Safety Integrated for Process Automation

Safety Integrated

Brochure
August 2014

Answers for industry.
In the light of the growing complexity of machines and plants along with rising engineering costs, efficient engineering is a key factor for success in the manufacturing industry.

Totally Integrated Automation, industrial automation from Siemens, makes engineering efficient. The open system architecture that covers the entire production process ensures the efficient interaction of all automation components. This is guaranteed with consistent data management, global standards, and uniform hardware and software interfaces. These common features minimize the engineering overheads. This reduces costs, shortens the time to market and increases flexibility.

The holistic approach of Totally Integrated Automation paves the way for better production: faster, more flexible, and more intelligent. This, in turn, is the basis for real added value in all automation tasks, particularly:

- Integrated engineering
- Industrial data management
- Industrial communication
- Industrial security
- Safety Integrated

Totally Integrated Automation creates the perfect framework for strategically harnessing optimization potential – throughout the entire production process:

- Time and cost savings thanks to efficient engineering
- Non-productive times minimized thanks to integrated diagnostic functions
- Greater flexibility in production thanks to integrated communication
- Plant and network security thanks to integrated security functions
- Protection of personnel, machinery, and the environment with seamlessly integrated safety technology
- Improved quality thanks to data consistency
- Simplified implementation of automation solutions with global standards
- Better performance with the interaction of system-tested components
In the context of Totally Integrated Automation, Safety Integrated ensures reliable protection for personnel, machinery, and the environment – alongside maximum efficiency and flexibility. The comprehensive safety portfolio of control, drive and switchgear technology meets all functional safety requirements for plants and machines, and offers professional support and expertise for all safety needs.

Safety Integrated is the seamless integration of safety technology into standard automation. This offers key benefits for both machine manufacturers and plant operators: significant reductions in engineering costs, greater availability, and system consistency. In precise terms, this means: Safety Integrated enables the faster and simpler realization of safe and productive plants and machines.

Through the integration of safety functions in TIA, standard automation (basic process control system) and safety-related automation are combined in a uniform complete system. Common hardware, engineering and management components can be utilized for the automation of continuous and discontinuous processes, faster and more precise control procedures and integrated safety functions.
Safety engineering from Siemens
Process automation with integrated safety

The ongoing protection of people, plants and the environment is essential for long-term success. This is why staff at Siemens are constantly working on products and services to improve process and plant safety and security. Our experts are familiar with both the statutory regulations and the safety engineering standards, and actively study and implement the latest provisions. Meeting these requirements demands advanced safety, availability and maintenance concepts.

Safe production without weak points

In the process industry where procedures are often extremely complex, there can be no weak points in the automation systems. Any fault or malfunction can have fatal consequences. The minimization of potential danger to personnel, plants and the environment using technical tools must therefore be the top priority – but without this affecting the industrial production process.

In order to reliably eliminate sources of danger and minimize risks, you require an efficient safety engineering concept that meets the high demands of functional safety.

One key aspect of any modern plant safety concept is the safety instrumented system (SIS). This system is based on a combination of standard automation and drive components with additional safety functions. The result is Safety Integrated – a comprehensive portfolio for the simple implementation, operation and maintenance of safe applications.

Completely integrated in the standard automation

SIMATIC S7-400 F/FH controllers with the corresponding I/O offer a maximum degree of safety, fault-tolerance and availability for your applications. PROFIBUS and PROFINET provide the latest fieldbus technology for efficient communication between the controller and distributed I/O – right down to the individual field device and for zone 1 and zone 2 potentially explosive atmospheres.

Engineering, commissioning and maintenance costs can be significantly reduced using the safety lifecycle management tool SIMATIC Safety Matrix. Linking cause and effect makes configuring safety applications simple and easy.

Functions for the partial stroke test make it possible to check the operation of the emergency shutdown valves during runtime, which improves plant safety. Maintenance intervals can even be extended with no changes in risk.

Seamless integration of all of these products into the SIMATIC PCS 7 process control system makes highly efficient and flexible automation and safety applications possible. SIMATIC PCS 7 adds comprehensive IT security to the integrated process safety.
Your requirement defines the solution

Extreme operating conditions require special solutions. Hardened and coated components are also available for use in extended temperature ranges, at high levels of relative humidity, in corrosive environments and in applications subject to high mechanical loads.

Drive technology products – safety relays, motor management systems (MCC), frequency converters, motors and gears – are designed to meet the strictest of safety standards. A wide range of explosion-protected motors are available for potentially explosive gas and dust atmospheres.

With excellent products and decades of experience, we can also implement top-quality solutions for specific tasks. These can range from plant monitoring to fire protection all the way to communication technology and access control.

SIMATIC PCS 7 safety & security

Advanced standardization, openness and global networking are unfortunately also associated with increased cyber criminality. Numerous threats result due to malware or unauthorized persons, e.g.:

- Overloading or failure of networks
- Espionage and stealing of access or process data
- Unauthorized interventions in the process automation
- Direct sabotage

In order to protect plants containing the SIMATIC PCS 7 process control system, Siemens has developed an extremely effective holistic safety concept which links together a wide range of security measures that are continuously upgraded. This defense-in-depth concept operates at three levels:

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

The security measures for process automation with SIMATIC PCS 7 based on this defense-in-depth concept are described in detail in the "Security concept PCS 7 and WinCC - Basic Document" manual.

With its Industrial Security Services, Siemens also facilitates the development of customized security solutions for the entire lifecycle of the plant. The services include a detailed security assessment, the selection and implementation of the best measures, and updates and risk adjustments.

However, absolute safety cannot be guaranteed even with all the known protective measures. By combining SIMATIC PCS 7 IT security with safety engineering, you can nevertheless neutralize the effects of cyber criminality.

Additional information can be found on the Internet at: www.siemens.com/industrial-security
Standardized and flexible safety products

A complex network of standards and regulations requires...

As plant owner you are obliged by law to achieve the highest possible levels of safety for people and the environment. To achieve this, all rules, directives and regulations must be applied at the plant location. A danger and risk analysis must be carried out if a potential danger exists. This then describes the existing risks, and the current and additional measures to reduce them are defined. The residual risk must always be below the tolerable degree.

Complete and comprehensive documentation (e.g. a safety plan) must be drawn up for the complete lifecycle, in other words from analysis to implementation, operation and decommissioning of the plant. This facilitates fault diagnostics as well as the repeatability of all processes, and serves as proof should damage ever occur.

The required availability must also be ensured. Flexible and scalable redundancies can be implemented easily and inexpensively with the flexible modular redundancy (FMR) of the Siemens safety-instrumented system.

... and a reliable partner helps you to comply with all requirements.

For more than 25 years now, Siemens has been implementing first-class automation solutions for process safety in a wide range of sectors as a reliable industrial partner. These solutions are highly efficient and offer significant savings. Of course, they also comply with the applicable national and international standards such as IEC 61508 (up to SIL 3), ANSI/ISA-84 and IEC 61511.

