing hazardous elements. A characteristic measure for a safety function is SIL (Safety Integrity Level). It describes the safety function's probability of a dangerous failure per hour, e.g. 10^{-7}/h for SIL3. In contrast, the objective of *high availability (fault tolerance)* is to maintain the automation even in case of failures. A characteristic measure for high availability is the ratio of uptime to the total operation time, for example 99.99%. Redundancy is a means that can be used together with others to achieve this objective.

PROFIsafe is designed such that it can be deployed with or without redundancy for fault tolerance. Figure 14 shows possible combinations.

7.5. Installation guidelines

It is the goal of PROFIsafe to integrate safety communication into the standard PROFIBUS and PROFINET networks with minimal impact on the existing installation guidelines. In order to achieve reliable performance and to fulfill legal requirements, following the PROFIsafe specifications and guidelines is highly recommended. Some major issues to be considered are mentioned below.

	PROFIsafe	Redundancy	PROFIsafe and Redundancy
Application	Factory and process automation: Presses, robots, level switches, shutdown valves, as well as burner control and cable cars	Process automation; Tranportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels	Process automation; Transportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels
High Availability	-	No downtimes at best (fault tolerance)	No downtimes at best (fault tolerance)
Safety	No dangerous failures (required by law or insurances)	Redundancy by itself does not provide safety	No dangerous failures (required by law or insurances)

Figure 14: Safety and High Availability (Fault Tolerance)

Preconditions

All standard and F-Devices on the network shall be electrically safe as outlined in Chapter 7.1.

All F-Devices shall be certified according to IEC 61508 and, in case of process automation according to IEC 61511. They shall be tested and approved for PROFIsafe conformity by PI Test Laboratories.

All other standard devices within a PROFIsafe network shall prove conformity to PROFIBUS or PROFINET via a PI certificate or equivalent evidence.

Constraints

For PROFIBUS DP, no spurs or branch lines are permitted.

For PROFINET IO, the following rules apply:

- Less than 100 switches in a row
- Only one F-Host per submodule
- All network components must be suitable for industrial environment (e.g. IEC 61131-2)
- Router required to separate PROFIsafe islands (characterized by unique F-Addresses/ Codenames)

Cabling

PROFIBUS and PROFINET both specify the use of shielded cables and double-sided connection of the shield with the connector housing for best electromagnetic immunity. As a consequence, equipotential bonding is usually required. If this is not possible, fiber optics may be used.

At the risk of a high frequency of spurious trips, machine designers may use cables without shielding in case of specified electromagnetic compatibility with minor burst and surge interferences.

Availability

Even with shielded cables unacceptable signal noise may be introduced onto the data lines of a device if, for example, the intermediate DC link of a frequency inverter is not filtering well enough. Other sources of unacceptable signal quality may be due to missing terminating resistors and the like. This is not a safety but an availability issue. Sufficient availability of the control functions is a precondition of safety. Safety functions on equipment with insufficient availability may cause nuisance trips and as a consequence may tempt production personnel to manipulate or even remove these safety functions.

PI companies provide many tools, procedures, and checklists to investigate the transmission quality of networks.

