Plant and process safety with **Safety Integrated**

siemens.com/safety-integrated
siemens.com/process-safety

Table of contents

1

Functional safety in the process industries

1 Functional safety
in the process industries

Reliable protection of people, plant and the environment

When operating process plants, it is important to ensure the highest possible level of safety for people, machines and the environment. Legislation obliges plant operators to comply with all rules and regulations applicable at the operating site in terms of operational safety. Malfunctions or maloperations can have fatal consequences. Therefore, the regulations aim to minimize potential hazards by technical means. To reliably eliminate sources of danger and reduce risks, an efficient safety concept is needed that meets the high requirements of functional safety. Approaches to risk reduction are diverse and range from equipment and structural installations to safety instrumented systems (SIS) and evacuation or emergency plans. Whatever protective measures are selected and combined with each other – the accepted residual risk always remains. Safety is a relative term in our technologized world. Designing safety in such a way that nothing can happen under any circumstances, the “zero risk guarantee”, is practically impossible to achieve. The residual risk is defined as the risk that remains after the protective measures have been carried out in accordance with the state of the art in science and technology.

1.1 Functional safety

Correct function of safety-related systems

Elements of automation technology are frequently used to reduce risks. The proper function of these systems and components is summarized under the term “Functional Safety”. It is given when every protective function specified in a risk assessment is executed and its required reliability is achieved. Since the introduction of IEC standard 61508, this topic has been documented independently of the application. As an application-oriented standard for the process industries, IEC 61511 serves as an international standard for the design, construction and operation of safety-related systems in process plants. Such systems, consisting of controllers, sensors and corresponding actuators, ensure automatic safety shutdown if the process moves outside defined limit values.

In order to achieve functional safety of a machine or plant, it is imperative that the safety-relevant parts of the protective and control devices function both correctly and reliably and, in the event of a fault, behave in such a way that the plant remains in a safe state or is transferred to such a state. This requires the use of specially qualified technology that meets the requirements described in the relevant standards. The requirements for achieving functional safety are based on the fundamental objectives:

- Avoidance of systematic errors
- Control of systematic errors
- Control of random errors or failures

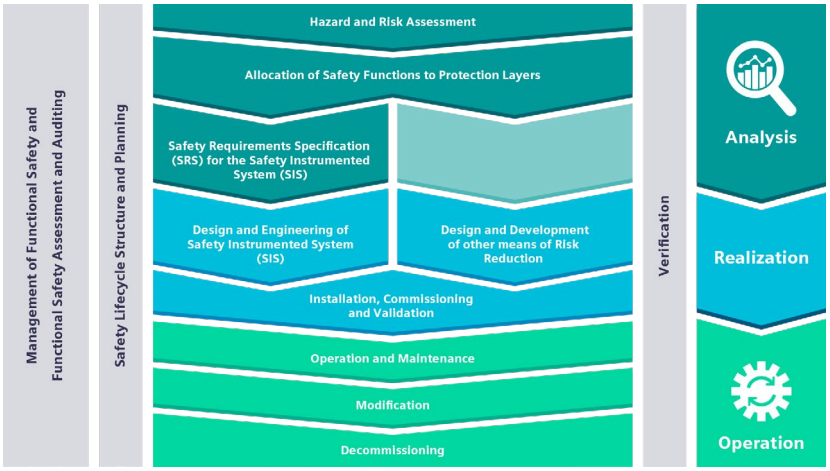
1 Functional safety
in the process industries

1.2 The safety life cycle

From idea to decommissioning – safety integrity for a lifetime

The aforementioned standards view safety as a holistic approach to systematically identifying risks and implementing the highest safety standards in industrial plants. Two things derive from this:

1. Safety cannot be guaranteed by individual operating equipment, but only by an ongoing safety assessment that considers all risk reduction measures. For maximum effectiveness of the measures, a holistic system approach is used that examines the complete safety life cycle (SLC).
2. Safety and service life are closely linked, as PCT protective devices must always operate reliably. Safety requirements must be implemented efficiently throughout the entire plant life cycle.



The safety life cycle according to IEC 61511

The introduction of the SLC concept is intended to ensure that the user observes and documents all aspects of functional safety – from initial design through implementation to operation with final decommissioning. Specifically, the SLC is divided into three main phases: Analysis, Implementation and Operation. During the analysis phase, the safety needs of a plant are determined; accordingly, the requirements for a protection system are defined. During the implementation phase, the security achieved by selecting technologies and architectures is verified and documented. In the operation phase, the required activities for operation, maintenance and modification of the security applications must be recorded.

1 Functional safety
in the process industries

1.3 The management of functional safety

Responsibility in safety-related activities in all phases of life

Manufacturers or operators of safety-related systems or components are obliged to meet the requirements of IEC 61508 for "functional safety management". The establishment of a safety management (Functional Safety Management – FSM) is therefore mandatory. For this purpose, all management activities required to achieve functional safety must be described. For all subphases and sections of the safety lifecycle of systems, IEC 61508 requires the definition of responsibilities. For the achievement and maintenance of functional safety, the following basic requirements have to be fulfilled:

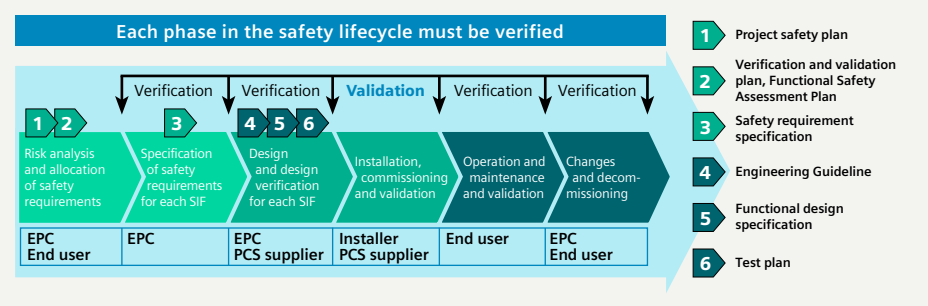
1. a precise job description and

2. the assignment to responsible persons.

The Functional Safety Manager initiates and controls all activities of the Safety Lifecycle Management. He advises the project manager and the other members of the project team on all functional safety issues.

The product life cycle of safety-related systems or components in accordance with IEC 61508 is effectively safeguarded and optimized in terms of business management through the application of needs-based process-oriented quality management.

A certified Functional Safety Management System as a supplement to the existing QM system is suitable as a verification and documentation basis for all parties involved throughout all phases of the IEC 61511 life cycle for safety applications.



Management of functional safety in the safety life cycle

1.3.1 Analysis phase

To identify possible hazards and assess their risk, process plants with hazard potential must be analyzed in a targeted manner. A suitable method for this is, for example, the HAZOP analysis (HAZard and OPerability Analysis). Based on the findings of the analysis and their evaluation, the protection levels are defined and the safety tasks and functions are assigned to these levels.

The safety instrumented system (SIS) is one level of protection. An important result of the analysis is the Safety Requirement Specification (SRS) for the safety-instrumented system. The SRS describes all safety functions (Safety Instrumented Function – SIF) including the requirements placed on them and specifies the required Safety Integrity Level (SIL). The SIL is a measure of risk reduction.

1 Functional safety
in the process industries

The IEC 61508 and IEC 61511 standards define four different safety levels: SIL 1–4. The higher the numerical value, the greater the risk reduction. The SIL is thus the measure of the probability that the safety system can correctly fulfill the required safety functions for a specific period of time.

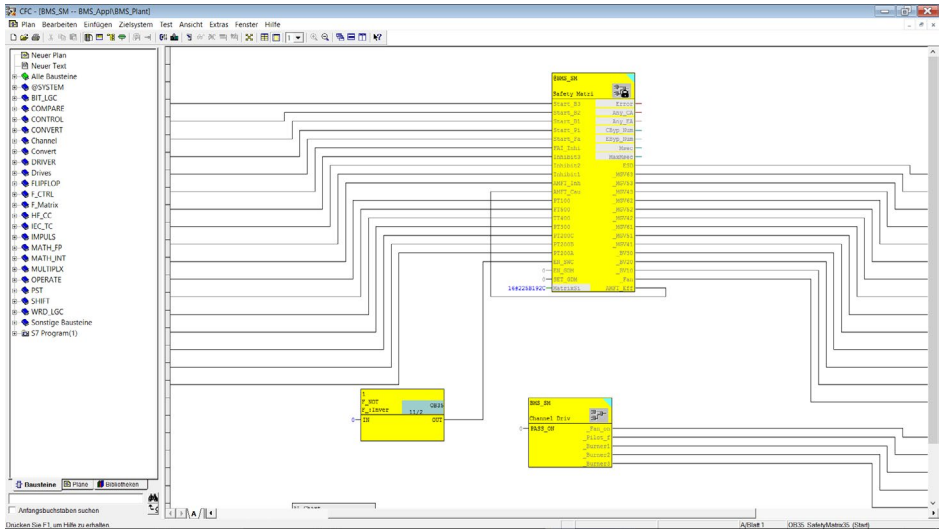
Safety Integrity Level	Probability of failure on demand (PFD) per year[1)]	Risk Reduction Factor = 1/PFD
SIL 4	≥ 10^{-5} to < 10^{-4}	10 000 to 100 000
SIL 3	≥ 10^{-4} to < 10^{-3}	1 000 to 10 000
SIL 2	≥ 10^{-3} to < 10^{-2}	100 to 1 000
SIL 1	≥ 10^{-2} to < 10^{-1}	10 to 100

[1)] Demand mode of operation

Safety Integrity Level (SIL) according to IEC 61508

1.3.2 Realization phase

The SRS is the basis for further plant planning, in particular for the design of the SIS and its safety functions as well as for other risk reduction measures. It is decisive for the selection of the SIS and the hardware and software for implementing the safety functions. Planning and design are followed by installation, commissioning, and validation of the system. In addition to the safety functions and requirements, the SRS also contains the associated tests and test criteria. Thus, the SRS is at the same time a template for verification and validation.



Realization with F Systems and CFC

1.3.3 Operation and maintenance phase

This phase covers the operation and optimization of the plant up to the point of decommissioning. Uniform, standardized documentation can simplify verification and validation of the project and accelerate implementation and commissioning. In general, all phases of the safety lifecycle and the associated activities for functional safety must be documented. These documents form the basis for the safety verification of the plant and the safety-related systems used. They are required for the acceptance of the safety functions and the safety system. In the event of a modification, all phases of the safety lifecycle must be run through again and documented.

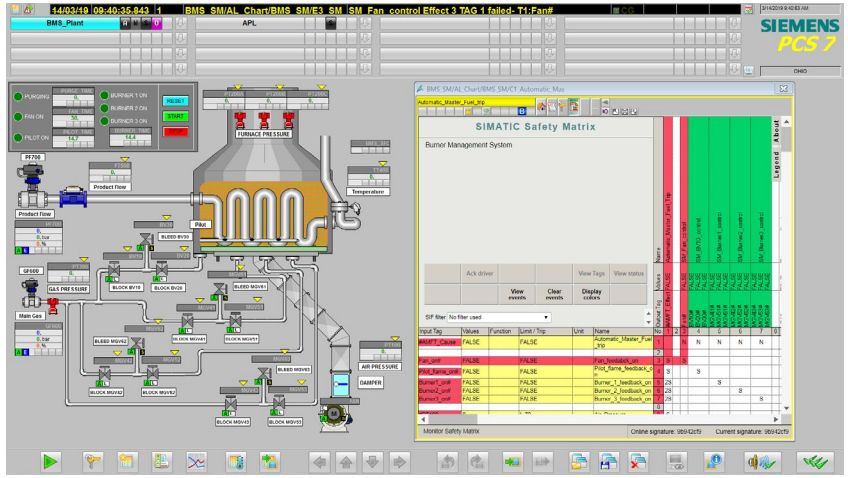
2

Siemens ensures safety with products and services

2 Siemens ensures safety **with products and services**

Safety viewed holistically and covered with suitable portfolio

Functional safety in the process industries can only be considered in a holistic context. The more complicated the processes in process plants become, the more important it is to use safety technology that is characterized by flexibility and reliability. The extensive product portfolio is flanked by comprehensive services that Siemens offers in plant and process safety. Everything can be flexibly combined for maximum on-site safety!