IEC 61508 – basic standard

IEC 61508 defines methods to achieve the functional safety of products. Compliance with it is verified by corresponding certificates. The standard is globally applicable, and serves as the basis for specifications and for the drafting and operating of safety instrumented systems.

IEC 61511 – application-specific standard for the process industry

IEC 61511 implements IEC 61508 for the process industry. It mainly serves as a guideline for planning, implementing and operating safety instrumented systems in process engineering plants. A decisive component: the demand for higher-level organization of all sequences (Functional Safety Management, FSM).

IEC 61511 requires safety verification for the complete safety loop from the sensor to the controller and actuator. This covers not only the individual hardware and software products, but also all planning, operation and change processes implemented during the lifecycle of the plant.

Application-specific standards

- Burner systems
  - EN 230: Automatic burner control systems for oil burners
  - EN 298: Automatic burner control systems for gas burners and gas burning appliances with or without fans
  - EN 50156-1: Electrical equipment for furnaces and ancillary equipment - requirements for application design and installation
  - NFPA 85: Boiler and Combustion Systems Hazards Code
- Fire detection and fire alarm systems
  - EN 54-2/A1: Fire detection and fire alarm systems – control and indicating equipment

Safety Integrity Level (SIL)

IEC 61508 and IEC 61511 define four different Safety Integrity Levels. The higher the SIL, the larger the reduction in risk expected of the Safety Instrumented Function. The SIL is thus a measure of the probability that a Safety Instrumented Function will work correctly and bring the process to the safe state when there is a demand.
Integration for greater efficiency

Simple integration into control system

The innovative safety-instrumented system can be connected to any digital control system (DCS). It comprises safety-related components from the following product range:

- SIMATIC S7-400 (F/FH) controllers, e.g. the SIMATIC PCS 7 AS 410 automation system
- SIMATIC ET 200M, ET 200iSP, ET 200S and ET 200pro distributed I/O
- SITRANS, SIPART and SIMOCODE process instruments/devices

The facility for integration into the innovative SIMATIC PCS 7 process control system is unique here. This combination allows shorter engineering times, a better operating performance, savings in the stocking of spare parts, and lower total maintenance costs.

Common interfacing using proven standards

The proven PROFIBUS and PROFINET fieldbus technologies are used when connecting standard and safety-related I/O modules/submodules and devices. Safety-related communication and standard communication use the same bus medium. This also applies to the interfacing of fail-safe pressure transmitters, for example the SITRANS P DS III to PROFIBUS PA with PROFinet according to SIL 2.

Safety Integrated fieldbus technology with PROFinet enables certified, safety-related communication between F/FH controllers, distributed safety I/O and safety-related process instruments. Redundancy or ring topologies at all levels of fieldbus communication allow maximum availability.

Advantages at a glance

- One engineering system for process control and process safety applications
- A common controller platform for process automation and process safety
- Direct and seamless communication between DCS and SIS
- Automatic integration of various safety-related alarms and messages with time stamps
- Considerable cost savings
Safety Integrated for process automation – the comprehensive range of products and services

The safety instrumented system from Siemens comprises safe controllers, safe bus systems and I/O as well as the safe instrumentation, for example for pressure measurements.

With Safety Integrated, we can offer first-class, comprehensive and uniform solutions for the process and production industries on this basis, and combine these with excellent services for all life phases of a safety instrumented system.

In the following detailed presentation of Safety Integrated, we limit ourselves to the process industry.

On the basis of our complete range and decades of experience, we can implement first-class automation solutions for process safety. Our comprehensive range of offers includes:

- Emergency and process shutdown systems (ESD/PSD) according to IEC61511, S84
- Burner management systems (BMS) according to EN298, NFPA 85
- Fire and gas applications (F&G) according to EN 54, NFPA 72

Additional information on Safety Integrated for Process Automation is available on the Internet: www.siemens.com/simatic-pcs7/process-safety
## Range of products for the process industry

| Engineering | Configuration of safety functions (up to SIL 3) using TÜV-certified function blocks and Continuous Function Chart (CFC) or SIMATIC Safety Matrix (Cause&Effect matrix) |
| Automation systems | Fail-safe, fault-tolerant controllers with a redundant or non-redundant design (SIL 3) for the bottom, mid and top performance ranges |
| PROFIsafe with PROFIBUS/PROFINET | For standard and safety-related communication on just one bus cable, certified according to IEC 61508 (SIL 3) |
| SIMATIC ET 200M | Modular I/O for multi-channel applications with safety-related signal modules (F-DI, F-DO, F-AI), SIL 2/SIL 3; IP20 degree of protection |
| SIMATIC ET 200iSP | Modular, intrinsically-safe I/O with safety-related electronic modules (F-DI Ex, F-DO Ex, F-AI Ex), SIL 3, IP30 degree of protection |
| SIMATIC ET 200S | Bit-modular I/O with safety-related electronic modules (F-DI, F-DO) and safety-related motor starters, SIL 2/SIL 3; IP20 degree of protection |
| SIMATIC ET 200pro | Modular, very compact I/O with safety-related electronic modules (F-DI, F-DI/F-DO), SIL 2/SIL 3; F-switch for switch-off of standard I/O and control of motor switches; IP65/66/67 degree of protection |
| Process instruments/process devices | Safe process instruments/devices on PROFIBUS: SITRANS P DS III PA pressure transmitters (SIL 2) with PROFIsafe, SIMOCODE pro with DM-F local/PROFIsafe (SIL 3), SIPART PS2 PA (SIL 2) |
| | Safe process instruments/devices for connection to ET 200M remote I/Os: SITRANS P DS III analog/HART (SIL 2), SITRANS TW series (SIL 1), SITRANS TH200/300 (SIL 2), SITRANS TR200/300 (SIL 2), SITRANS LVL200 (SIL 2), SITRANS LR250 HART (SIL 2), SITRANS FC430 (SIL 2), SIPART PS2 2/4-wire (SIL 2) |
| Applications | Partial Stroke Test Predefined function blocks and faceplates for online valve test to enable preventive valve diagnostics without affecting production |
Integrated control & safety

SIMATIC PCS 7 –
complete integration of the safety-instrumented system

Safety Integrated for Process Automation from Siemens allows the best possible type of integration of the safety instrumented system into the process control system. With this common integration, the basic process control system (BPCS) and the safety instrumented system are based on common hardware.

The resulting reduction in space requirements, scope of hardware and wiring, and assembly, installation and engineering overheads results in significant cost savings over the entire lifecycle of the plant.

Thanks to the innovative concept of Safety Integrated, all other integration levels can also be covered.

A distinction is basically made between the following three integration levels:

- **Interfaced**
  The BPCS and the safety instrumented system are based on different hardware, and are connected together by a gateway for data exchange. Engineering for each of the systems is performed via separate engineering tools.

- **Integrated**
  The BPCS in the process control system and the safety-instrumented system are based on different hardware, communication and engineering, but are implemented over standard systems.

- **Common**
  The BPCS and the safety instrumented system are combined in the process control system. They use common hardware (controller, fieldbus, I/O). Standard and safety-related programs are executed in parallel and independent of each other.