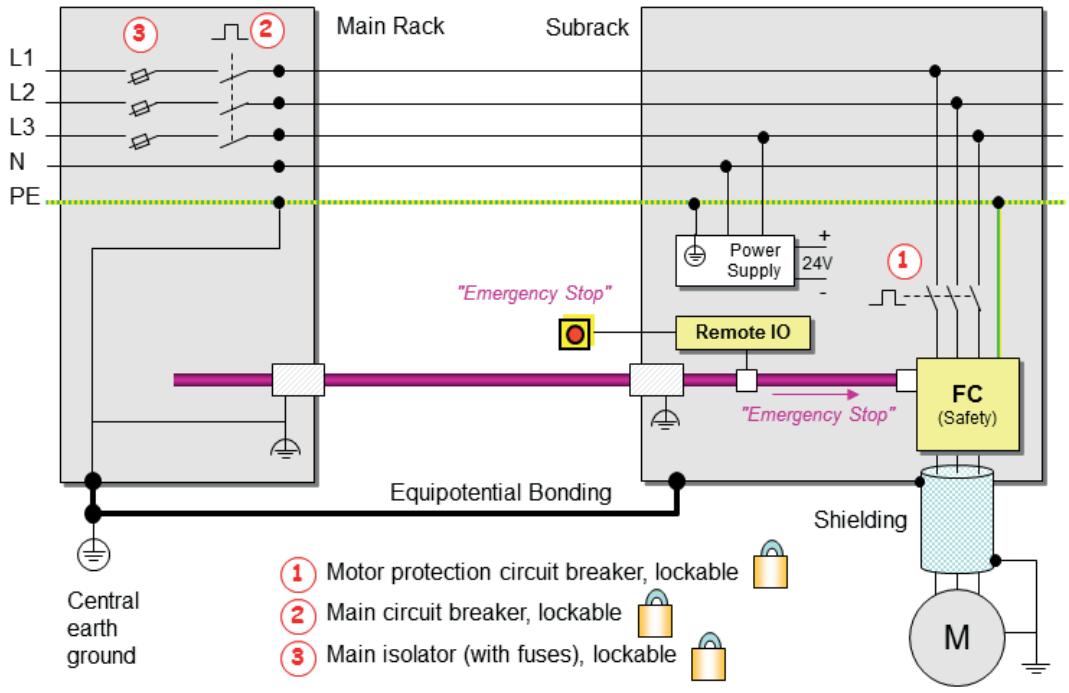

Figure 15: Emergency switching off concept (IEC 60204-1)

PROFIsafe has been the enabling technology for many safety devices, especially drives with integrated safety. Nowadays, drives can provide safe states without de-energizing the motor. For example the safety subfunction "SOS" (safe operating stop) holds the motor under closed loop control in a certain position. This new possibility requires a paradigm shift for the user. In earlier times, pushing an emergency stop button caused the power lines to be physically disconnected from the motor and, therefore, there was no electrical danger for a person exchanging the motor.

The new IEC 60204-1 provides concepts on how to protect against electrical shock (emergency switch-off) with lockable motor protection circuit breakers, main circuit breakers and main isolators with fuses. Figure 15 demonstrates these concepts. It also shows the recommended 5-wire power line connections (TN-S) with separated N and PE lines and the shielded cables between drives and motors. The IEC 60204-1 is a valuable source for many other safety issues complementing the PROFIsafe technology. The corresponding national standard NFPA 79 considers some deviations for the North American market (figure 3).

7.6. Wireless transmission

More and more applications such as Automated Guided Vehicles (AGV), rotating machines, gantry robots, and teach panels use wireless transmission in PROFIBUS and PROFINET networks. PI specifies details for WLAN and Bluetooth as well. PROFIsafe, with its error detection mechanism for bit error probabilities up to 10^{-2} is approved for all kinds of "Black Channels". However, the security issues below must be considered in addition.

7.7. Security

With PROFINET being based on Industrial Ethernet as an open network and particularly in the context of wireless transmission the issue of security has been raised.

PI is pushing the concept of building so-called security zones which can be considered to be closed networks (figure 16). The only possibility to cross open networks such as Industrial Ethernet Backbones from one security zone to another is via *Security Gates*. The *Security Gates* use generally accepted mechanisms such as VPN (Virtual Private Network) and Firewalls to protect themselves from intrusion. PROFIsafe networks always shall