Monitoring and operation with SIMATIC PCS 7 and SIMATIC Safety Matrix

2.1 Safety technology from Siemens

Seamless integration of safety technology into standard automation

The safety-related system from Siemens not only includes safe controllers, bus and I/O systems, but also safe drives including motor management and safe instrumentation. Safety Integrated is the comprehensive, certified Siemens product range for functional safety in the process industries. Siemens integrates safety-related functions directly into standard products and thus offers universal solutions that can be flexibly adapted. Safety Integrated means for plant operators:

- Optimum protection for people, plant and the environment
- Flexible adaptation to the safety requirements
- Minimal engineering effort
- System consistency
- Reduced downtime
- Increased availability
- Economic operation

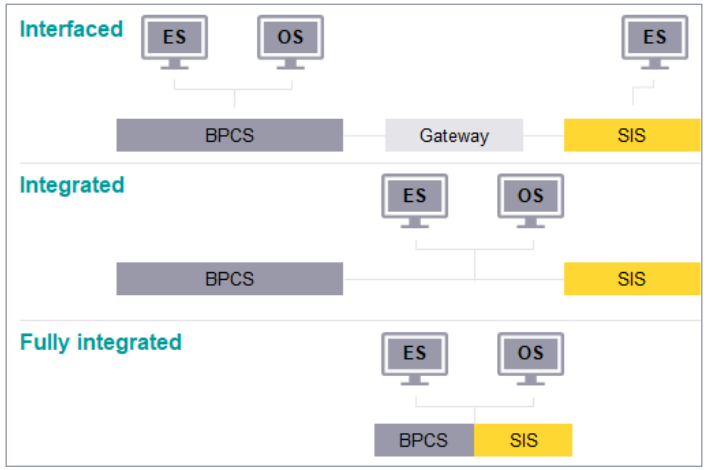
With Safety Integrated, we offer first-class, comprehensive, and end-to-end solutions for the process industries on this basis and combine them with excellent services for all life phases of a safety-related plant. A specialized process safety team provides highly qualified services and can draw on over 60 years of experience. This wealth of experience in the safety environment of the process industries, combined with the know-how of a leading and innovative electrical group, opens up unique opportunities throughout the safety lifecycle of your plants.

2 Siemens ensures safety with products and services

2.2 Integrated Control & Safety

Fully Integrated: Complete integration of the safety-related system

Safety Integrated for Process Automation from Siemens allows the best possible form of integration of the Safety Instrumented System into the process control system. With this complete integration, the Basic Process Control System (BPCS) and the SIS are based on a common hardware. The resulting reduction in space requirements, hardware, and wiring, as well as assembly, installation and engineering effort, results in significant cost savings over the entire life cycle of the plant.



Integration stages of the Safety Instrumented System in the process control system

Thanks to the innovative concept of Safety Integrated, however, all other integration levels can also be covered. In principle, the following three levels are distinguished:

2.2.1 Interfaced

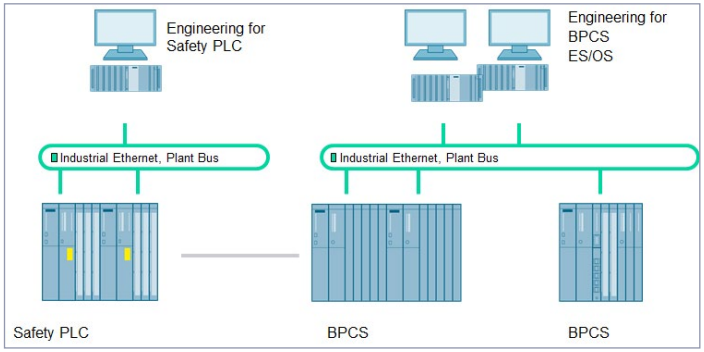
The BPCS and the safety-related system are based on separate automation systems and can be interconnected via a gateway or the I/O level for data exchange. The engineering of the systems is done via separate tools. The SIMATIC AS-410 is used for this purpose, based on SIMATIC PCS 7 and the SIMATIC Safety Integrated product portfolio. The SIMATIC AS 410 is usable as a single and a redundant system. For small or mid-size safety applications up to SIL 3 the AS 410E is available.

See also Chap. 4

2 Siemens ensures safety with products and services

The advantages at a glance

- Strict separation: BPCS is separated from the safety system
- Mutual influence of both systems excluded due to separate data basis
- Manufacturer-independent: any BPCS can be used



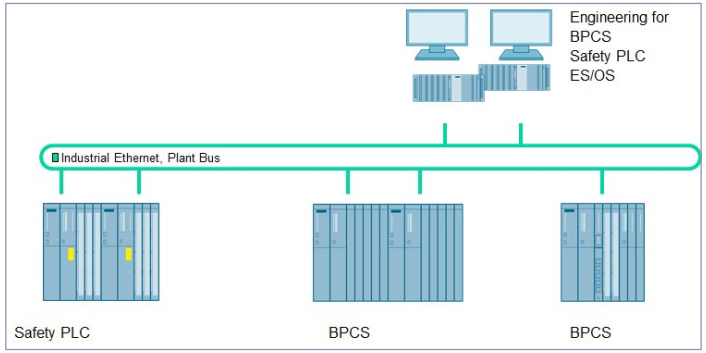
Interfaced solution

2.2.2 Partly Integrated

The BPCS in the process control system and the safety-related system are based on different SIMATIC AS-410 automation systems. However, all systems use the same engineering and operator system. Functionally, however, safety functions and functions of the SIMATIC PCS 7 process control system are strictly separated from each other. No safety functions are processed in the BPCS systems.

The advantages at a glance

- Lower costs for hardware and installation as well as in spare parts inventory
- Reduced engineering and maintenance costs
- Less training effort



Partly Integrated

2 Siemens ensures safety with products and services

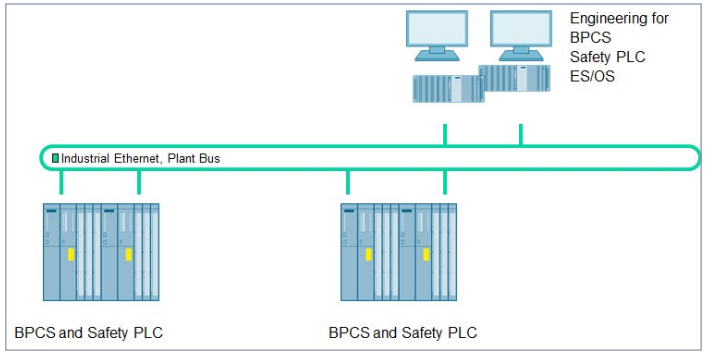
2.2.3 Fully Integrated

The BPCS and the safety-related system are combined in the process control system. They use common hardware (controller, fieldbus, I/O periphery). Standard programs and safety-related programs run in parallel and independently of each other. In the fully integrated solution, the engineering system and the automation system of SIMATIC PCS 7 are used for both the control and the safety system. The fully integrated solution is TÜV-certified and approved for applications up to SIL 3.

The advantages at a glance

- Seamless integration incl. time synchronization
- Maximum possible savings potential with regard to hardware used and spare parts to be kept on hand
- Common HMI, compatible configuration tools
- Minimal training effort

The modularity and flexibility of Safety Integrated allow you to define the degree of integration individually. You determine the degree of diversity, independence or physical separation yourself and can decide, for example, whether you want BPCS functions and safety functions to be executed in one controller (automation system) or in separate controllers.



Fully Integrated

Many of the advantages of Safety Integrated can already be used because this system can be integrated into any open process control system via standardized communication via PROFIBUS/PROFINET and Industrial Ethernet. These include:

- Processing of standard and TÜV-certified safety functions in the same S7-400 controller
- No separate safety bus: standard communication and safety-related communication run via the same fieldbus (PROFIBUS or PROFINET with PROFIsafe)
- Mixed operation of standard modules and safety-related I/O modules in remote I/O stations SIMATIC ET 200SP HA, SIMATIC ET 200iSP and ET 200M
- Reduced training effort due to uniform engineering
- Reduced spare parts inventory through use of standardized hardware

2 Siemens ensures safety with products and services

However, the full potential of Safety Integrated can only be exploited through its unique combination with the universal SIMATIC PCS 7 process control system from Siemens. This allows you to benefit from additional advantages such as:

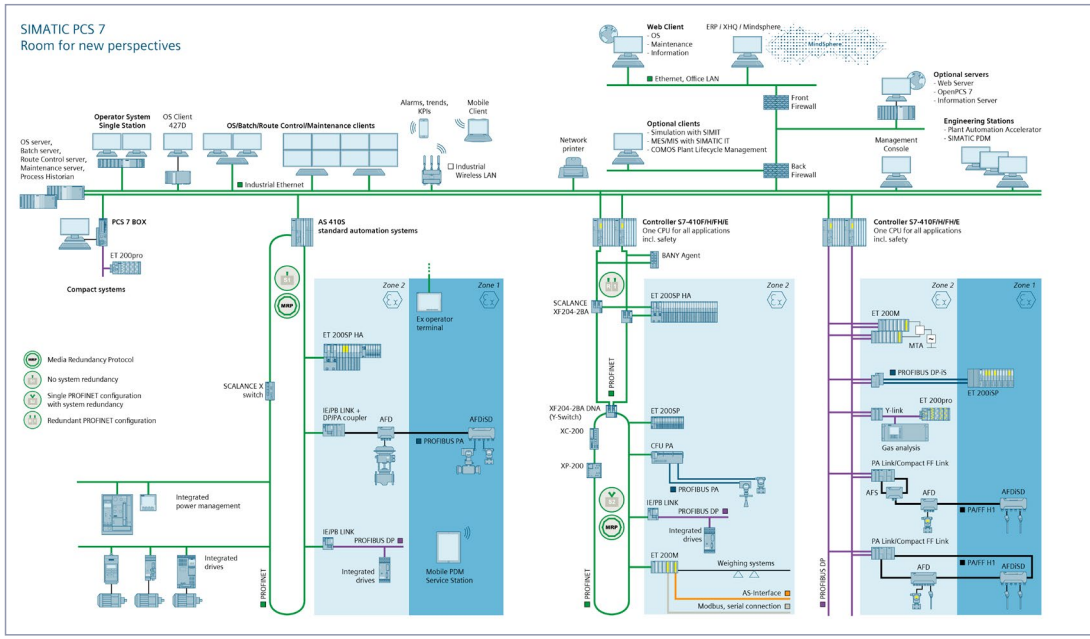
- A common engineering system for BPCS and SIS
- A common controller platform
- Consistent data management: no time-consuming data handling between BPCS and SIS
- Integration of the safety-related applications into the process visualization on the operator station
- Automatic integration of time-stamped safety-related fault messages into the process control system
- Integration of safety-related hardware into asset management with the Maintenance Station for diagnostics and preventive maintenance

The safety system usually communicates with systems and tools for engineering, process, and operational management as well as diagnostics and maintenance via the plant bus, and in the case of client-server systems also via a terminal bus if necessary. In modern, open process control systems, the plant bus and terminal bus are usually industrial Ethernet LANs.

In the user interface of these systems and tools, the Safety Integrated System is represented by operable image blocks.

The Safety Integrated System is integrated into the plant bus via robust Ethernet connections in the controllers and Industrial Ethernet switches such as SCALANCE X that are suitable for the bus medium used.

The SIMATIC PCS 7 plant bus, which is based on Industrial Ethernet in accordance with the IEEE 802.3 standard, is often designed as an optical ring for reasons of interference immunity and availability. For very high availability requirements, it can also be configured as an optical double ring that tolerates double faults such as the failure of a switch on ring 1 and the simultaneous disconnection of the bus cable from ring 2.



SIMATIC PCS 7 system architecture

2 Siemens ensures safety with products and services

2.3 Flexible Modular Redundancy (FMR)

Cost-optimized safety through flexibly scalable fault tolerance

With Flexible Modular Redundancy (FMR), Siemens offers an innovative concept for implementing cost-effective scalable safety solutions. This allows multiple fault tolerance levels to be implemented exactly where they are required for the respective application.

Depending on the automation task and the safety requirements, the project engineer can define the degree of redundancy for the individual architecture levels controller, fieldbus, and I/O periphery separately and coordinate it with the field instrumentation. Within a level, each component can be set up redundantly, even physically separated. All components also meet the requirements of safety level SIL 3.

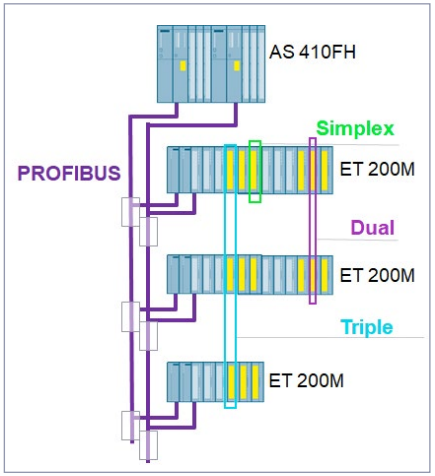
Fault-tolerant architectures that tolerate multiple simultaneous faults can thus be tailored directly to specific tasks. As shown by example configurations with I/O systems on the PROFIBUS DP and PROFIBUS PA fieldbuses, the sum of the tasks can result in a mix of different redundancy levels within an architecture level (1oo1, 1oo2, 2oo3, NooM).

Reliability modeling shows that FMR achieves higher availability levels than conventional redundant architectures with uniformly double or triple stacking.