The modularity and flexibility of Safety Integrated permit individual definition of the degree of integration. For example, you can decide yourself whether you wish to execute the basic control system functions and the safety functions in one controller (automation system) or in separate controllers.

Many advantages of Safety Integrated can already be used thanks to the fact that this system can be integrated into any open process control system using standardized communication over PROFIBUS/PROFINET IO and Industrial Ethernet. These include:

- Processing of standard and safety functions in the same S7-400 controller
- No separate safety bus: Standard and safety-related communication take place over the same fieldbus (PROFIBUS or PROFINET, each with PROFIsafe)
- Mixed operation of standard and safety-related I/O modules in ET 200M, ET 200iSP, ET 200S and ET 200pro remote I/O stations
Example of a combination of a basic process control system and safety system in SIMATIC PCS 7

However, the maximum potential of Safety Integrated can only be utilized through the unique combination with the universal SIMATIC PCS 7 process control system from Siemens. You then profit from further advantages such as:

- One common engineering system for BPCS and SIS
- A common controller platform
- Integrated data management: No complex data handling between BPCS and SIS
- Integration of safety-related applications into process visualization on the operator station
- Automatic integration of safety-related fault messages with time stamps 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 over the plant bus (with client/server systems also over a terminal bus if necessary) with systems and tools for engineering, process control, plant management, diagnostics and maintenance. In the case of modern, open process control systems, the plant and terminal buses are usually industry-compatible Ethernet LANs.

In the GUI of these systems and tools, the Safety Integrated System is represented by operator-accessible faceplates.

The Safety Integrated system is integrated into the plant bus using rugged Ethernet interfaces in the controllers and Industrial Ethernet switches such as SCALANCE X as suitable for the bus medium used.

The SIMATIC PCS 7 plant bus based on Industrial Ethernet according to the IEEE 802.3 standard is often designed as an optical ring for noise immunity and availability reasons. It can also be configured as a redundant optical ring if very high availability demands exist, and this tolerates double faults such as the failure of a switch on Ring 1 and a simultaneous open-circuit in the bus cable of Ring 2.

The terminal bus of SIMATIC PCS 7 can also be distributed between two redundant rings. Each PCS 7 station is connected to one of two Industrial Ethernet interfaces on each of the two separate rings. The SIMATIC NET SOFTNET-IE RNA communication software on the PCS 7 stations organizes communication processes based on the PRP.
Flexible Modular Redundancy
Cost-optimized safety with flexible and scalable fault tolerance

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

Depending on the automation task and safety requirements, this allows the configuration engineer to define the degree of redundancy individually for each of the architecture levels controller, fieldbus and I/O, and to match it to the field instrumentation. Each component within a level can be provided with a redundant configuration, and also physically separated. All components also meet the requirements of safety integrity level SIL 3.

Fault-tolerant architectures which can tolerate several simultaneously occurring faults can therefore be exactly tailored to specific tasks. As shown in configuration examples with I/O at the PROFINET and PROFINET PA fieldbuses, the sum of the tasks can produce a mix of different degrees of redundancy within one architecture level (1oo1, 1oo2, 2oo3 or 1oo2, 2oo3).

Modeling of the reliability has shown that FMR provides higher availability levels than conventional redundant architectures with a uniform double or triple structure. Since FMR only provides redundancy where it is actually required, more attractive and cost-effective safety applications are possible with FMR than with conventional redundancy architectures.

Advantages at a glance
- Safety not bound to redundancy: Safety Integrated technology provides safety even with single systems
- Redundancy increases availability
- Selection of redundancy matching the Safety Instrumented Function (SIF)
- I/O and field device redundancy independent of CPU redundancy
- No time-limited safety operation in the event of component failure (degraded mode)

Flexible Modular Redundancy (FMR) using the example of a safety-related, fault-tolerant PROFIBUS DP configuration with remote I/Os

FMR using the example of a safety-related, fault-tolerant configuration with direct device interfacing
Safety Integrated fieldbus technology

PROFIsafe – secure communication via PROFIBUS or PROFINET

The PROFIsafe profile allows safety-related communication between the automation system (controller) and the process I/O via both PROFIBUS and PROFINET. The choice of field communication via PROFINET IO or PROFIBUS DP/PA has a significant influence on the architecture of the safety-instrumented system.

The PROFIsafe profile is implemented as an additional software layer within the devices/systems without modifying the communication mechanisms of PROFIBUS or PROFINET. PROFIsafe expands the frames with additional information with which the PROFIsafe communication partners can recognize and compensate for transmission errors such as delays, incorrect sequences, repetitions, losses, faulty addressing or data corruption. The fault detection measures listed in the table are carried out and checked for this purpose in every communication partner.

PROFIsafe communication complies with standards and safety requirements up to SIL 3.

<table>
<thead>
<tr>
<th>Error</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Consecutive number</td>
</tr>
<tr>
<td>Repetition</td>
<td>●</td>
</tr>
<tr>
<td>Loss</td>
<td>●</td>
</tr>
<tr>
<td>Insertion</td>
<td>●</td>
</tr>
<tr>
<td>Incorrect sequence</td>
<td>●</td>
</tr>
<tr>
<td>Data falsification</td>
<td>●</td>
</tr>
<tr>
<td>Delay</td>
<td>●</td>
</tr>
<tr>
<td>Coupling of safety-related messages and standard messages (masquerade)</td>
<td>●</td>
</tr>
<tr>
<td>FIFO faults</td>
<td>●</td>
</tr>
</tbody>
</table>

PROFIsafe fault detection measures of communication partners

Detailed information on PROFIBUS can be found on the Internet at: www.siemens.com/profibus

Detailed information on PROFINET is available at: www.siemens.com/profinet
Safety-related communication via PROFIBUS

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

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

PROFIBUS is ideal here because it enables high-speed communication with the intelligent distributed I/O devices by means of a communications protocol (PROFIBUS DP) as well as communication and simultaneously a power supply for transmitters and actuators (PROFIBUS PA). PROFIBUS is simple, rugged and reliable, can be expanded online by further distributed components, and can be used in both standard environments and hazardous areas.

In addition, it offers versatile facilities for communication and line diagnostics, as well as for diagnostics of the intelligent field devices connected. 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 vendors in one segment (interoperability) as well as the vendor-independent replacement of devices from within a profile family.

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

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

There are two main configuration versions (see figure):

- Single-channel, non-redundant configuration
- Redundant, high availability and fault-tolerant configuration

Examples of safety-related configuration versions with PROFIBUS
At the individual architectural levels (controller, fieldbus, I/O), the configuration alternatives shown in the figure are available depending on the I/O used (ET 200M, ET 200iSP, ET 200S, ET 200pro remote I/O stations or PROFIBUS PA devices with PA profile 3.0 or higher).

With the aid of fieldbus isolating transformers (RS 485-iS coupler) and RS 485-iS electrical transmission technology, PROFIBUS DP can also be run as an intrinsically-safe fieldbus in all environments up to hazardous zone 1 or 21.