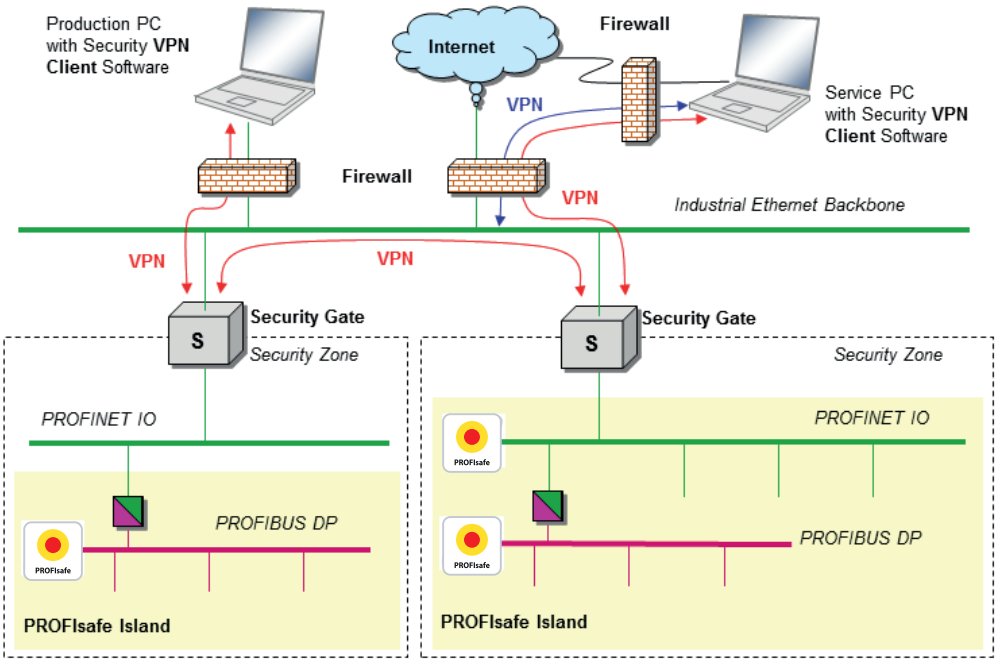

Figure 16: Security concepts for "closed" and "open" networks

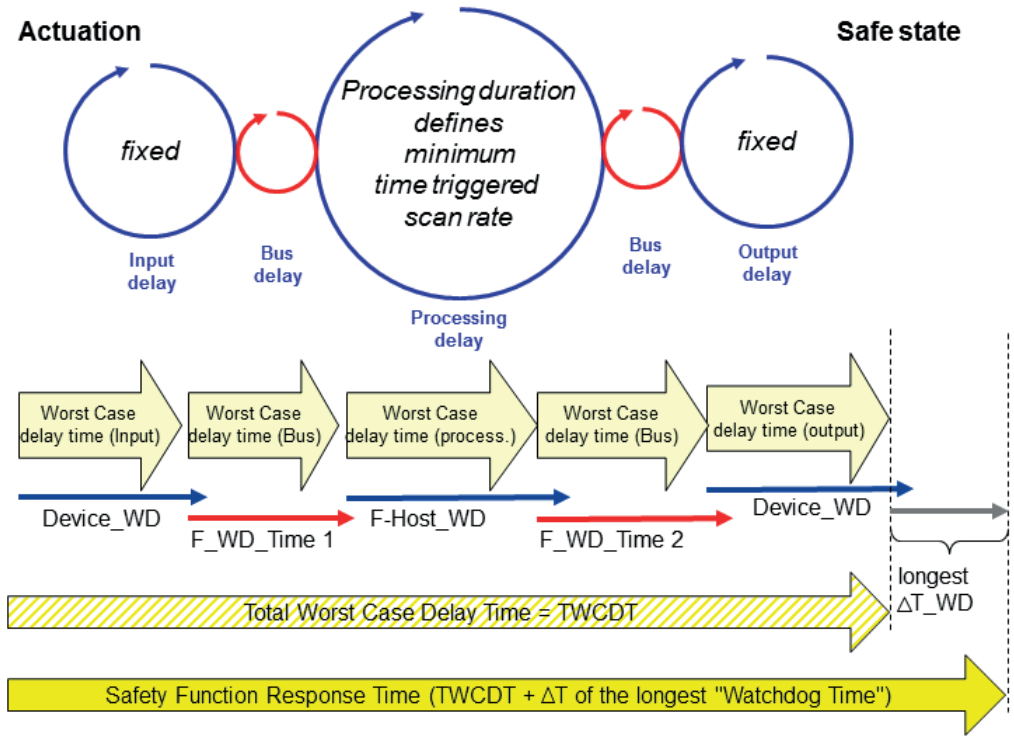

Figure 17: Safety Function Response Time (SFRT)

be located inside security zones and protected by *Security Gates*. If connections to open networks cannot be avoided, refer to PROFINET Security Guideline, V2.0; Order No. 7.002.