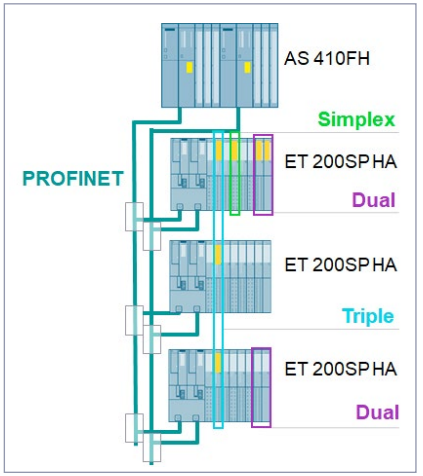
Since FMR provides redundancy only where it is needed, comparatively more attractive and cost-effective security applications can be realized with FMR than with classic redundancy architectures.

Advantages at a glance

- Safety not tied to redundancy:
  Safety-integrated technology offers safety even with single systems
- Redundancies serve the availability
- Redundancy selection to match the Safety Instrumented Function (SIF)
- Peripheral and field device redundancy independent of CPU redundancy
- No time-limited safety operation in case of component failure (so-called degraded mode)



FMR with PROFIBUS



FMR with PROFINET

2 Siemens ensures safety with products and services

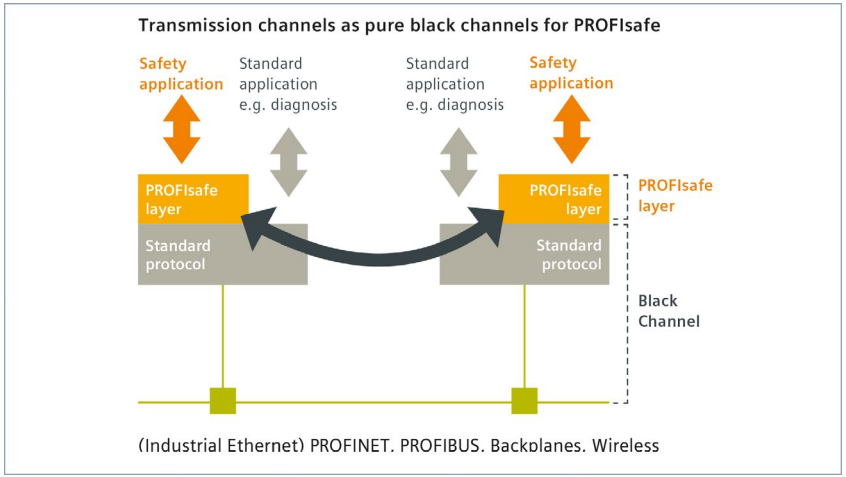
2.4 Safety-Integrated Fieldbus Technology

PROFIsafe – Safe communication via PROFIBUS or PROFINET

The PROFIsafe profile enables safety-related communication between the automation system (controller) and the process periphery via PROFIBUS as well as via PROFINET. The decision for field communication via PROFINET or PROFIBUS DP/PA has a significant influence on the architecture of the safety-related system.

The PROFIsafe profile is implemented as an additional software layer in the devices/systems without changing the communication mechanisms of PROFIBUS or PROFINET. Non-safe and safety-related communication can be used in parallel. The PROFIsafe telegrams are extended with additional information that allows the PROFIsafe communication partners to detect and compensate for transmission errors such as delay, incorrect sequence, repetition, loss, misaddressing, or data corruption. For this purpose, the error detection measures shown in the table are executed and controlled in each communication partner.

PROFIsafe communication is based on the IEC 61158 and IEC 61784-3-3 standards and meets the safety requirements up to SIL 3 according to IEC 61508 / IEC 62061 or PL e / Cat4 according to ISO 13849. Siemens systems support the current (as of 2021) PROFISAFE profile 2.6.1.



PROFIsafe Black Channel – Procedure

Error	Measure			
	Consecutive number	Time expectation with acknowledgment	Identification of transmitter and receiver	Data backup CRC
Repetition	●			
Loss	●	●		
Insertion	●	●	●	
Incorrect sequence	●			
Data falsification				●
Delay		●		
Coupling of safety-related messages and standard messages (masquerade)		●	●	●
FIFO faults		●		

PROFIsafe fault detection measures of communication partners

2 Siemens ensures safety with products and services

2.4.1 Communication via PROFIBUS

At the field level, decentralized peripheral devices such as remote I/O stations with their I/O modules, transmitters, drives, valves or operator terminals communicate with the controllers via a powerful real-time bus system.
This communication is characterized by:

- cyclic transmission of process data and
- acyclic transmission of alarms, parameters and diagnostic data.

PROFIBUS, which uses a communication protocol to enable fast communication with intelligent distributed I/O devices (PROFIBUS DP) as well as communication and simultaneous power supply for transmitters and actuators (PROFIBUS PA), is predestined for this purpose. It is simple, reliable and robust, can be expanded online with new decentralized components and can be used in standard environments as well as in hazardous areas.

It also offers a wide range of options for communication and line diagnostics as well as for diagnosing the connected intelligent field devices. Furthermore, it is fully integrated into the global asset management of the SIMATIC PCS 7 process control system.

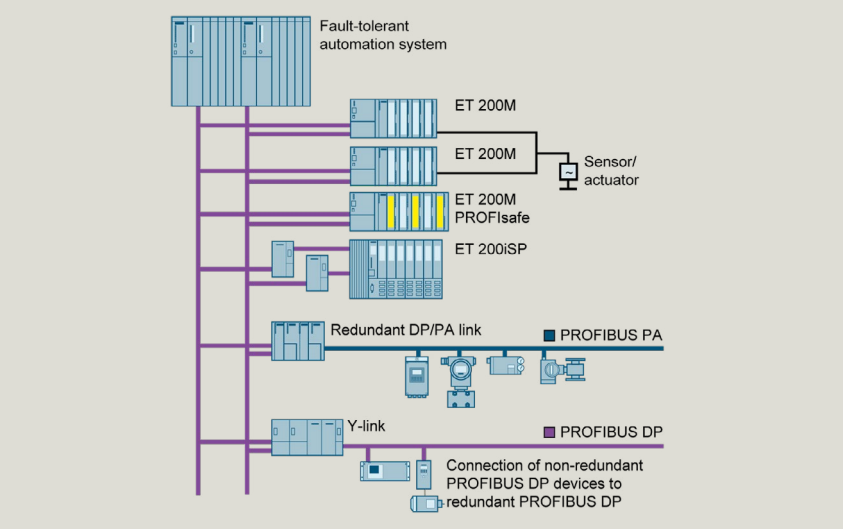
PROFIBUS supports the coexistence of field devices from different manufacturers on one line (interoperability) as well as the exchange of devices of a profile family independent of the manufacturer.

In addition to all these features, the following PROFIBUS functions are particularly relevant for process automation:

- Integration of already installed HART devices
- Redundancy
- Safety-related communication with PROFIsafe up to SIL 3 according to IEC 61508
- Clock synchronization
- Time Stamping

In general, a distinction is made between the following two design variants (see figure):

- Single-channel, non-redundant design
- Redundant, highly available and fault-tolerant design



Examples for safety systems with PROFIBUS

2 Siemens ensures safety with products and services

At the individual architecture levels (controller, fieldbus, I/O periphery), project planning alternatives are available depending on the I/O periphery used (SIMATIC ET 200SP HA, SIMATIC ET 200iSP, ET 200M or PROFIBUS PA devices).

With the aid of fieldbus isolating repeaters (RS 485-iS couplers) and RS 485-iS electrical transmission technology, the PROFIBUS DP can also be run as an intrinsically safe fieldbus up to Ex zone 1 or 21 (SIMATIC ET 200iSP remote I/O stations).

The PROFIBUS PA fieldbus developed for the direct integration of sensors and actuators is integrated into the PROFIBUS DP via a network transition in simple or redundant design. With a simple network transition, PROFIBUS PA can be created in a line or tree structure on a simple or redundant PROFIBUS DP. Higher availability levels are achieved by the redundant network transition in connection with a line or ring structure. A configuration with redundant network transition and ring structure can tolerate single errors such as the failure of a DP/PA coupler or the interruption of the bus line.

2.4.2 Communication via PROFINET

PROFINET, which is based on the international IEC 61158 and IEC 61784-2 standards, combines the advantages of the open Ethernet network standard and the PROFIBUS fieldbus system. PROFINET stands for maximum transparency, open IT communication, network security, and real-time communication down to the field level. This standard means high availability and flexibility for plant expansions as well as simple and fast device replacement.

The safety-oriented communication is based on the PROFIsafe profile and is primarily focused on PROFINET communication between the automation system (controller) and process peripherals.

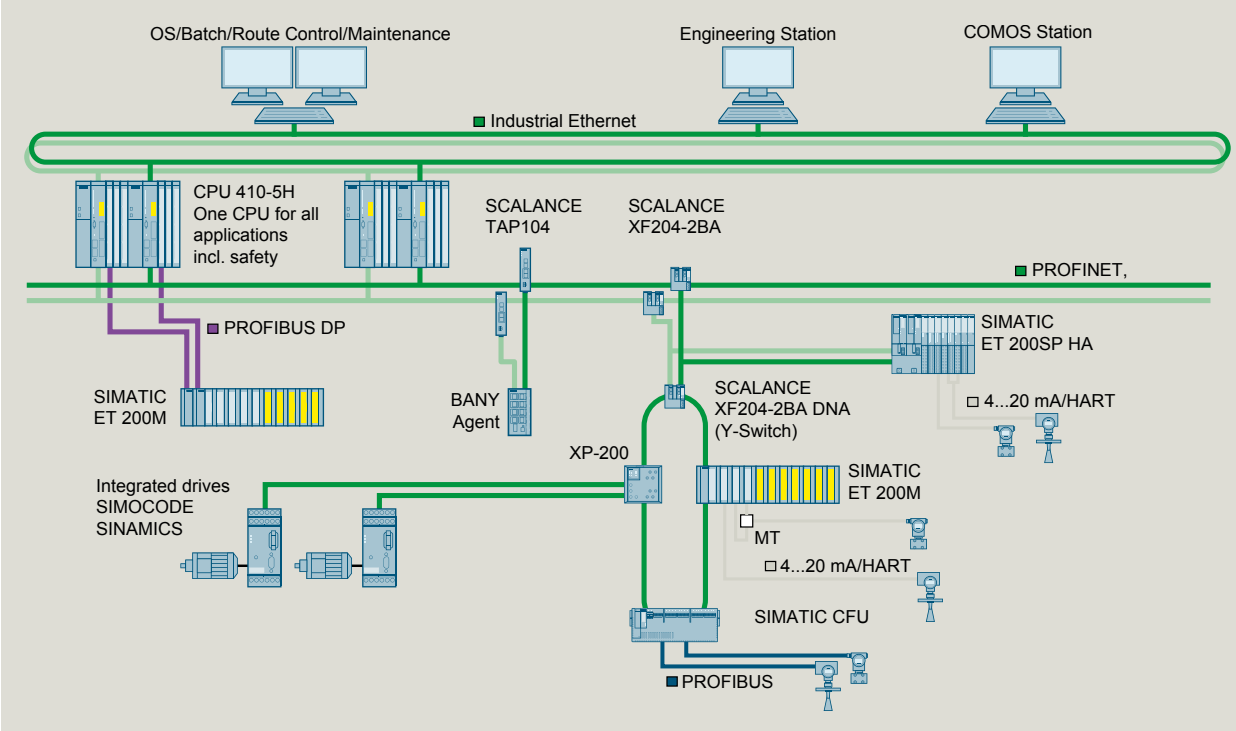
Safety-related SIMATIC PCS 7 automation systems of the S7-400 series can be easily and effectively networked via PROFINET with SIMATIC ET 200M, SIMATIC ET 200SP HA remote I/O stations. In the automation system (controller) the PROFINET interface of the CPU is available for this purpose.

With SIMATIC PCS 7 from version 9.0 and a large number of hardware and software innovations, the functional scope of PROFINET in PCS 7 has been significantly expanded, for example by flexible scalable availability with functionalities such as:

- Simple (S1) or redundant (S2 and R1) system connection
- Media redundancy (via the media redundancy protocol – MRP) for easy assurance of network and plant availability
- Changes during operation

Based on the topologies line, star, tree and ring, a wide range of network configurations can be implemented. Industrial Ethernet products are used as network components, e.g. SCALANCE X switches and media converters, FastConnect connection elements as well as electrical and optical transmission media.