The PROFIBUS PA fieldbus developed for direct linking of sensors and actuators is integrated into the PROFIBUS DP over a redundant or non-redundant router. Using a non-redundant router, a PROFIBUS PA of line or tree topology can be implemented on a redundant or non-redundant PROFIBUS DP. Higher availability is achieved by the redundant router in combination with a line or ring topology. A configuration with a redundant router and ring topology is able to tolerate single faults such as the failure of a DP/PA coupler or an open-circuit in the bus cable.

**Active Field Distributors**

With all these configurations, up to 31 PA devices can be integrated into the PROFIBUS PA segment over AFD4, AFD8 or AFDiS active field distributors. The number of field distributors per segment is limited to up to 8 AFD4/AFD8, up to 5 AFDiS or up to 5 AFDiS and AFD4/AFD8 in any combination. An AFD4 can connect up to 4 field devices via short-circuit-proof spur line connections, an AFD8 up to 8, and an AFDiS up to 6.

Active field distributors AFD4/AFD8 can be used in operating environments up to hazardous zone 2/22, and active field distributors AFDiS in operating environments up to hazardous zone 1/21. The AFDiS spur lines can be laid up to zone 0/20 for connecting suitable devices.
Safety-related communication via PROFINET

PROFINET is based on the international standards IEC 61158 and IEC 61784 and combines the advantages of the open network standard, Ethernet, and the PROFIBUS fieldbus system. PROFINET stands for maximum transparency, open IT communication, network security, and real-time communication down to the field level.

Safety-related communication is based on the PROFIsafe profile and is primarily centered on PROFINET IO communication between the automation system (controller) and the process I/O.

Safety-related SIMATIC PCS 7 automation systems from the S7-400 series can be networked simply and effectively with ET 200M remote I/O stations over PROFINET IO. The PROFINET interface of the CPU in the automation system (controller) is used for this purpose. The ET 200M remote I/O stations can be connected either directly via the IM 153-4 PN High Feature interface module or with SCALANCE X switches to PROFINET IO.

A wide variety of network configurations can be implemented based on line, star, tree and ring topologies. Industrial Ethernet products such as SCALANCE X switches and media converters, FastConnect connection elements, and electrical and optical transmission media are used as network components.

In terms of availability, the ring is the first choice both on the AS Single Station (F system) and on the AS Redundancy Station (FH system). On the AS Single Station (F system), media redundancy of the ring means that bus interruptions or failure of a node will not result in failure of the entire segment.

Maximum availability, however, is achieved with a PROFINET ring on an AS Redundancy Station (FH system). Here, the type of PROFINET IO communication referred to as system redundancy enables the I/O devices to establish a communication link to each of the two CPUs over the topological network. In contrast to the single-sided I/O device connection to only one CPU, failure of a CPU in this case does not automatically lead to failure of the connected I/O devices.
Safety-related SIMATIC controllers are used for critical applications in which an incident can result in danger to persons, plant damage or environmental pollution. Working together with the safety-related F-modules of the ET 200 distributed I/O systems or directly via fail-safe transmitters connected via the fieldbus, they detect both faults in the process and their own internal faults and automatically set the plant to a safe state in the event of a fault.

SIMATIC S7-400 safety-related controllers are ideal for implementing safety-instrumented process automation applications. These are capable of multitasking, i.e. several programs can be executed simultaneously in a CPU, whether BPCS (standard) or safety-related applications. The programs function without feedback, i.e. faults in BPCS applications have no effect on safety-related applications and vice versa. Special tasks with very short response times can also be implemented.

Redundant configurations with two CPUs working according to the 1-out-of-2 principle also increase availability. Two subsystems of identical design, electrically isolated from one another to optimize EMC, are synchronized over fiber-optic cables. In the event of a fault, there is a bumpless switchover from the active subsystem to the backup subsystem. The two subsystems can be fitted in the same rack, or fitted up to 10 km apart. Spatial separation provides additional safety gains in the case of extreme effects in the local environment of the active subsystem, e.g. by fire.

SIMATIC S7-300 safety-related controllers can also be used for smaller process safety applications, e.g. burner controls. These controllers are otherwise primarily used in safety-related controls in factory automation.

All controllers referred to are TÜV-certified and comply with the safety integrity levels up to SIL 3 according to IEC 61508. They are able to process BPCS and safety functions in parallel in one CPU. Mutual influencing during the processing is prevented in that the safety-related and BPCS program components remain strictly separated and that the data exchange is executed by special conversion blocks. The safety functions are executed twice in different processor sections of one CPU through redundant, multi-channel command processing. Potential errors are detected by the system during the subsequent comparison of results.

Safety programs being executed on different controllers of a plant can also carry out safety-related communication with each other over the Industrial Ethernet plant bus. Possible communication partners are SIMATIC S7-400 and S7-300 controllers.

I/O connection via PROFIBUS DP

The distributed process I/O can be integrated into a PROFIBUS DP segment either directly or via a lower-level PROFIBUS PA fieldbus. Several PROFIBUS DP segments with distributed process I/Os can be operated on one SIMATIC S7-400 (F/FH) safety-related automation system.

Depending on the type, either one or two PROFIBUS DP interfaces are already integrated into each CPU of the automation system. With additional PROFIBUS DP connections, up to four further PROFIBUS DP interfaces can be configured per CPU.

I/O connection via PROFINET (PN)

SIMATIC S7-400 (F/FH) safety-related automation systems can be networked simply and effectively with remote I/O stations over PROFINET IO, for example with ET 200M. Only the PROFINET interface (2-port switch) integrated in the CPU can be used for this purpose in the automation system.

Configurations with redundant automation systems and “system redundancy” PROFINET IO communication provide maximum availability with minimal fault reaction times. Each I/O device establishes a communication link to each of the two CPUs of the redundant automation system over the topological network.
SIMATIC S7-400 controller series

SIMATIC S7-400 safety-related controllers are extremely rugged, and are characterized by high processing and communication performance. They can be operated either with one CPU (single-channel) or with two redundant CPUs, depending on the configuration.

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

- AS Single Station with only one CPU (safety-related): AS 410F, AS 412F, AS 414F, AS 416F, and AS 417F
- AS Redundancy Station with two redundant CPUs (safety-related and fault-tolerant): AS 410FH, AS 412FH, AS 414FH, AS 416FH, and AS 417FH

In the safety-related AS bundles, the controller hardware is combined with the safety function of S7 F systems.

By selecting preconfigured ordering units, you can define the configuration of the AS bundles and their order numbers in interactive mode. A configurator provided in the Industry Mall on the Internet (see www.siemens.com/industrymall) will support you here.

The ordering units of the AS bundles are also listed in a table in the SIMATIC PCS 7 Catalog ST PCS 7. Individual components can be selected from the ST PCS 7 and ST 70 catalogs. Both catalogs are available on the Internet at: www.siemens.com/simatic/printmaterial

AS 410F/FH

The AS 410F/FH automation systems that can be used with SIMATIC PCS 7 V8.0+SP1 or higher have been developed exclusively for the SIMATIC PCS 7 process control system. Their key feature is the innovative CPU 410-5H Process Automation, whose automation performance can be graded with expansion cards for 100 PO, 500 PO, 1 000 PO, 1 600 PO and ≥ 2 000 PO (PO 2k+).