For wireless transmission, the IEEE 802.11 standard provides sufficient security measures for PROFIsafe networks. Only the Infrastructure Mode is permitted; the Adhoc Mode shall not be used. More details can be found in the PROFIsafe specification.

7.8. Response time

Usually the response times of normal control functions are fast enough for safety functions as well. However, some time-critical safety applications need safety function response times (SFRT) to be considered more thoroughly such as presses protected by light curtains. A machine designer has to know at what distance the light curtain must be mounted away from the hazardous press. It is common agreement that a hand moves at a maximum of 2 m/s. The minimum distance to be considered then is s = 2 m/s x SFRT if the resolution of the light curtain is high enough to detect a single finger (EN 999). Otherwise correction summands are needed.

The model in figure 17 is used to explain the calculation of the SFRT. The model consists of an input F-Device, a PROFIsafe bus transmission, signal processing in a F-Host, another PROFIsafe bus transmission, and an output F-Device, each with its own statistical cycle times. The maximum time for a safety signal to pass through this chain is called TWCDT (Total Worst Case Delay Time) considering that all parts require their particular maximum cycle times. In case of safety, the considerations go even further: The signal could be delayed even more if one of the parts just fails at that point in time. Thus, a delta time needs to be added for that particular part which represents the maximum difference between its watchdog time and its worst case delay time (there is no need to consider more than one failure at one time). Eventually, TWCDT plus this delta time comprise the SFRT.

Each and every F-Device shall provide information about its worst case delay time as required in the PROFIsafe specification in order for the engineering tools to estimate the SFRTs.

8. For integrators

8.1. Directives & standards

In many countries, the safety requirements for hazardous machineries are regulated by law. Within the EU this is the Machinery Directive 2006/42/EC. This directive contains a list of so-called harmonized standards. For a machine builder, there is presumption of conformity to the directives if the relevant standards are fulfilled.

Relevant standards in the context of PROFIsafe are, for example, IEC 62061, ISO 13849, and ISO 12100 (see Chapter 1.3. and figure 2).

8.2. Risk reduction strategy

It is always better to design a machine with inherent safety such that it avoids any hazards. In its first part, the ISO 12100 lists all kinds of possible hazards. In its second part, it shows an iterative strategy on how to reduce the risk of any automated equipment via a risk assessment. This risk assessment consists of a risk analysis and a risk evaluation:

- Specify the limits and the intended use of the machine
- Identify the hazards and the associated hazardous situations during the whole life cycle of the machine
- Estimate the risk for each identified hazard and hazardous situation
- Evaluate the risk and make decisions about the need for risk reduction

By using the "3-step-method"

- inherently safe design measures,
- safeguarding and possibly complementary protective measures,
- information for use about the residual risk,

the designer can eliminate the hazards or reduce the risk associated with the hazards by protective measures.

Safeguarding and complementary protective measures are the building up of safety functions such as a light curtain, the associated logic operation, and a circuit breaker to de-energize the motor.

8.3. Application of IEC 62061

Both IEC 62061 and ISO 13849 provide methods for dealing with safety functions. While IEC 62061 fits well to the PROFIsafe technology and programmable safety controllers (F-Hosts), the ISO 13849 fills the gap for hydraulic, pneumatic, electric, and mechanical components.

The IEC 62061 requires a safety plan for the whole life cycle of the machinery covering design strategies, personnel roles and responsibilities, commissioning, change and maintenance until dismantling.

ISO and IEC now are eager to harmonize and to improve the two approaches of IEC 62061 and ISO 13849 via the project "ISO/IEC 17305" (figure 2).

8.4. Risk evaluation

The functional safety standards offer similar concepts for the risk evaluation of safety functions, based on ISO 12100:

Risk = severity of harm and probability of occurrence of that harm

The probability of occurrence consists of the exposure of persons, the occurrence, and the possibility of avoidance.