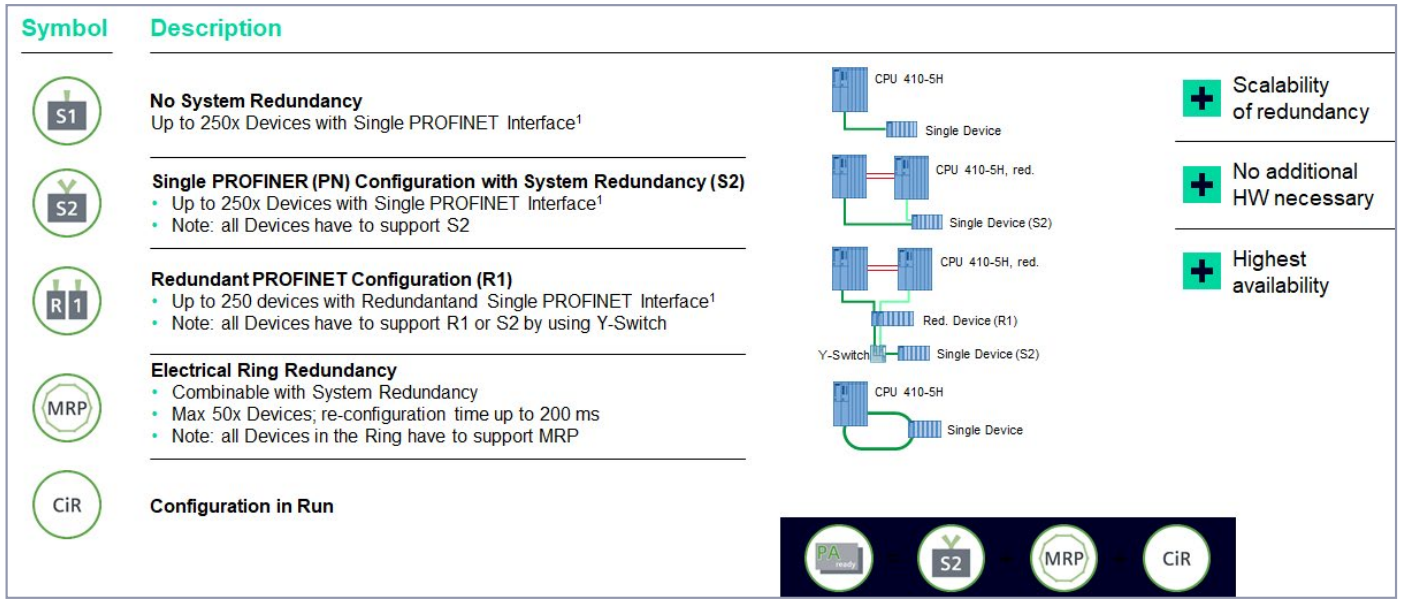
2 Siemens ensures safety with products and services



PROFINET follows the Ethernet standard according to IEEE 802.3 100 percent and is thus the reliable, future-proof standard that paves the way for digitalization in the process-related environment. Combine investment protection with future security: The open Industrial Ethernet standard ensures the integration of existing plant components and technologies as well as existing bus systems. Appropriate solutions and products are available for this purpose, such as the IE/PB LINK for integrating PROFIBUS DP or the SIMATIC CFU PA for integrating PROFIBUS PA. On the other hand, worldwide standardization in accordance with IEC 61158/61784 and consistent further development ensure the use of PROFINET over the entire life cycle of the plant and beyond. Wireless communication technologies such as WLAN according to IEEE 802.11 or mobile radio can also be reliably integrated.

2 Siemens ensures safety with products and services

PROFINET has the following redundancy mechanisms:



PROFINET redundancy and function

Configurations with redundant automation systems and PROFINET IO communication in “system redundancy” design achieve the highest availability with minimum error response times. Here, each I/O device establishes a communication link with each of the two CPUs of the redundant automation system via the topological network. The Siemens-specific symbolism “PA-ready” is used to specify PROFINET IO devices that meet the requirements of process automation. A system or device is PA-ready if it supports MRP, S2 redundancy and configuration in run (CiR). The different network structures can be combined. This makes it possible to adapt the network structure of the system exactly to the requirements. The most important mechanisms here are media redundancy in the ring (MRP) and S2 and R1 redundancy.

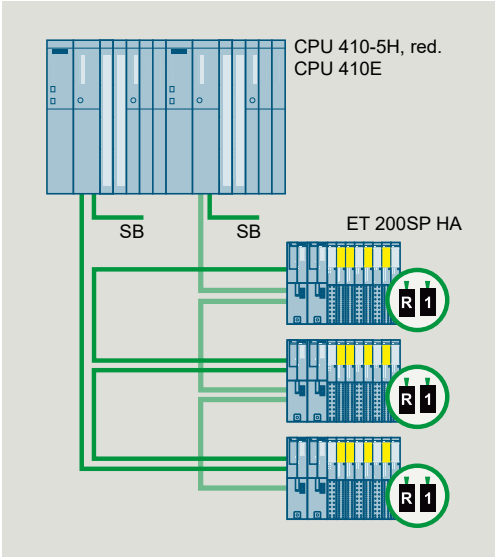
2 Siemens ensures safety with products and services

In order to fully exploit the new possibilities of PROFINET, the hardware portfolio has been fundamentally enhanced:

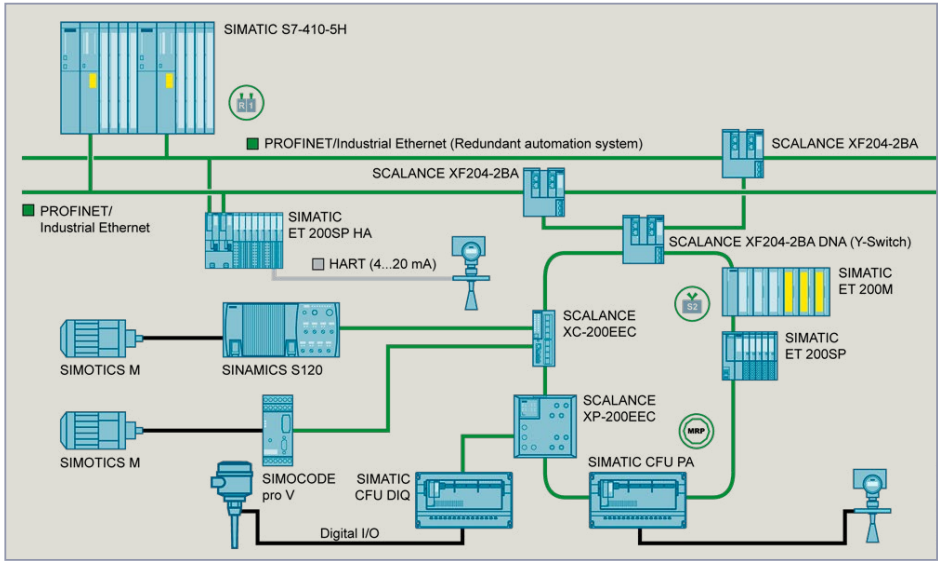
- CPU 410-5H
- SIMATIC ET 200SP HA
- SIMATIC CFU PA (for non-safety-related applications)
- SCALANCE XF204-2BA DNA (“Y-Switch”)

The SIMATIC PCS 7 CPU 410-5H enables redundant automation systems and redundant devices (R1) to be built up into a highly available H-System by means of redundant PROFINET configuration.

Through the SCALANCE XF204-2BA DNA “Y-switch”, a network setup with system redundancy (S2) to the field level can be connected to an H-system (R1). MRP networks are also supported by the switch: Redundant communication of devices in the ring is established by the media redundancy protocol (MRP).



R1 redundancy



Redundant network structure R1, S2 and MRP

2 Siemens ensures safety with products and services

The SIMATIC ET 200SP HA distributed I/O and the SIMATIC CFU PA (Compact Field Unit) field distributor have a PROFINET interface for S2 redundancy. This creates flat and flexible architectures that support flatter plant expansions without holding reserves and offer potential for significant savings in wiring. The motto “one cable for everything” makes it possible to operate profiles such as PROFIsafe, PROFIdrive, and other TCP/IP protocols in parallel without affecting basic plant communication. These hardware components rely on BusAdapter technology, which enables simple and flexible connection to the PROFINET network either via copper (RJ45/FastConnect) or fiber optics.

PROFINET in combination with appropriate hardware components supports you in planning, operating, and commissioning: convenient device replacement without additional tools through automatic neighborhood detection as well as clear and simple installation guidelines including automatic addressing and naming.

Configuration in Run (CiR)

To ensure that your plant remains available during this work, the components allow changes to be made to the plant during operation (“Configuration in Run”, CiR) without affecting the process engineering process. This is available for an H-system (H-CiR) as well as for a Single Station (CiR).

Benefits of PROFINET at a glance

- Ethernet at the field level
- Highest availability on demand
- Higher flexibility
- Ease to use
- Security of investment

2 Siemens ensures safety with products and services

2.5 Functional Safety and Industrial Security

Observe individual peculiarities of functional safety and IT security

Functional safety and (industrial) IT security are two different disciplines. Today, both have the same significance in process plants. Despite many approaches that appear to be common, it is important to consider the individual characteristics of both safety approaches and to take them into account in parallel over the entire life cycle. Siemens therefore pursues an integrative approach to safety and security measures for its customers, while at the same time establishing a comprehensive security culture throughout the entire company.

2.5.1 Safety Lifecycle Consulting

For standardized processes, clear responsibilities, and plannable use of resources

With Safety Lifecycle Services, Siemens not only contributes the necessary expert knowledge for proving safety, but also advanced working tools and methods that eliminate systematic errors in all project phases. Jointly, we develop a concept for the safe operation of your process. We evaluate the safety-related properties of the chemical substances and reaction mixtures with regard to safe process control for your individual process steps.

Our experts are experienced leaders of HAZOP and safety meetings. In systematic risk analyses, we assess and document the safe operation of your plant and process. We support you in licensing and contacts with authorities, e.g. in the development of explosion protection concepts, the implementation of European occupational safety legislation or occupational safety regulations and the preparation of the safety report according to the Seveso Directive in the EU. Some of our experts are accredited in Germany according to § 29b (1) BImSchG (Federal Immission Control Act).

We use targeted audits to check your plants and processes for compliance with the state of the art in safety technology, conformity with laws and regulations, and compliance with applicable permits.

In addition to these classic topics of process and plant safety, we offer all necessary services for the implementation of safety-related systems. In accordance with IEC 61511 – and all other dependent standards – we offer consulting and support in all phases of your safety life cycle up to verification and validation (e.g. SIL verification, hardware and software audits).

If, despite all precautions, a (near) accident should occur, we are available to you as experts in the field of process safety with our help in analyzing the accident. To investigate complex accidents, we use special measurement methods that go far beyond routine testing. The experience gained from numerous accident analyses in the past is incorporated into our work.

2 Siemens ensures safety with products and services

An excerpt from our range of services:

- Management, functional safety assessment and audits
- Structure and planning of the SLC (Safety Plan)
- Development of explosion protection concepts
- Safety and risk analyses (e.g. HAZOP)
- Hazard and safety assessment
- Assignment of the safety functions to the protection levels
- Specification of safety requirements (SRS)
- Verification and validation (e.g. SIL verification, hardware/ software audit)
- Modification
- Training

See: www.siemens.com/process-safety

2.5.2 Safety specialists with certified qualification

Siemens employs safety experts with certified qualifications for Safety Lifecycle Services. These have completed a structured training program to become Siemens Functional Safety Professionals (SFSP) or Siemens Functional Safety Experts (SFSE), which Siemens organizes and offers in close cooperation with TÜV. Employees of the operator (end customer) and Solution Partners (system integrators) can also participate in this training program. Our Solution Partners are highly qualified partner companies that offer professional consulting and services for all relevant safety aspects. They are familiar with safety technology in the process industries and have:

- Know-how about the Safety Lifecycle of IEC 61511
- Knowledge of Safety Engineering with S7 F Systems and SIMATIC Safety Matrix
- Extensive experience in projects with safety applications in the process industries

TÜV Süd certified persons

2 Siemens ensures safety with products and services

2.6 Industrial Security

Industrial safety is a constantly changing challenge

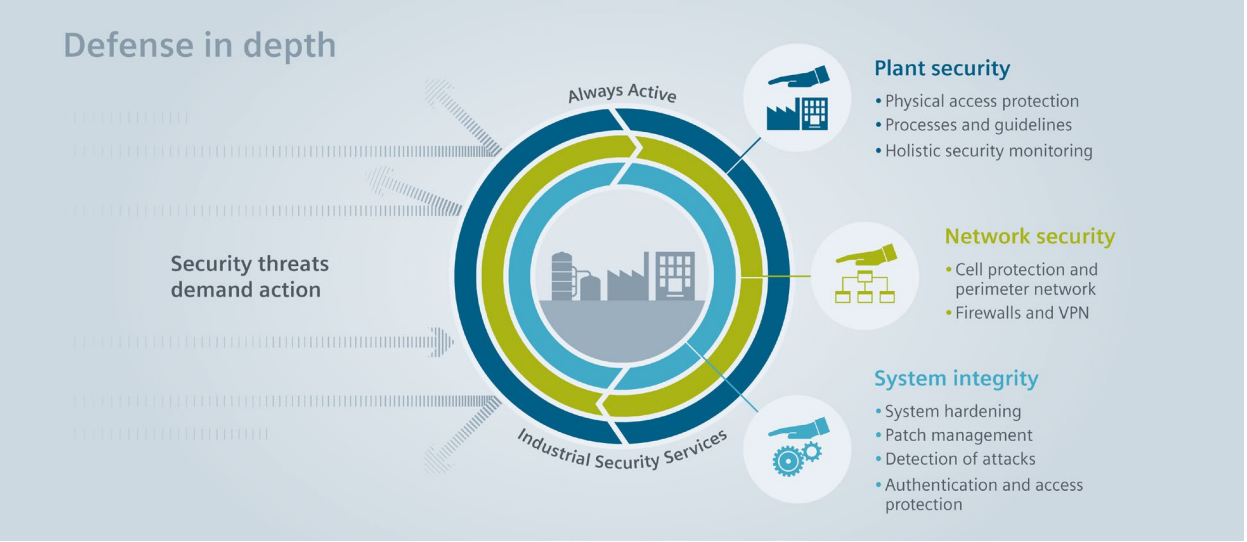
Digitalization and the increasing networking of machines and industrial plants are also increasing the risk of cyberattacks. Corresponding protective measures are therefore mandatory, especially for critical infrastructure facilities. In order to comprehensively protect industrial plants against cyberattacks from inside and outside, measures must be taken at all levels simultaneously – from the operating level to the field level, from access control to copy protection.