With its high-performance hardware and optimized firmware V8.0, this CPU can cover the entire performance range of the AS 412F/FH, AS 414F/FH, AS 416F/FH and AS 417F/FH, which are scalable by CPU type. It has an interface for PROFINET IO (2-port switch) and an interface for PROFIBUS DP. 16 MB of work memory for program and data, and 48 MB of load memory are already integrated. Two prepared slots allow the synchronization of two redundant subsystems via sync modules and sync cables (FOC).

Other features
- Cycle time up to 10 ms/9 process tasks
- Up to 7 500 I/Os at the DP and PN interface (16 KB each for inputs and outputs)
- PCB protective coating (conformal interface)
- High-precision time stamping
- Recessed RESET button
- Preset hardware parameters
<table>
<thead>
<tr>
<th>CPU type</th>
<th>CPU 410-5H Process Automation</th>
<th>CPU 412-5H PN/DP</th>
<th>CPU 414-5H PN/DP</th>
<th>CPU 416-5H PN/DP</th>
<th>CPU 417-5H PN/DP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component of the AS bundle</td>
<td>AS 410F (1 ×) / AS 410FH (2 ×)</td>
<td>AS 412F (1 ×) / AS 412FH (2 ×)</td>
<td>AS 414F (1 ×) / AS 414FH (2 ×)</td>
<td>AS 416F (1 ×) / AS 416FH (2 ×)</td>
<td>AS 417F (1 ×) / AS 417FH (2 ×)</td>
</tr>
<tr>
<td>Technical setup</td>
<td>S7-400 with distributed I/O</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load memory, RAM (integrated / memory card)</td>
<td>48 MB / –</td>
<td>512 KB / up to 64 MB</td>
<td>512 KB / up to 64 MB</td>
<td>1 MB / up to 64 MB</td>
<td>1 MB / up to 64 MB</td>
</tr>
<tr>
<td>Main memory</td>
<td>32 MB</td>
<td>1 MB</td>
<td>1 MB</td>
<td>16 MB</td>
<td>16 MB</td>
</tr>
<tr>
<td>■ Total</td>
<td>16 MB</td>
<td>512 KB</td>
<td>2 MB</td>
<td>6 MB</td>
<td>16 MB</td>
</tr>
<tr>
<td>■ For program</td>
<td>16 MB</td>
<td>512 KB</td>
<td>2 MB</td>
<td>10 MB</td>
<td>16 MB</td>
</tr>
<tr>
<td>■ For data</td>
<td>4 MB</td>
<td>2 MB</td>
<td>2 MB</td>
<td>16 MB</td>
<td></td>
</tr>
<tr>
<td>Execution time</td>
<td>7.5 ns</td>
<td>31.25 ns</td>
<td>18.75 ns</td>
<td>12.5 ns</td>
<td>7.5 ns</td>
</tr>
<tr>
<td>Fieldbus connection</td>
<td>PROFIBUS (DP), PROFINET (PN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Number and type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Number of DP segments</td>
<td>2 (DP and PN)</td>
<td>3 (MPI/DP, DP, PN)</td>
<td>3 (MPI/DP, DP, PN)</td>
<td>3 (MPI/DP, DP, PN)</td>
<td>3 (MPI/DP, DP, PN)</td>
</tr>
<tr>
<td>■ Number of DP slaves</td>
<td>1 96 (DP)</td>
<td>2 32 (MPI/DP); 64 (DP)</td>
<td>2 32 (MPI/DP); 96 (DP)</td>
<td>2 32 (MPI/DP); 125 (DP)</td>
<td>2 32 (MPI/DP); 125 (DP)</td>
</tr>
<tr>
<td>■ Number of PROFINET IO devices</td>
<td>250</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Dimensions (W × H × D) in mm</td>
<td>50 × 290 × 219</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SIMATIC S7-300 controller series

The SIMATIC S7-300F controllers have a very rugged and compact design. They are only offered in a single-channel version with one CPU. Fault-tolerant controllers with redundant CPUs are not available in this series.

Combining the two CPU types S7-315F and S7-317F with different fieldbus interfaces (DP or PN/DP) results in a product range with four controllers which is rounded off by what is currently the most powerful controller, S7-319F-3 PN/DP (see table below).

Controllers with S7-315F-2 DP or S7-317F-2 DP CPUs are exclusively designed for fieldbus communication using PROFIBUS DP.

Controllers with S7-315F-2 PN/DP, S7-317F-2 PN/DP or S7-319F-3 PN/DP CPUs additionally support the PROFINET standard, which is already established in factory automation.

You can expand the S7-300F CPUs centrally using the safety-related F-modules of the ET 200M I/O system. Distributed expansion is possible with remote I/O stations and safety-related F-modules/submodules of the ET 200M, ET 200S, ET 200pro and ET 200eco I/O systems.

<table>
<thead>
<tr>
<th>CPU type</th>
<th>CPU 315F-2 DP</th>
<th>CPU 315F-2 PN/DP</th>
<th>CPU 317F-2 DP</th>
<th>CPU 317F-2 PN/DP</th>
<th>CPU 319F-3 PN/DP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical setup</td>
<td>S7-300 with distributed I/O or central, safety-related I/O</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load memory (MMC), max.</td>
<td>8 MB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main memory</td>
<td>384 KB</td>
<td>512 KB</td>
<td>1.5 MB</td>
<td>1.5 MB</td>
<td>2.5 MB</td>
</tr>
<tr>
<td>Execution time</td>
<td>0.12 µs</td>
<td>0.12 µs</td>
<td>0.04 µs</td>
<td>0.04 µs</td>
<td>0.01 µs</td>
</tr>
<tr>
<td>Fieldbus connection</td>
<td>PROFIBUS (DP)</td>
<td>PROFIBUS (DP), PROFINET (PN)</td>
<td>PROFIBUS (DP)</td>
<td>PROFIBUS (DP), PROFINET (PN)</td>
<td>PROFIBUS (DP), PROFINET (PN)</td>
</tr>
<tr>
<td>Integrated interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number and type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of DP segments</td>
<td>2 (MPI and DP)</td>
<td>2 (DP/MPI and PN)</td>
<td>2 (DP/MPI and DP)</td>
<td>2 (DP/MPI and PN)</td>
<td>3 (DP/MPI, DP, PN)</td>
</tr>
<tr>
<td>Number of DP slaves</td>
<td>124</td>
<td>124</td>
<td>124</td>
<td>124</td>
<td>256</td>
</tr>
<tr>
<td>Number of PROFINET IO devices</td>
<td>–</td>
<td>128</td>
<td>–</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Dimensions (W × H × D) in mm</td>
<td>40 × 125 × 130</td>
<td>40 × 125 × 130</td>
<td>80 × 125 × 130</td>
<td>40 × 125 × 130</td>
<td>120 × 125 × 130</td>
</tr>
</tbody>
</table>
Versatile, distributed I/O systems