8.5. SIL/PL/Cat determination

Both IEC 62061 and ISO 13849 provide calculated characteristics. One is the required SIL and the other the required PL and Category (see Chapter 1.3.). It is possible to transform one into the other. In the long run it can be expected that the difference will disappear for the user when the risk evaluation is performed in engineering tools via "questionnaires". It is expected that the new ISO/IEC 17305 will be helpful in this respect.

8.6. Safety function design

IEC 62061 defines so-called safety-related electrical control system (SRECS) for safety functions with subsystems for sensing, processing, and actuation. Subsystems may contain elements (e.g. switches).

The easiest way to design a safety function is to use certified or pre-evaluated F-Devices (sensors, actuators) and a certified F-Host connected via PROFIsafe.

8.7. Achieved SIL

The F-Devices provide the necessary information in their safety manual to determine the achieved SIL of a particular safety function. In the first step, the least SIL_{CL} (claim limit) of all the safety devices (F-Devices, F-Host) is selected. This determines the maximum achievable SIL of the entire safety function. In some cases system manufacturers may offer system support to upgrade to a higher SIL via redundancy of F-Devices and corresponding system software.

In the second step, the PFH_d values are added and the result is checked against the permitted value ranges for a particular SIL.

The least SIL value from these two steps determines the achievable SIL.

In the following sections, you will see how you can combine F-Modules within remote I/O with classic electromechanical safety devices such as emergency stop buttons, door switches, etc. as shown in figure 4.

8.8. Electro mechanics

IEC 62061 provides four predetermined architectures A, B, C, and D for subsystems to connect classic safety devices. Formulas to calculate failure probabilities are provided for these circuits. With the help of B_{10} values for the mechanical switches, the estimated number of switch cycles, the diagnostic coverage, and a common cause factor, the necessary probability of dangerous failures can be calculated with the formulas and added to determine the overall SIL.

8.9. Non-electrical parts

The ISO 13849-1 defines so-called SRP/CS (Safety-Related Parts of Control Systems) also for hydraulic, pneumatic, electric, and mechanic components. A PL and a PFH_d value can be determined for such a component with the help of this standard and transformed into the SIL determination for the safety function according to IEC 62061.

8.10. Validation

IEC 62061 requires a validation plan to be part of the overall safety plan. According to this plan the machinery shall be tested, checked, and documented.

9. F-Device families

PROFIsafe as an enabling technology has been initiating new possibilities for standard and safety devices. This chapter is to provide a brief overview of some important F-Devices and typical applications.

9.1. Remote I/O

Standard remote I/O are now able to incorporate safety modules without changing the head stations. F-Modules such as digital input/output, analog input/output, power modules, motor starters, and frequency converters with integrated safety are available. The F-Modules can be grouped together and allow shut-down in groups. Emergency stop buttons need very costly yearly inspections as each button has to be tested individually. The new technology allows for easy collection of all actuations over the year. This way only the remaining unactuated buttons have to be tested, thus saving costs.

9.2. Optical sensors

Optical safety sensors such as light curtains and laser scanners are standardized within IEC 61496. Optical sensors are ideally suited to protect entry/exit portals in a flexible manner. The example in figure 18 also shows how PROFIsafe complements the safety features of laser scanners and drives with integrated safety. See details below.

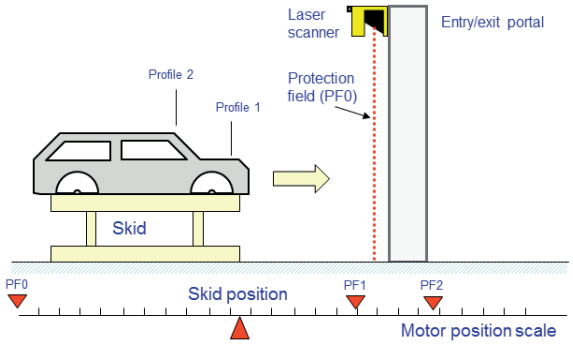

Figure 18: Software "muting sensors" for laser-scanners

9.3. Drives

The safety subfunctions of drives are standardized in IEC 61800-5-2. These safety subfunctions usually require a safe position indicator. The value is available to the user via PROFIsafe and can replace physical "end-of-travel"-switches or physical "muting"-sensors. As shown in figure 18 the motor position affects the protection fields of laser

scanners according to the profiles of car bodies at entry/exit portals of a manufacturing cell.