2.6.1 Siemens Security Concept: Defense in Depth

With Defense in Depth, Siemens offers a multi-layered concept that protects your plant both all around and in depth. The concept is based on plant security, network security and system integrity – according to the recommendations of IEC 62443, the leading standard for security in industrial automation.

2.6.1.1 Plant Security

Plant security uses various methods to secure the physical access of persons to critical components. This starts with classic building access and extends to securing sensitive areas with code cards. Comprehensive security monitoring provides transparency about the security status of production facilities. Thanks to continuous analyses and correlations of existing data, as well as the comparison of these with threat indicators, security-relevant events can be identified and classified according to risk factors. On this basis and through regular status reports, operators receive an overview of the current security status of the production facility, which enables a rapid response in the event of a threat.



Network security as a central component of Siemens' industrial security concept

2 Siemens ensures safety with products and services

2.6.1.2 Network Security

Network security means protecting automation networks from unauthorized access. This includes the control of all interfaces, such as between the office and plant networks or remote maintenance access to the Internet and can be achieved with the help of firewalls and, if necessary, by setting up a DMZ (demilitarized zone = security-shielded zone). The DMZ is used to provide data for other networks without granting direct access to the automation network. The safety-related segmentation of the plant network into individual protected automation cells serves to minimize risks and increase safety. The cells are divided and the devices assigned according to communication and protection requirements. Data transmission can be encrypted via Virtual Private Network (VPN) and thus protected against data espionage and manipulation. The communication participants are authenticated securely. With Industrial Security Appliances SCALANCE S, Industrial Routers SCALANCE M or Security Communication Processors for SIMATIC, automation networks, automation systems and industrial communication can be secured.

2.6.1.3 System Integrity

The third supporting pillar of Defense in Depth is securing system integrity. The focus here is on protecting automation systems and control components SCADA HMI and OS systems against unauthorized access or meeting special requirements such as know-how protection. For this purpose, Siemens has integrated both the security concept and the security mechanisms in fully integrated safety solutions. The focus is also on user authentication, access and change authorizations, and system hardening, i.e. the robustness of the components against possible attacks.

For more information, see the Internet at:
www.siemens.com/industrial-security

2.6.2 SIMATIC PCS 7 Security

The top priority of SIMATIC PCS 7 is the unconditional maintenance of control over production and processes by the operating personnel – even in the event of security threats. The prevention or restriction of the spread of a security threat to systems and networks should be achieved while maintaining the complete operability and observability of production and processes. The security concept for SIMATIC PCS 7 has the task of ensuring that only authenticated users can perform authorized operations on authenticated devices via the operating options assigned to them. These operations may only be performed via unique and planned access paths in order to ensure safe production or coordination during a job without any hazards for people, the environment, the product, the goods to be coordinated and the company's business. The SIMATIC PCS 7 security concept describes a Defense in Depth strategy based on the international standard IEC 62443. The security protection measures for process automation with SIMATIC PCS 7 based on this concept are described in detail in the manuals "SIMATIC Process Control System PCS 7 Compendium Part F – Industrial Security" and "Process Control System PCS 7 Security Concept PCS 7 & WinCC (Basis)". Several levels of protection are created to minimize risks and increase the safety of the plants.

- Plant security denies unauthorized persons physical access to critical components
- Network security protects production from unauthorized access from office environments or the Internet
- System integrity prevents unauthorized modifications to process automation

2 Siemens ensures safety with products and services

Elements of the SIMATIC PCS 7 security concept:

- Physical access protection
- Cell segmentation through firewalls
- System hardening
- Patch management
- User administration (SIMATIC Logon)
- Malware detection and prevention
- Training and processes

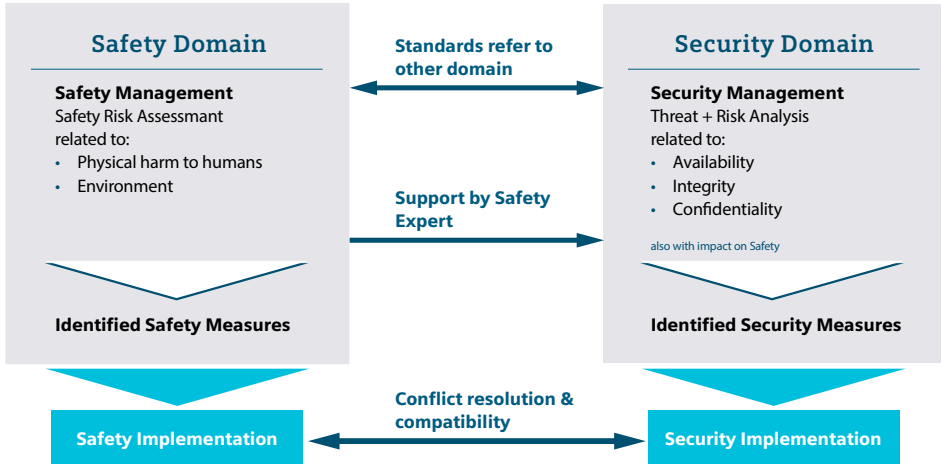
With Industrial Security Services, Siemens also supports the development of customized security solutions for the entire life cycle of the plant. The offer includes a detailed security assessment, the selection and implementation of the optimum measures, and updating and risk adjustment. However, even with all known protective measures, absolute security cannot be guaranteed. However, by combining SIMATIC PCS 7 IT Security with security technology, the effects of cybercrime can be neutralized.

For more information, see the Internet at:
www.siemens.com/industrial-security

2.6.3 Security and essential functions

Essential functions are all functions required to protect health and the environment and to ensure safety and availability of the plant. According to IEC 62443-3-3, these functions include, but are not limited to, the Safety Instrumented Function (SIF).

In order to create a secure environment in the sense of security for the essential functions, a holistic and realistic security approach is required. Safety and security are two different subject areas which, although they have similar approaches in some cases, also pursue divergent aspects and can nevertheless influence each other.



Safety & Security, 2 fields of activity

2 Siemens ensures safety with products and services

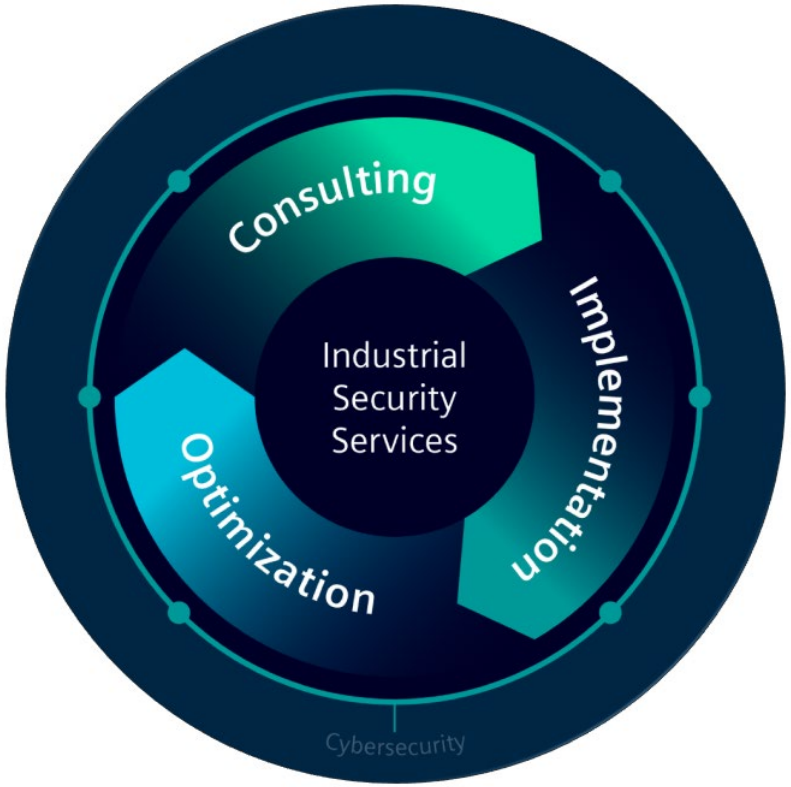
IEC 61508/11 (functional safety) and IEC 62443 (security) also refer to each other in this respect. The security measures can have an influence on the automation architecture of the plant. Depending on the hazard assessment and the result of the risk analysis, various plant configurations are possible. The Siemens solutions cover different configurations.

2.6.4 Industrial Security Services

A holistic approach ensures industrial security in three steps

Industrial Security Services include the necessary hardware and software, but above all service experts who combine expertise in automation, digitalization, and security. The experts support you right from the start and work with you to develop the necessary strategy, implement it and continuously optimize protection. The offering follows the holistic approach of Digital Enterprise Services in the three steps of consulting, implementation, and optimization with corresponding modules.

For more information, visit:
www.siemens.com/industrial-security



3

Safety-related hardware and software from SIMATIC

3 Safety-related hardware and **software from SIMATIC**

With certified products to a safe investment

The range of safety-related Siemens products for the process industries includes controllers, bus and I/O systems as well as instrumentation.

3.1 Safety-related SIMATIC systems in the process industries

Safety-related SIMATIC automation systems are used for critical applications in which a fault can endanger human life, damage the plant or cause environmental damage. In conjunction with the safety-related F modules of the ET 200 decentralized I/O systems or safe transmitters connected directly via fieldbus, they detect faults in the process as well as their own internal faults and automatically transfer the plant to a safe state in the event of a fault.

The SIMATIC AS 410/410E safety-related automation systems and the SIMATIC S7-400 series are predestined for implementing safety-related applications in process automation. They are multitasking-capable, i.e. several programs can run simultaneously in one CPU – BPCS (standard) applications as well as safety-related applications. The programs are reaction-free, i.e. errors in BPCS applications have no effect on safety-related applications and vice versa. Special tasks with very short response times are also possible.

Redundancy configurations with two CPUs operating on the 1-out-of-2 principle also increase availability. Two identically configured subsystems, which are galvanically isolated from each other to optimize EMC properties, are synchronized with each other via fiber optics. In the event of a fault, the active subsystem switches smoothly to the backup system. Both subsystems can be mounted on a common subrack or spatially separated from each other by up to 10 km. Spatial separation provides additional safety benefits in the event of extreme external influences in the local environment of the active subsystem, e.g. fire.

For smaller process safety applications, e.g. burner controls, the SIMATIC AS 410 Entry can also be used.

All mentioned controllers are certified by TÜV and fulfill safety requirements up to SIL 3 according to IEC 61508. They can process BPCS and safety functions in parallel with one CPU. Mutual interference during processing is prevented by the fact that safety-oriented programs and BPCS programs remain strictly separated from each other and data exchange takes place via special conversion blocks. The safety functions are processed twice in different processor parts of a CPU by redundant, diverse instruction processing. Possible errors are detected by the system during the subsequent comparison of the results.

Safety programs running on different controllers in a plant can communicate with each other in a safety-oriented manner via the Industrial Ethernet plant bus. Possible communication partners are also the controllers of the SIMATIC S7-400 and S7-300 series.