The distributed I/O systems of the Safety Integrated System can be differentiated as follows:

- ET 200M: Modular I/O for multi-channel applications with safety-related signal modules (F-DI, F-DO, F-AI), SIL 2/SIL 3; IP20 degree of protection
- ET 200iSP: Modular, intrinsically-safe I/O with safety-related electronic modules (F-DI Ex, F-DO Ex, F-AI Ex), SIL 3, IP30 degree of protection
- ET 200S: Bit-modular I/O with safety-related electronic modules (F-DI, F-DO) and safety-related motor starters, SIL 2/SIL 3; IP20 degree of protection
- ET 200pro: Modular, very compact I/O with safety-related electronic modules (F-DI, F-DI/F-DO), SIL 2/SIL 3; F-switch for switch-off of standard I/O and control of motor switches; IP65/66/67 degree of protection

The safety functions of the SIMATIC controllers are perfectly matched to the safety-related F-modules/submodules of these I/O systems. Any ET 200 station can be configured quickly and easily using the SIMATIC Selection Tool. The tool is familiar with the configuration rules and supports users in the selection of all components and associated accessories in interactive mode.

The SIMATIC Selection Tool is available on the Internet at: www.siemens.com/tia-selection-tool

Detailed information on all ET 200 distributed I/O systems is available at www.siemens.com/et200

---

1) Dust atmospheres: installation of components always in an enclosure with IP6x degree of protection
2) With 10 A DC standard power supply
3) Also complies with FM/UL according to Class I Division 2

Safety-related process I/O in potentially explosive gas and dust atmospheres
The ET 200M and ET 200iSP I/O systems described below are particularly relevant to implementation of safety-instrumented applications in the process industry.

<table>
<thead>
<tr>
<th>Safety-related, distributed I/O systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device characteristics</strong></td>
</tr>
<tr>
<td>Degree of protection</td>
</tr>
<tr>
<td>For use in hazardous areas</td>
</tr>
<tr>
<td>Temperature range</td>
</tr>
<tr>
<td>Resistance to vibration</td>
</tr>
<tr>
<td>Redundancy</td>
</tr>
<tr>
<td>Online modification functions</td>
</tr>
<tr>
<td>Number of I/O modules/submodules</td>
</tr>
<tr>
<td>Mixing of standard and F-modules/submodules</td>
</tr>
<tr>
<td>Time stamp functionality</td>
</tr>
</tbody>
</table>

| F-modules/submodules                     |
| DI                                       | 12/24 × DC 24 V, 4/8 × NAMUR [Ex ib] | 4/8 × NAMUR Ex |
| DO                                       | 10 × DC 24 V/2 A, 8 × DC 24 V/2 A | 4 × DC 17.4 V/40 mA Ex |
| AI                                       | 3/6 × 0 ... 20 mA or 4 ... 20 mA HART, 15 bits + sign | 4 × 0 ... 20 mA or 4 ... 20 mA Ex HART, 15 bits + sign |

| PROFIBUS connection                      |
| Interface module                         | IM 153-2 High Feature | IM 152-1 |

| PROFINET connection                      |
| Interface module                         | IM 153-4 PN High Feature | – |

¹ As SIPLUS extreme component also for extended temperature range -40/-25°C to +60/+70°C and corrosive atmosphere/condensation
**SIMATIC ET 200M**

**ET 200M configuration**

An ET 200M station can accommodate up to 12 I/O modules of S7-300 design. Hot swapping is permissible when using active bus modules.

The following safety-related F-modules can be used in applications up to SIL 3, and can be combined with standard modules without restrictions in a station without isolating module:

- SM 326 F-DI 24 × DC 24 V (6ES7326-1BK02-0AB0)
- SM 326 F-DO 10 x DC 24 V, 2 A (6ES7326-2BF10-0AB0)
- SM 326 F-DO 8 x DC 24 V, 2 A (6ES7326-2BF41-0AB0)
- SM 336 F-AI HART 6 x 0/4 ... 20 mA (6ES7336-4GE00-0AB0)

If an SM 326 F-DI NAMUR is used in SIL 3 applications, an isolating module is always required for mixed configurations with standard modules.

For SIL 3 applications with other F-modules, an isolating module is also required under the following conditions:

- Operation of F-modules as central I/O of S7-300F controllers
- Design of PROFIBUS DP with copper cables
- Design of PROFIBUS DP with fiber-optic cables and joint operation of the fail-safe and standard modules in an ET 200M station

**F-modules**

- ET 200 rack
  - only for SIL 3 operation, SIL 2 also possible without isolating module

**F-signal modules for ET 200M**

The F-signal modules of ET 200M (DI/DO/AI) can be used for diagnostics of both internal and external faults. They carry out self-tests, e.g. for short-circuit or wire break, and automatically monitor the discrepancy time defined in the parameter settings.

Depending on the version, the input modules support 1oo1 and 1oo2 evaluation on the module. Further evaluations, e.g. 2oo3 evaluation for analog inputs, are carried out by the CPU.

The digital output modules enable safe disconnection through a second disconnect path in the event of a faulty output.

Design of ET 200M with isolating module

F-AI HART analog input module for ET 200M (6 x 0/I4 ... 20 mA)
<table>
<thead>
<tr>
<th>Module types</th>
<th>Digital input</th>
<th>Digital output</th>
<th>Analog input</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SM 326F</strong></td>
<td>8 (1-channel) 4 (2-channel) Isolated by channel</td>
<td>8, electrically isolated in groups of 5 P/P switching</td>
<td>6 (1-channel) 3 (2-channel) 15 bits + sign 2-wire or 4-wire connection</td>
</tr>
<tr>
<td><strong>SM 326F NAMUR [EEEx ib]</strong></td>
<td>10, electrically isolated in groups of 5 P/P switching</td>
<td>8, electrically isolated in groups of 4 P/M switching</td>
<td></td>
</tr>
<tr>
<td><strong>SM 336F HART</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Max. number of inputs/outputs**
  - SM 326F: 24 (1-channel for SIL 2 sensors) 12 (2-channel for SIL 3 sensors) electrically isolated in groups of 12
  - SM 326F NAMUR: 12 (2-channel for SIL 3 sensors) 8 (1-channel)
  - SM 336F HART: 8 (1-channel) 4 (2-channel) 10, electrically isolated in groups of 5 P/P switching

- **Max. achievable safety class according to IEC 61508/EN 954-1**
  - SM 326F: 1-channel/1oo1: SIL 2 2-channel/2oo2: SIL 3 (SIL 3 without isolating module)
  - SM 326F NAMUR: 1-channel/1oo1: SIL 2 2-channel/1oo2: SIL 3 (SIL 3 without isolating module)
  - SM 336F HART: 1-channel/1oo1 and 2-channel/1oo2 (SIL 3 without isolating module)

- **Input or output voltage**
  - SM 326F: 24 V DC
  - SM 326F NAMUR: 24 V DC
  - SM 336F HART: 24 V DC

- **Input or output current**
  - SM 326F: –
  - SM 326F NAMUR: –
  - SM 336F HART: –