Section 5.2 lists many more possible safety subfunctions which will cause revolutionary applications to occur in the near future.

9.4. Robots

Safety features for robots can be found in ISO 10218. The new safety subfunctions for drives foster robots to integrate those features and provide new functionality such as "collaborative robots", where persons work hand-in-hand with robots.

9.5. F-Gateways

For PROFIsafe F-Gateways to AS-i Safety-at-work (ASIsafe) exist. These devices combine the advantages of both worlds. While ASIsafe can easily collect the signals from many emergency stop buttons connected in series, PROFIsafe is easily able to deal with sophisticated F-Devices such as drives with integrated safety.

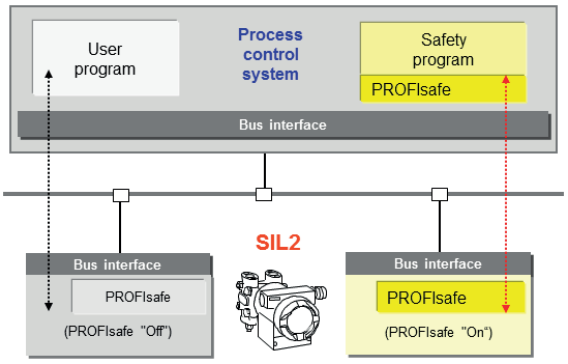

Figure 19: PROFIsafe and NE97 for PA-Devices

9.6. PA-Devices

It was previously mentioned that safety for process automation follows its own sector standard IEC 61511. NAMUR, as standards body for chemical and pharmaceutial industries publishes the companion standard NE97 specifying how safety communication can be used with safety field devices. A "proven-in-use" PA Device, equipped with a PROFIBUS MBP-IS interface, accommodates a PROFIsafe driver that can be configured "Off" or "On". In "OFF"-mode it represents a standard PA Device, in the "ON"-mode a F-Device (figure 19).

Alternatively, NAMUR initiated another companion standard, the VDI 2180, which facilitates the development of safety-related PA Devices.

Currently most of the PROFIsafe applications in process automation deploy remote I/O with F-Modules for 4-20mA or HART communication. Figure 20 demonstrates the two possibilities for using PROFIsafe with "proven-in-use" PA Devices. This is a good compromise even though it suffers from the lack of the direct fieldbus advantages such as wide range measurements, parameterization and sophisticated diagnosis.

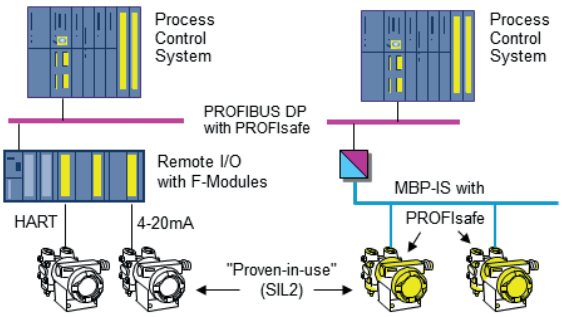

Figure 20: Two possibilities for PROFIsafe and PA-Devices

Level switches

Level switches for tanks benefit much from the PROFIsafe technology. PROFIBUS PA with its MBP-IS and RS485-IS explosion-proof transmission technologies fit well into the requirements of these F-Devices. PROFIsafe provides the safety transmission of the shut-down signals while the standard "black channel" informs the user about the status of the sensors.