3 Safety-related hardware and **software from SIMATIC**

Fail-safe SIMATIC controllers for the process industries

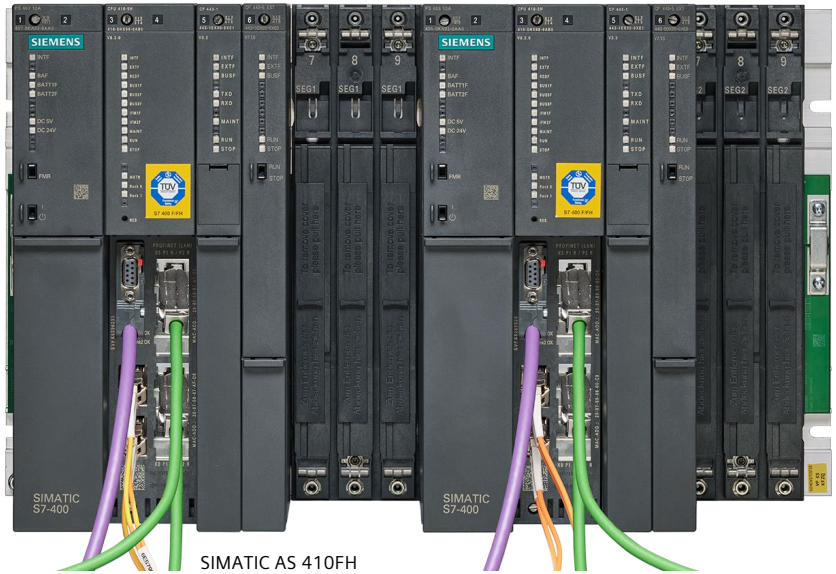
	AS-Typ	F-Systems	Distributed safety	Safety Matrix with PCS 7	STEP 7 / TIA Portal	PCS 7	ET 200M F-/0	ET 200iSP F-/0	ET 200SP HA F-/0	Number of POs
Failsafe automation systems SIL 3										
SIMATIC S7-400 single systems	S7-412F	●		●	●	●	●	●	●	30
	S7-414F	●		●	●	●	●	●	●	350
	S7-416F	●	●	●	●	●	●	●	●	1200
	S7-417F	●		●	●	●	●	●	●	2000
SIMATIC S7-400 redundant systems	S7-412FH	●		●	●	●	●	●	●	30
	S7-414FH	●		●	●	●	●	●	●	350
	S7-416FH	●		●	●	●	●	●	●	1200
	S7-417FH	●		●	●	●	●	●	●	2000
SIMATIC PCS 7 AS 410 Single	AS 410FE	●		●		●	●	●	●	200
	AS 410F	●		●		●	●	●	●	EC
SIMATIC PCS 7 AS 410 redundant	AS 410FHE	●		●		●	●	●	●	200
	AS 410FH	●		●		●	●	●	●	EC

Overview and applicability

The ordering units of the AS-Bundles are also shown in tabular form in the SIMATIC PCS 7 catalog ST PCS 7. Individual components can be selected in the ST PCS 7 and ST 70 catalogs. Both catalogs can be accessed via the Internet at:

www.siemens.com/simatic/brochures

3 Safety-related hardware and **software from SIMATIC**



SIMATIC AS 410FH

3.2 Safety-related controllers for the process industries

3.2.1 AS410 F/FH

With the robust all-round system AS 410, the SIMATIC PCS 7 process control system has an exclusive automation system from the SIMATIC S7-400 series that can be used in all domains due to its versatility. The AS 410F/FH automation systems, which can be used from SIMATIC PCS 7 V8.0+SP1, were developed exclusively for the SIMATIC PCS 7 process control system. At its heart is the innovative CPU 410-5H Process Automation, whose automation performance can be increased with expansion cards for 100 PO, 500 PO, 1 000 PO, 1 600 PO and ≥ 2 000 PO (PO 2k+) can be graduated.

With its powerful hardware and optimized firmware as of V8.0, this is able to map the entire performance spectrum of the AS 412F/FH, AS 414F/FH, AS 416F/FH and AS 417F/FH, which can be scaled via the CPU type. It is equipped with one interface each for PROFINET IO (2-port switch) and PROFIBUS DP. 16 MByte RAM each for program and data as well as 48 MByte load memory are already integrated. Two prepared slots enable the synchronization of two redundant subsystems via sync modules and sync lines (fiber optic cables).

Other features:

- Cycle time up to 10 ms/9 Process Tasks
- Up to 7 500 I/Os at DP and PN interface (16 KByte each for inputs and outputs)
- Printed circuit board protection through coating (conformal coating)
- Fanless operation up to 70°C ambient temperature
- High precision time stamping
- Recessed RESET button
- Preset hardware parameters (PCS 7 Skinning)

3 Safety-related hardware and **software from SIMATIC**

3.2.2 AS410E F/FH

The SIMATIC CPU 410E offers an optimal single automation solution for applications with a limit of up to 200 process objects. In combination with the CPU 410-5H, the CPU 410E can also be used as a decentralized automation solution, e.g. for highly modular technological modules that can be integrated into the overall plant via plug-and-produce.

	CPU 410E	CPU 410-5H
Working memory (for program and data)	4 MByte	32 MByte
Load memory (integrated, non-volatile)	48 MByte	48 MByte
CPU processing times for bit operations, typ.	7.5 ns	7.5 ns
I/O data	1536 Byte inputs/outputs	16 kByte inputs/outputs
Number of process objects	up to 200	100...2 k+

3.2.3 Controller series S7-400 F/FH

Safety-related controllers of the SIMATIC S7-400 series are very robust and feature high processing and communication performance. Depending on the configuration, they can be operated either with one CPU (single-channel) or with two redundant CPUs.

In the context of SIMATIC PCS 7, they are available as ready-assembled and tested AS-Bundles. These can be categorized as:

- AS Single Station with only one CPU (safety-related):
  - AS 412F
  - AS 414F
  - AS 416F
  - and AS 417F
- AS Redundancy Station with two redundant CPUs (safety-related and fault-tolerant):
  - AS 412FH
  - AS 414FH
  - AS 416FH
  - and AS 417FH

In the safety-related AS-Bundles, the controller hardware is combined with the safety functions of S7 F Systems.

By selecting preconfigured order units, the equipment of the AS-Bundles as well as their order number can be defined interactively. A configurator offered in the Industry Mall on the Internet (www.siemens.com/industrymall) supports you in this process.

3 Safety-related hardware and **software from SIMATIC**

3.3 Safety-related distributed I/O systems

The SIMATIC PCS 7 process control system offers a wide range of options for the acquisition and output of process signals via sensors and actuators as well as for the connection of process peripherals to the automation systems, for example via signal and function modules in remote I/O stations on the fieldbus:

- PROFIBUS DP (ET 200M, ET 200iSP)
- PROFINET IO (ET 200SP HA, ET 200M)

3.3.1 SIMATIC ET 200SP HA

The SIMATIC ET 200SP HA modular distributed I/O system impresses with its particularly easy handling during installation and assembly. The new terminal arrangement and push-in technology enable tool-free wiring. The SIMATIC ET 200SP HA is suitable for demanding safety and standard applications in the process and manufacturing industries, where high availability and R1 are essential. With digital F I/O modules, the proven advantages of the powerful I/O system can also be used in process safety applications.

Highlights:

- Certified up to SIL 3
- Highest availability (power supply, PROFINET, I/O modules)
- Extended temperature range: -40°C to +70°C horizontal
- Installation up to Ex zone 2
- Module replacement and firmware update during operation
- Electronic nameplate with identification and maintenance data (I&M data) available

In addition to the possibility of operating the SIMATIC ET 200SP HA station redundantly via the PROFINET interface, the distributed I/O modules themselves can also be designed redundantly. This is implemented in a very space- and cost-saving way via a terminal block for integrated I/O redundancy. The new design technology with standardized terminal blocks makes redundant wiring as easy as in single operation.

ET 200SP HA with redundant interface

3 Safety-related hardware and **software from SIMATIC**

The following fail-safe distributed I/O modules are available for fail-safe applications based on SIMATIC Safety Integrated for Process Automation:

- Digital input module F-DI 16x24VDC HA with
  - 16 fail-safe digital inputs (SIL 3/Cat.4/PLe);
  - Internal short-circuit proof encoder supply for each channel;
  - Open-circuit monitoring and short-circuit monitoring (sensor supply) channel by channel.
- Digital output module F-DQ 10x24VDC/2A PP HA with
  - 10 fail-safe digital outputs (PP-switching, SIL 3/Cat. 4/PLe);
  - Short circuit and overload protection;
  - Short circuit, overload and wire break monitoring;
  - IO redundancy support.
- Analog input module F-AI 8x0/4...20 mA HART HA with
  - 8 fail-safe analog inputs (SIL 3/Cat.4/PLe);
  - Short-circuit proof sensor supply for 2- or 4-wire sensors per module;
  - Configurable input signal range per channel: 0 to 20 mA / 4 to 20 mA;
  - Output current for sensor supply: max 30 mA;
  - Configurable open-circuit and short-circuit monitoring;
  - HART support;
  - IO redundancy support.

3.3.2 SIMATIC ET 200iSP

The ET 200iSP remote I/O stations can be installed directly in Ex zones 1, 2, 21 or 22 as well as in non-hazardous areas in accordance with ATEX Directive 94/9/EC. When installed in Ex zones 1 or 21, the RS 485-iS coupler serves as a barrier. The intrinsically safe sensors, actuators and HART field devices can also be placed in zone 0 or 20 if required.

Thanks to the modular architecture, ET 200iSP stations can be flexibly configured and expanded. Availability can be increased by redundant design of the pressurized power supply and the interface modules.

Terminal modules mountable on an S7-300 profile rail serve as carriers for the different module types. Automatic slot coding and “standing wiring” enable the simple and safe exchange of individual modules during operation (“hot swapping”) without firing. Wiring and wiring test are already possible in advance without the electronic modules.

ET 200iSP

3 Safety-related hardware and **software from SIMATIC**

The range of electronic modules includes analog and digital I/O modules for the automation of the technological functions of the process (Basic Process Control) as well as safety-related F I/O modules for the implementation of safety applications. The different types of electronic modules can be arranged mixed within one station.

Up to 32 electronic modules can be inserted between the interface module and the termination module. The station thus has a width of 107 cm. However, the number of electronic modules that can be operated in a station may be limited depending on the current consumption of the modules used. However, up to 16 electronic modules can be plugged in without restriction.

F signal modules for SIMATIC ET 200iSP

The F I/O modules equipped with safety functions implement the safety applications in cooperation with the safety-oriented controllers (automation systems). The input modules acquire the process signals, evaluate them, and prepare them for further processing by the automation system. The output modules convert the safety-related signals output by the automation systems so that they are suitable for controlling the connected actuators.

3.3.3 SIMATIC ET 200M

SIMATIC ET 200M offers maximum benefit for complex user-specific automation tasks. An ET 200M station can accommodate up to 12 I/O modules in S7-300 configuration technology. When using active bus modules, modules can be exchanged and expanded during operation (hot swapping).

The following safety-related F modules can be used in applications up to SIL 3 and can be mixed without restriction with standard modules in a station without a separating module:

- SM 326 F-DI 24 × DC 24 V
- SM 326 F-DO 10 x DC 24 V, 2 A
- SM 326 F-DO 8 x DC 24 V, 2 A
- SM 336 F-AI HART 6 x 0/4...20 mA

3 Safety-related hardware and **software from SIMATIC**

3.4 Safety Engineering

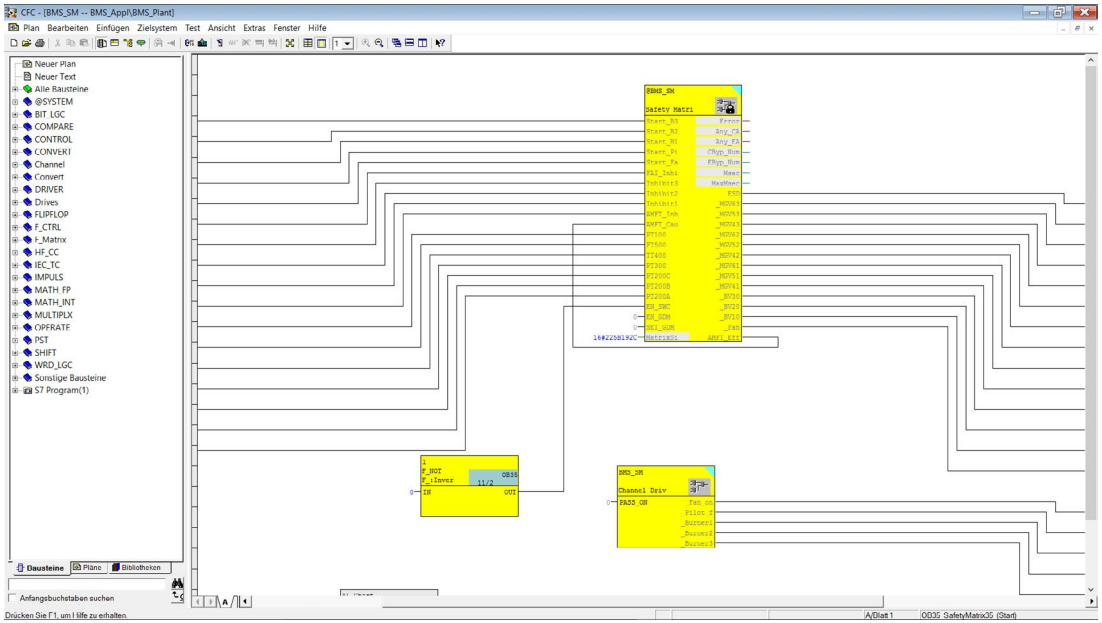
The F function block library in S7 F Systems and the SIMATIC Safety Matrix are available for configuring and programming the safety-related controllers.