- **Short-circuit-proof sensor supply**
  - SM 326F: 4 for every 6 channels, electrically isolated in groups of 2
  - SM 326F NAMUR: 8 for each channel, individually isolated
  - SM 336F HART: –

- **Special features**
  - SM 326F: Support of time stamping (SOE)
  - SM 326F NAMUR: Detection of signals from the Ex area
  - SM 336F HART: “Keep last valid value” parameter, channel-selective passivation

- **Redundancy mode**
  - SM 326F: Channel-selective
  - SM 326F NAMUR: Channel-selective
  - SM 336F HART: Channel-selective

- **Module and channel diagnostics**
  - SM 326F: –
  - SM 326F NAMUR: –
  - SM 336F HART: –

- **PROFINET**
  - SM 326F: –
  - SM 326F NAMUR: –
  - SM 336F HART: –

- **Dimensions W x H x D (in mm)**
  - SM 326F: 80 × 125 × 120
  - SM 326F NAMUR: 80 × 125 × 120
  - SM 336F HART: 40 × 125 × 120

© Siemens AG 2014
Field devices, sensors and actuators can be connected simply, quickly and reliably to I/O modules of the ET 200M remote I/O stations using MTA terminal modules (Marshalled Termination Assemblies). MTA versions are available for standard I/O modules as well as for redundant and safety-related I/O modules.

The MTA terminal modules listed in the table below are available for the sensor/actuator connection to F-modules of the ET 200M remote I/O stations.

<table>
<thead>
<tr>
<th>MTA type</th>
<th>Input/output range</th>
<th>I/O redundancy</th>
<th>Article No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 channels F AI HART (safety-related)</td>
<td>4... 20 mA (with/without HART) or 0... 20 mA (without HART)</td>
<td>6</td>
<td>6ES7650-1AH62-5XX0(^1) 6ES7336-4GE00-0AB0 6ES7922-3BD00-0AU0 (3 m) -3BJ00-0AU0 (8 m)</td>
</tr>
<tr>
<td>24 channels F DI (safety-related)</td>
<td>24 V DC</td>
<td>6</td>
<td>6ES7650-1AK11-7XX0 6ES7326-18K02-0AB0 6ES7922-3BD00-0AS0 (3 m) -3BJ00-0AS0 (8 m)</td>
</tr>
<tr>
<td>10 channels F DO (safety-related)</td>
<td>24 V DC, 2 A</td>
<td>6</td>
<td>6ES7650-1AL11-6XX0 6ES7326-2BF10-0AB0 6ES7922-3BD00-0AN0 (3 m) -3BJ00-0AN0 (8 m)</td>
</tr>
<tr>
<td>10 channels F DO relays (safety-related)</td>
<td>120... 230 V AC, 5 A; 24 V DC, 5 A</td>
<td>6</td>
<td>6ES7650-1AM31-6XX0 6ES7326-2BF10-0AB0</td>
</tr>
</tbody>
</table>

\(^1\) This terminal module cannot provide a 24 V DC current for the supply of 4-wire transmitters. For the redundant 24 V DC supply of 4-wire transmitters via MTA, you also need an MTA Power Supply 24 V DC terminal module.
ET 200iSP configuration

In accordance with ATEX directive 94/9/EC, the ET 200iSP remote I/Os stations can be installed directly in the Ex zones 1, 2, 21 or 22 as well as in non-hazardous areas. For installation in hazardous zones 1 or 21, the RS 485-iS coupler acts as a barrier. The intrinsically-safe sensors, actuators and HART field devices can also be located in zone 0 or 20 if necessary.

ET 200iSP stations can be flexibly configured and expanded thanks to the modular architecture. Availability can be increased with a redundant design for the pressure-enclosed power supply and for the interface modules.

Terminal modules for mounting on an S7-300 mounting rail are used as holders for the various different module types. Automatic slot coding and independent wiring enable simple and reliable hot swapping of individual modules without a fire certificate. Installation and testing of the wiring is possible in advance without the electronic modules.

In addition to analog and digital I/O modules for the automation of the technological functions of the process (Basic Process Control), the range of electronic modules also includes safety-related F-I/O modules for implementing safety applications. The various types of electronic module can be arranged mixed within a station.

Up to 32 electronic modules can be inserted between the interface module and the termination module. In this case, the station is 107 cm wide. However, the number of electronic modules that can be operated in a station may be limited by the power consumption of the modules used. However, up to 16 electronic modules can be inserted without limitation.

F-signal modules for ET 200iSP

The F-I/O modules with safety functions implement safety applications together with the safety-related controllers (automation systems). The input modules record 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.
Overview of F-signal modules for SIMATIC ET 200iSP

<table>
<thead>
<tr>
<th>Module types</th>
<th>Digital input</th>
<th>Digital output</th>
<th>Analog input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. number of inputs/outputs</td>
<td>8 F-DI Ex NAMUR</td>
<td>4 F-DO Ex DC 17.4 V/40 mA</td>
<td>4 F-AI Ex HART</td>
</tr>
<tr>
<td>Max. achievable safety class</td>
<td>1-channel/1oo1: SIL 3</td>
<td>4, sourcing/sourcing output</td>
<td>SIL 3 with</td>
</tr>
<tr>
<td>according to IEC 61508/EN 954-1</td>
<td>2-channel/2oo2: SIL 3</td>
<td></td>
<td>1 module: 1oo1 evaluation</td>
</tr>
<tr>
<td>Input or output voltage</td>
<td>NAMUR</td>
<td>17.4 V</td>
<td>–</td>
</tr>
<tr>
<td>Input or output current</td>
<td>–</td>
<td>40 mA per channel</td>
<td>4 ... 20 mA or 0 ... 20 mA</td>
</tr>
<tr>
<td>Short-circuit-proof sensor supply</td>
<td>8 for each channel</td>
<td>–</td>
<td>4 for each channel</td>
</tr>
<tr>
<td>Operating environment</td>
<td>Hazardous and non-hazardous areas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Special features</td>
<td>Support of time stamping</td>
<td>Output current doubled for an actuator with the parallel connection of two outputs</td>
<td>HART communication in measuring range 4 ... 20 mA</td>
</tr>
<tr>
<td>Module and channel diagnostics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions W x H x D (in mm)</td>
<td>30 x 129 x 136.5</td>
<td>30 x 129 x 136.5</td>
<td>30 x 129 x 136.5</td>
</tr>
</tbody>
</table>

Safe process instruments and process devices for connection to ET 200M remote I/Os

Siemens currently offers the following safe process instruments/devices for operation on ET 200M remote I/Os:

- **Process instrument/process device**
  - **Pressure measurement**
    - SITRANS P DS III analog/HART: SIL 2
  - **Temperature measurement**
    - SITRANS TW series: SIL 1
    - SITRANS TH200/TH300: SIL 2
    - SITRANS TR200/TR300: SIL 2
  - **Flow measurement**
    - SITRANS FC430 compact: SIL 2
  - **Level measurement**
    - SITRANS LVL200: SIL 2
    - SITRANS LR250 HART: SIL 2
  - **Valve positioner**
    - SIPART PS2, two-wire version: SIL 2
    - SIPART PS2, four-wire version: SIL 2

Detailed information, technical specifications and ordering data on these devices are available on the Internet at: [www.siemens.com/processinstrumentation](http://www.siemens.com/processinstrumentation)
Direct device interfacing via fieldbus with high safety and availability

Redundant routers together with a PROFIBUS PA of ring topology enable cheaper safety-related and fault-tolerant applications than the previous standard architectures (see figure on left).