ESD valves

Similar improvements can be achieved for ESD (Electronic Shut-Down) valves. The main objective here is to periodically test the valve function through "partial valve strokes" and trend monitoring of the end position and of the time elapsed to reach this position. This can be done automatically via F-Hosts and allows predictive maintenance whenever it is convenient for the user. The RS485-IS communication together with barriers allows fast shut-down even within an Ex-i environment.

Pressure transmitter

Safe pressure transmitters combine the function of measuring the tank filling and of protection against overflow ("level switch") via comparison with a setpoint value.

Gas and fire sensors

These sensors are in service on unmanned oil platforms for example. Additional position information makes it possible to automatically batten down the relevant hatches.

10. User benefits

In the meantime, more than 5 million PROFIsafe nodes have been installed.

More than 50 million PROFIBUS devices and more than 10 million PROFINET devices have now been installed.

Therefore, the top priority for development has always been and will continue to be ensuring that the system remains fully compatible with the devices that are already in the field.

Thanks to the autonomous functional safety communication protocol of PROFIsafe and its "Black Channel" approach, it is even possible to cross-over from PROFINET to PROFIBUS without any major difficulties. The identical PROFIsafe driver software can be used in both PROFINET and PROFIBUS devices.

Introduction of PROFIsafe has been causing a three-step quantum leap:

- From safety-related relay logic to safe programmable logic
- From multi-wire to functional safe serial communication
- From isolated to cooperating safety-related devices

The following statements perfectly sum up the benefits from several points of view.

10.1. Integrators and end users

- Same cost savings as with the introduction of standard PROFIBUS: reduced wiring, flexible configurations, parameterization, and diagnosis
- Easy and cost-efficient system design with a broad product spectrum from all types of manufacturers
- In general no special installation restrictions
- Highly innovative safety applications through easy communication between sophisticated F-Devices
- High flexibility in the replacement of existing relay technology as well as expansion and retrofit of existing installations
- Integrated technology for both factory and process automation
- Training, documentation, and maintenance required for only one bus technology
- Programming of standard and safety-related applications with only one tool and certified function blocks
- Easy documentation of safety-related configurations and logics
- Cost saving system acceptance due to certified devices
- International acceptance through IEC 61508-conforming technology.
- Positive assessments by IFA and TÜV

10.2. Device manufacturers

- TÜV-certified software allows for easy implementation and cost-efficient reproduction of a PROFIsafe solution
- Different architectures of safety-related programmable controllers can adopt the PROFIsafe communication
- Trailblazer for new innovative device functions

10.3. For future investments

- Huge installed base of PROFIBUS and PROFINET devices
- PROFIBUS/PROFINET organizations and support centers are present worldwide
- Use of all existing and future standards defined by PI also for safety-related applications
- PROFIsafe is an international standard in IEC 61784-3-3 and GB/T standard in China
- Future software to assist the life-cycle of safety applications from design through assessment, validation, and documentation, thus further reducing efforts

11. PROFIBUS & PROFINET International (PI)

As far as maintenance, ongoing development, and market penetration are concerned, open technologies need a company-independent institution that can serve as a working platform. As regards the PROFIBUS and PROFINET technologies, this was achieved by founding the PROFIBUS Nutzerorganisation e.V. (PNO) in 1989 as a non-profit interest group for manufacturers, users, and institutions. The PNO is a member of PI (PROFIBUS & PROFINET International), an umbrella group which was founded in 1995. PI now has more than 25 regional user organizations (RPA: Regional

PI Associations) and approximately 1,400 members, meaning that it is represented on every continent and is the world's largest interest group for the industrial communications field (figure 21).