3.4.1 SIMATIC S7 F Systems with F-Block Library (CFC Programming)

The S7 F Systems engineering tool enables the parameterization of the safety-related controllers as well as the safety-related F modules from the ET 200 range. It supports project planning with functions for:

- Comparing safety-related F programs
- Detection of F program changes by checksum
- Separation of safety-related functions and standard functions

Access to the F functions can be protected by a password. The F function block library integrated in S7 F Systems contains ready-made function blocks for creating safety-oriented applications with the CFC or the safety matrix based on it. The certified F blocks are very robust and catch program errors such as division by zero or value overflow. Complex programming for error detection and error reaction is not necessary and saves time and effort.

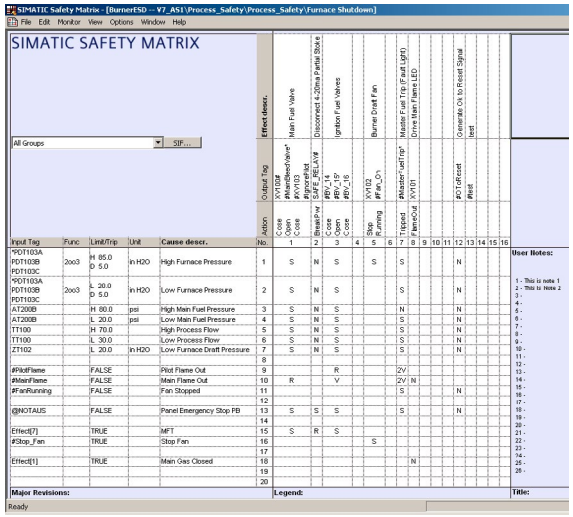


3 Safety-related hardware and **software from SIMATIC**

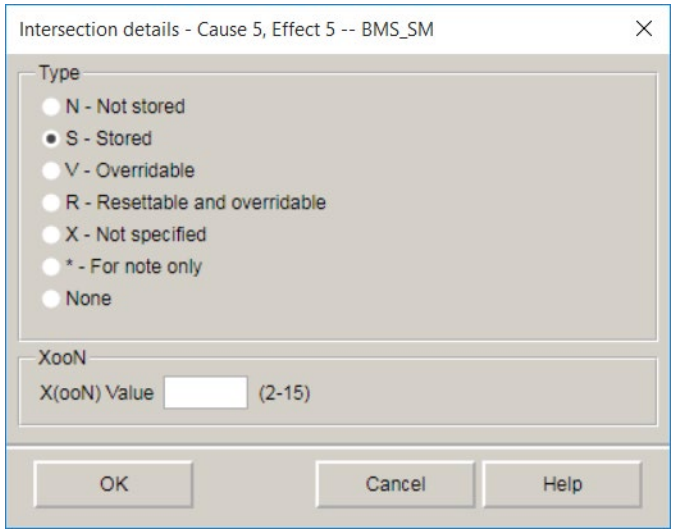
3.4.2 The safety lifecycle management tool Safety Matrix

With SIMATIC S7 Safety Matrix, Siemens offers a TÜV-certified safety lifecycle management tool for safety applications up to SIL 3 according to IEC 61508. SIMATIC S7 Safety Matrix consists of the following individual products, which differ in terms of functionality and area of application:

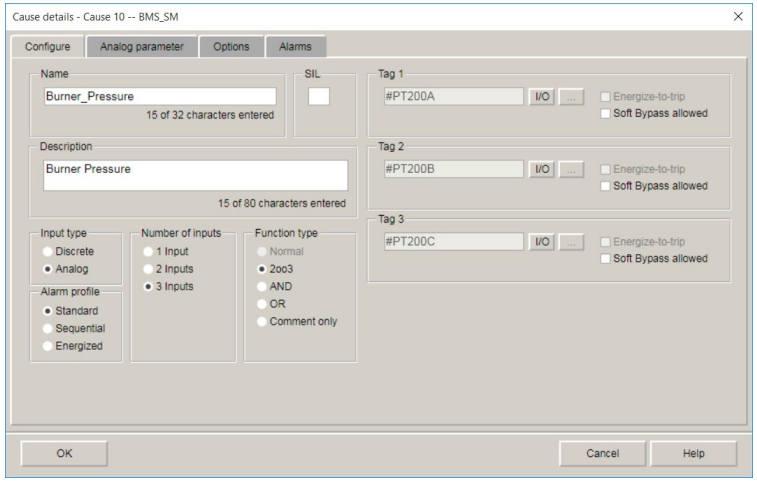
- Safety Matrix Engineering Tool
- Safety Matrix Viewer



Safety Matrix Editor



Definition of the operations and functions forming the cause logic



Definition of a cause

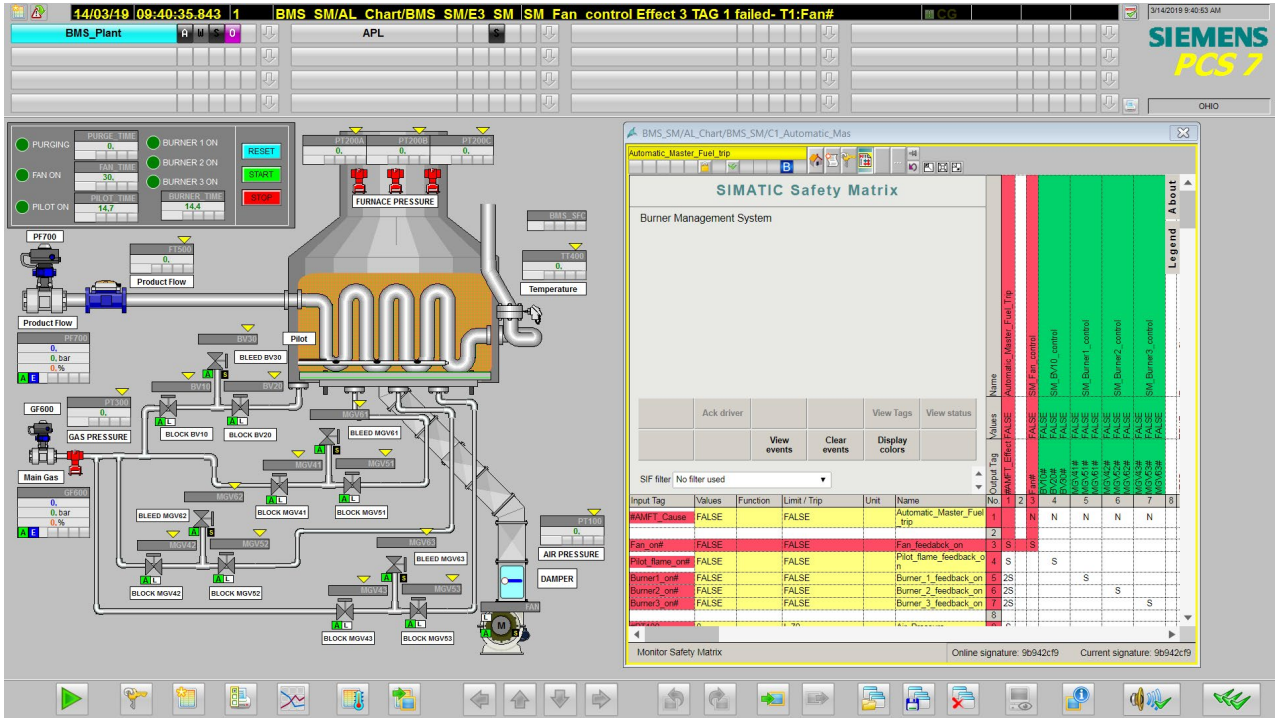
3 Safety-related hardware and **software from SIMATIC**

The consistent use of the SIMATIC Safety Matrix in all phases of the safety life cycle reduces investment and operating costs.

Advantages Safety Matrix at a glance:

- No programming knowledge required
- Generally understandable for all parties
- Identical display of the matrix in configuration, operation and documentation
- Reduction of planning, implementation and acceptance times
- Optimal operator guidance
- Less downtime

Extensive information on the application and on the use of the Safety Matrix, which ensures benefits throughout the entire life cycle, can be found in the following brochure.



SIMATIC S7 Safety Matrix Viewer

4

Safety applications

4 Safety applications

Maximum safety, high availability, and low maintenance requirements

The innovative Siemens safety concept gives the user a choice regarding the degree of integration between the safety instrumented system (SIS) and the basic process control system (BPCS). If the physical separation of BPCS and SIS is not dictated by appropriate regulations, a common architecture with BPCS and SIS functionality in the same control system can be advantageous: reduced space requirements, minimized necessary hardware and wiring, and potentially lower assembly, installation, and engineering fixed costs – i.e., significant overall cost savings over the entire life cycle of the plant. Despite physical coexistence of functions, this common architecture still achieves the necessary logical separation that meets the requirements of functional safety standards such as IEC 61511.

The safety system is usually referred to as an Emergency Shutdown (ESD) or Process Shutdown (PSD) system. ESD systems shut down partial areas in an emergency, while PSD systems shut down an entire process or plant and thus transfer it to a safe state. This is backed up by safety-related applications such as burner controls, pressure monitoring, level monitoring, etc. All these applications operate according to the closed-circuit current principle – so-called “de-energized-to-trip” – which means that the de-energized state is the safe state. In contrast, energized-to-trip requires energy to reach the safe state. Examples are fire & gas applications or sprinkler systems. On the following pages you will find the most commonly used applications in the process industries.

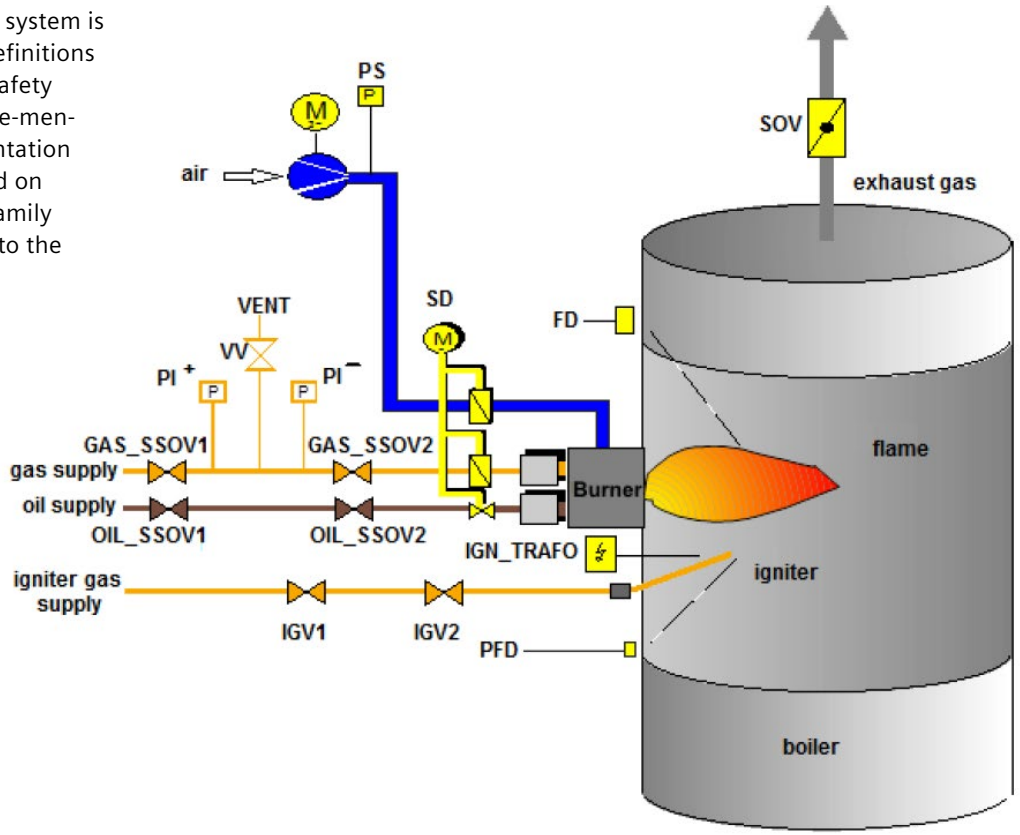
4.1 Burner Management System (BMS)

A burner management system (BMS) is an automated safety system consisting of field devices (sensors), logic systems and actuators. It secures the operation and service of firing systems in boilers, furnaces, and combustion chambers. From start-up to monitoring to shutdown of the firing process, the BMS is designed for absolute safety. Power generation, thermal power plants, district heating, pulp and paper, heat treatment and other processes in the chemical, petrochemical, oil and gas industries use BMS applications. BMS systems are used in numerous process applications such as boilers, thermal oxidizers, waste incinerators, blast furnaces and kilns.

A BMS safely starts up the burner and igniter, monitors flame conditions during operation, and properly deactivates the burner and igniter when necessary. This involves monitoring and controlling the combustion chamber venting, fuel supply, flame, and all field devices in the system. Burner startup is prevented until the necessary conditions, such as venting, have occurred. During startup and normal operation, the BMS monitors various safety interlocks to ensure safety. In case of problems, the BMS shuts down the burners to bring the process to a safe state and informs the operator accordingly.