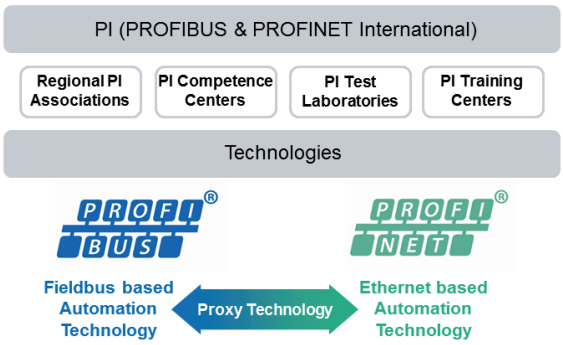

Figure 21: PROFIBUS & PROFINET International (PI)

11.1. Responsibilities of PI

The key tasks performed by PI are:

- Maintenance and further development of PROFIBUS and PROFINET
- Promotion of the worldwide establishment of PROFIBUS and PROFINET
- Protection of the investments of users and manufacturers through influence on international standardization
- Representation of the interests of members to standards bodies and unions
- Worldwide technical support for companies through PI Competence Centers (PICC)
- Quality control through a system for product certification at PI Test Laboratories (PITL) based on standard conformity tests
- Establishment of a worldwide training standard through PI Training Centers (PITC)

11.2. Technological development

PI has handed responsibility for technological development over to PNO Germany. The Advisory Board of PNO Germany oversees the development activities. Technological development takes place in the context of more than 50 working groups with input from more than 500 experts.

11.3. Technical support

PI supports more than 50 accredited PICCs worldwide. These facilities provide users and manufacturers with all kinds of advice and support. As institutions of PI, they are independent service providers and adhere to mutually agreed upon regulations. The PICCs are regularly checked for their suitability as part of an individually tailored accreditation process. Current addresses can be found on the PI website.

11.4. Certification

PI supports 10 accredited PITLs worldwide, which assist in the certification of products with a PROFIBUS/PROFINET interface. As institutions of PI, they are independent service providers and adhere to mutually agreed upon regulations. The testing services provided by the PITLs are regularly audited in accordance with a strict accreditation process to ensure that they meet the necessary quality requirements. Current addresses can be found on the PI website.

11.5. Training

The PITCs have been set up with the specific aim of establishing a global training standard for engineers and installation technicians. The Training Centers and their experts are officially accredited. Their competence with respect to PROFIBUS and PROFINET training and the associated engineering and installation services had been checked. A three days training "Profisafe Certified Designer" exists for PROFIsafe. Current addresses can be found on the PI website.

11.6. Internet

Available on the PI website www.profibus.com is actual information about the organization of PI and the PROFIBUS and PROFINET technologies. An online-product guide, a glossary, diverse web-based trainings are to be found there, as well as the download area with specifications, application profiles, installation guidelines, and other documents.

Place for Notes

PROFIsafe System Description
Technology and Application

Version April 2016
Order Number 4.342

Publisher:

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Ohiostraße 8 • 76149 Karlsruhe • Germany
Phone: +49 721 98 61 97 0 • Fax: +49 721 98 61 97 11
E-Mail: info@profibus.com
www.profibus.com • www.profinet.com

Exclusion of liability

Worldwide support with PI!

Regional PI Association (RPA)

Regional PI Associations (RPAs) represent PI around the world and are your personal local contacts. They are responsible for local marketing activities for purposes of spreading PROFIBUS, PROFINET, and IO-Link, which include among others trade fair appearances, seminars, workshops, and press conferences, as well as public relations activities.

PI Competence Center (PICC)

The PI Competence Centers (PICCs) collaborate closely with the RPAs and are your first point of contact when you have technical questions. The PICCs are available to assist you in the development of PROFIBUS or PROFINET devices and the commissioning of systems, and they provide user support and training.

PI Training Center (PITC)

PI Training Centers (PITCs) support users and developers in gaining experience with the PROFIBUS and PROFINET technologies and their possible uses. Individuals who successfully complete the final exam of the Certified Installer or Engineer course receive a certificate from PI.

PI Test Lab (PITL)

PI Test Labs (PITLs) are authorized by PI to conduct certification tests for PROFIBUS and PROFINET. You receive a certificate from PI for your product once it passes the test. The certification program plays a major role in the sustainable quality assurance of products and thus assures that the systems in use exhibit a high level of trouble-free operation and availability.

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Ohiostraße 8 • 76149 Karlsruhe • Germany
Phone: 721 98 61 97 0 • Fax: +49 721 98 61 97 11
E-Mail: info@profibus.com
www.profibus.com • www.profinet.com