4 Safety applications

However, if you want to operate a BMS, you face some challenges. For example, there are many application-specific standards that relate to burner management systems, the applicability of which depends on the site of operation and the type of plant being fired. These application-specific standards are mandatory and include, for example, U.S. standards such as NFPA 85, NFPA 86, NFPA 87, API 556, and European standards such as EN 230, EN 298, EN 746, EN 50156 and EN 12952-8. A burner management system is a safety instrumented system (SIS) based on the definitions of IEC 61511:2016, which describes the required safety functions. In addition to compliance with the above-mentioned standards, the trend in BMS is towards orientation towards performance-based safety standards based on IEC 61508, IEC 61511, and ISA S84. The SIMATIC family of fail-safe controllers is designed to be adaptable to the aforementioned mandatory application standards for a BMS and to meet the requirements. They are both IEC 61508:2010 certified and suitable for use in applications up to SIL 3. This further considers the trend to create and apply SIL concepts according to IEC 61511 and ISA 84.



4 Safety applications

4.2 Automatic overfill protection

Safety is of paramount importance in the storage and transfer of hydrocarbons. Any failure can endanger people, the environment, the plant, and its operation. The best practice solution for storage tank monitoring combines the existing API 2350 standard with the IEC 61511 standard on functional safety. In many regions, automatic overfill prevention with corresponding instrumentation (overfill prevention device, OPD) is mandatory. Siemens offers complete solutions – from safety instrumentation for level measurement to safe automation and safety-related positioners. The tank overfill prevention system reliably detects an overfill situation in the tank and takes appropriate action to prevent overfilling (e.g., by closing a valve to stop the flow into the tank). In addition, an alarm should be triggered to warn the operator.

It is recommended that these safeguarding systems be classified as safety-related systems and assessed, implemented, operated, and maintained according to their risk in accordance with the requirements of the best practice functional safety standard IEC 61511. In the U.S., these recommendations were also incorporated into the 4th version of the API 2350 standard. As a result of best practice, these safety systems must be expected to run separately and independently from the associated level measurement and control systems, and to operate automatically so that operator intervention is no longer required.

A tank overfill protection system can be used in individual tanks, small tank groups or extensive tank farms, such as those found in large ports and fuel depots. Tank farms are often spread over a large area, so it must be possible to set up automation and safety in a decentralized manner without any problems. Often, the technology also must be installed in potentially explosive areas.

4 Safety applications

There are different strategies for this, for example:

- Each tank can be permanently connected to a central control room.
- Centrally placed controls with distributed I/Os in the field are available for each tank or tank group.
- Controls and distributed I/Os can be placed decentrally at each tank or tank group.

Sometimes it can be useful to combine control and safety in the same dedicated safety system while maintaining performance and functional independence. Especially when using a decentralized control and safety strategy, this can reduce the number of SIS required. To meet the requirements of IEC 61511, it is important that the system provides the necessary logical separation to ensure that control tasks do not interfere with safety-related functions.

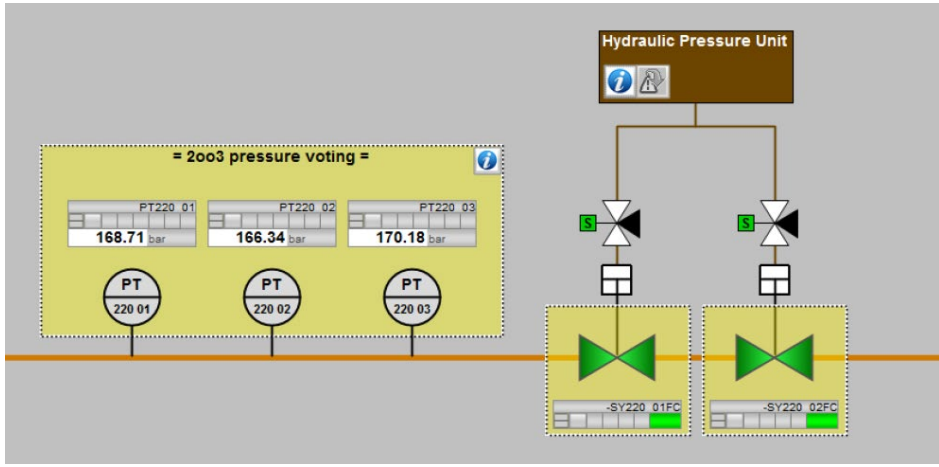
Especially for tank overfill protection, Siemens offers with AS 410FE and AS 410FHE a flexible, cost-effective, and reliable solution that can be used with our own range of process instruments as well as with a variety of sensors from other manufacturers.

4 Safety applications

4.3 Safety Shut-off Devices: High Integrity Pressure Protection Systems (HIPPS)

Overpressure protection must be ensured at wells and for downstream process equipment, pipelines or gas manifolds. HIPPS are installed to ensure overpressure protection for process equipment upstream and downstream. To avert overpressure scenarios and minimize the consequences that may be associated with them, HIPPS could be used to shut off, reduce, or divert overpressure sources. Damage to equipment or leakage of toxic and environmentally harmful liquids or gases is thus prevented. While a traditional relief system aims to remove any excess inflow, a HIPPS stops the inflow of excess liquids or gases, ensuring that no overpressure occurs. The use of a HIPPS can also help dramatically reduce the likelihood of overloading the existing conventional pressure relief system. This can eliminate high costs that would be associated with the purchase of new relief devices. Accordingly, the flare systems used can be sized much smaller. More generally, a HIPPS helps to minimize costs due to operational downtime.

HIPPS are safety systems designed and built in accordance with the IEC 61508 and IEC 61511 standards. As a Safety Instrumented Function (SIF), they usually consist of sensors, a logic solver, and actuators. Nowadays, most transmitters are electronic. Their task is to detect the impermissible pressure. The logic unit processes the input from the sensors into an output to the actuators, which perform the actual corrective action in the field by moving the process to a safe state. Typically, three sensors are connected to the logic solver, which is configured to form a 2oo3 system. This configuration is preferred for HIPPS as it ensures both availability and reliability of the system.



4 Safety applications

4.4 Fire and Gas (F&G)

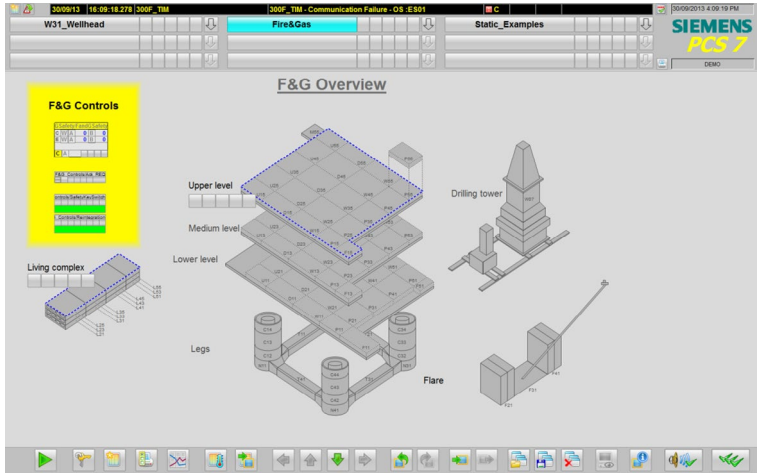
Systems for protection against fire and gas play an important role in the overall protection concept of industrial plants for the production and processing as well as the transport of crude oil, petrochemicals or hazardous gases. They must reliably detect and report fires and/or gas leaks, even under adverse conditions such as failure of the main power supply. To mitigate the consequences of damage, they are also partially capable of automatically initiating appropriate countermeasures, including extinguishing a fire or extracting a gas. The Safety Integrated System is certified to the required safety standards for this purpose. F&G applications are all about detecting and fighting fire outbreaks or gas leaks. The potential risk to people and the environment requires safety implementation in accordance with the higher-level safety standard of IEC 61511 “Functional safety in the process industry sector”. Compliance with specific standards is also required, such as EN 54-2 “Fire detection and fire alarm systems – Part 2: Control and indicating equipment” and NFPA 72 “National Fire Alarm and Signaling Code”.

The special feature of F&G is the operating principle of disconnection that often occurs here. The closed-circuit current principle is used for safety-related ESD and PSD shutdowns. The good state of the safety-instrumented function (SIF) is the switched-on state. In the event of a hazard, the SIF must be switched to the de-energized to trip (DTT) state. In F&G, however, the extinguishing devices are switched on, for example, in the event of firefighting. This is therefore the energized to trip (ETT) principle.

In addition to the safety-related processing, this shutdown reaction also includes a requirement for the availability of the shutdown. Thus, components and system parts must be designed redundantly to be able to react safely and available in case of demand. In addition, integrated diagnostics and line monitoring are required.

The SIMATIC Safety System fulfills the shutdown in both directions and is certified for this by TÜV SÜD up to SIL 3. In a single-channel safety architecture, the system can switch off the SIF in applications up to SIL 3 (DTT). By using redundant power supplies and controllers as well as redundant safety-related outputs, the SIMATIC Safety System can also safely switch on the SIF up to SIL 3 (ETT). This flexibility allows the implementation of different SIF architectures such as 1oo1, 1oo2, 2oo3, 2oo4 and NooM as well as safe switch-on and switch-off (2oo2).

Pictures of the F&G solution



Initial screen Oil and Gas Platform with the Fire and Gas Application

5

Certificates and documents

5 Certificates and documents

Here you will find a compilation of important or further documents on the subject. The issue status of the information corresponds to the issue status of the brochure. Updates of individual brochures and documents at a later date are possible.

5.1 TÜV certificates, reports and documents SIMATIC S7 F/FH Systems

(No. Z10 020080 006) https://support.industry.siemens.com/cs/ww/en/view/109482252

Overview of the TÜV certificates relevant for SIMATIC S7 F/FH Systems and the associated reports and appendices: https://support.industry.siemens.com/cs/ww/en/view/73192008

5.2 Brochures and manuals

Process Safety brochure : https://assets.new.siemens.com/siemens/assets/api/uuid:d8d5adf3-002a-4706-a995-a5272364cbbe/Alt-DIPA-I10297-00-7600-Anlagen-prozesssicherheit-ipdf-en_original.pdf

Safety Matrix brochure: https://assets.new.siemens.com/siemens/assets/api/uuid:237016c6-0f83-456e-8f75-60a3f99b4a55/safety-matrix-flyer-final.pdf

CPU410-5H: https://support.industry.siemens.com/cs/ww/en/pv/6ES7410-5HX08-4AB0/td?dl=en

SIMATIC S7 F/FH Systems: https://support.industry.siemens.com/cs/ww/en/view/109773062

ET 200SP HA: https://support.industry.siemens.com/cs/ww/en/view/109802478

ET 200SP HA F-DI: https://support.industry.siemens.com/cs/ww/en/view/109780930

ET 200SP HA-F-DQ: https://support.industry.siemens.com/cs/ww/en/view/109780931

ET 200SP HA F-AI: https://support.industry.siemens.com/cs/ww/en/view/109802504

ET 200iSP Fail-safe modules: https://support.industry.siemens.com/cs/ww/en/view/47357221

ET 200M Fail-safe modules: https://support.industry.siemens.com/cs/ww/en/view/19026151

SIMATIC PCS 7 Compendium Part B: https://support.industry.siemens.com/cs/ww/en/view/109757545

5 Certificates and documents

5.3 Security certificates and documents

5.3.1 Certificates

https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html

5.3.2 Brochures and manuals

SIMATIC CPU 410 Security Certification:	https://support.industry.siemens.com/cs/ww/en/view/109780143
Network Security Brochure:	https://support.industry.siemens.com/cs/ww/en/view/109766269
SIMATIC PCS 7 Compendium Part F:	https://support.industry.siemens.com/cs/ww/en/view/109766269
SIMATIC PCS 7 Safety Concept PCS 7 & WinCC (Basis):	https://support.industry.siemens.com/cs/ww/en/view/60119725
Cybersecurity – Defense-in-Depth concept for the water and wastewater industry:	https://support.industry.siemens.com/cs/ww/en/view/109780322
PROFINET in process automation with SIMATIC PCS 7:	https://support.industry.siemens.com/cs/ww/en/view/72887082

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article No.: DIPA-I10297-00-7600

siemens.com

Subject to changes and errors. The information provided in this brochure contains descriptions or performance characteristics which, in case of actual use, do not always apply as described or which may change as a result of further development of the products. The desired performance characteristics are only binding if expressly agreed in the contract. Availability and technical specifications are subject to change without notice.

All product designations may be trademarks or product names of Siemens AG or supplier companies, the use of which by third parties for their own purposes may violate the rights of the owners.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement and continuously maintain a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit

www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

www.siemens.com/industrialsecurity.