The PROFIBUS PA of ring topology is connected to two redundant PROFIBUS segments of an S7-400FH controller via the redundant router. AFD4, AFD8 and AFDiS active field distributors can integrate up to 31 field devices into the PROFIBUS PA ring over their short-circuit-proof spur line connections.

As shown in the figure on the right, safety-related and fault-tolerant applications can be implemented with relatively low device and cable requirements. The configuration of the ring can also be changed during runtime. Even brief opening-up of the ring in order to integrate a further AFD is possible without production failures. The diagnostics integrated in the redundant router and the active field distributors expands the existing possibilities for communication and cable diagnostics, and makes it easier to locate faults in the event of a cable break. The concept of Flexible Modular Redundancy is thus implemented down to the field level.
Safe field instrumentation on PROFIBUS PA

PROFIBUS PA devices for implementation of safety shutdowns

The SITRANS P DSIII digital pressure transmitter is the first commercially available PROFIBUS PA device for SIL 2 safety shutdowns conforming to IEC 61508/IEC 61511-1. To this end, Siemens has extended its standard measuring equipment for pressure, absolute pressure and differential pressure with a PROFIsafe driver.

In a safety application, the pressure transmitter can be connected to an FH controller from the SIMATIC S7-400 series over PROFIBUS PA and PROFIsafe. Advantages such as direct communication links and power supply to intrinsically-safe devices, increased information contents and reliability of measured value transmission are then combined with each other.

The digital input of the electropneumatic PROFIBUS PA positioner SIPART PS2 PA can be used for the safe shutdown. With a redundant, multi-channel design, measuring circuits can also be implemented up to safety integrity level SIL 3.

The SIMATIC PDM Process Device Manager is used to initially start up the SITRANS P DSIII pressure transmitter as a regular PROFIBUS PA device. You subsequently activate the PROFIsafe functions.

The device description (DD) required for this, the safety manual as well as further information are available on the Internet at: www.siemens.com/sitransp
Safety Lifecycle Management

Analysis, implementation, operation and maintenance

The installation and operation of potentially dangerous plants in the process industry are subject to the international standard IEC 61511, the standard for the functional safety of safety-instrumented systems.

The procedure for implementing functional safety is described in this standard in accordance with the safety lifecycle of the plant, which is divided into the analysis, implementation and operation phases.

In each phase of the safety lifecycle, overall responsibility lies with the plant manufacturer, for example a general contractor acting on behalf of the end user. This responsibility may be delegated in some areas with the outsourcing of work packages. The scope of delivery for each of these packages and the interfaces, dependencies and responsibilities must, however, be clearly defined.

The functional safety manager initiates and monitors all safety lifecycle management activities. He or she advises the project manager and the other members of the project teams on all matters relating to functional safety.

Analysis phase

Process plants which are potentially dangerous must be specifically analyzed in order to identify possible dangers and to assess their risks. An appropriate method for this is, for example, the HAZOP analysis (Hazard Operational Analysis).

Protection levels are defined on the basis of the findings of the analysis and an evaluation of these findings, and safety tasks and functions are assigned to these protection levels. The safety instrumented system (SIS) is one of these protection layers.

An important result of the analysis is the Safety Requirement Specification (SRS) for the safety instrumented system. The SRS describes all Safety Instrumented Functions (SIF) including the demands placed on them, and specifies the required Safety Integrity Level (SIL). The SIL is a measure of the reduction in risk.
Implementation phase

The SRS is the basis for further planning of the plant, especially for the design of the safety instrumented system (SIS) and its safety functions as well as for other measures for reducing the risk. It is decisive for the selection of the SIS and of the hardware and software for implementing the safety functions.

Design and planning are followed by installation, commissioning, and validation of the plant. The SRS includes the associated tests and test criteria as well as the safety functions and requirements. The SRS therefore also forms the basis for verification and validation.

Operation and maintenance phase

This phase comprises operation and optimization of the plant up to the time it is decommissioned.

Safety verification documents

One set of standardized documentation facilitates project verification and validation and speeds up implementation and commissioning.

All phases of the safety lifecycle and the associated activities for functional safety are to be documented. These documents (see figure above) are the basis for proving the safety of the plant and of the safety-instrumented systems used. They are required for acceptance of the safety functions and the safety system. All phases of the safety lifecycle must be carried out and documented again following any modifications.

Safety Lifecycle Services

With Safety Lifecycle Services, Siemens provides not only the necessary expertise for safety verification, but also progressive tools and methods that exclude systemic errors in all project phases.

This is all the more important since errors in an early project phase are often costly and time-consuming to correct at a later date. Moreover, it means that plant operators do not have to acquire the necessary expertise themselves and continuously adapt to the latest guidelines and technologies.

The following service modules are available:

- Management, evaluation of "functional safety" and audits
- Configuration and planning of the SLC (Safety Plan)
- Hazard and safety assessment
- Assignment of the safety functions to the protection levels
- Safety Requirement Specification (SRS)
- Verification and validation (e.g. SIL verification, hardware/software audit)
- Modification
- Training
Qualified and certified safety experts

<table>
<thead>
<tr>
<th>Knowledge skills</th>
<th>System integrator</th>
<th>Siemens employee</th>
<th>End user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workshop IEC 61511 – Practical use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workshop PCS 7 Process Safety (F-Technology), with exam</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workshop TÜV Functional Safety for process industry, with exam/certification</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project and technical skills</th>
<th>Siemens employee</th>
<th>System integrator</th>
<th>End user</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 years experience in process safety, evaluation of 2 projects</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience skills</th>
<th>Siemens employee</th>
<th>System integrator</th>
<th>End user</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFSP Certificate: Siemens Functional Safety Professional (SFSP)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employees know-how</th>
<th>Siemens employee</th>
<th>System integrator</th>
<th>End user</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 years experience, evaluation for SFSE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Siemens Functional Safety Expert (SFSE)</th>
<th>Siemens employee</th>
<th>System integrator</th>
<th>End user</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFSE Certificate: Siemens Functional Safety Expert (SFSE)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Content of the accredited SFSP/SFSE training program

Siemens employs safety experts with accredited qualifications for Safety Lifecycle Services. They have completed a training program and qualified as Siemens Functional Safety Professionals (SFSP) or Siemens Functional Safety Experts (SFSE). This program is organized and run by Siemens in close cooperation with the TÜV.

The training program is also open to employees of the operator (end user) and solution partners (system integrators).

Solution Partners

To be able to meet growing demands in the area of safety engineering, Siemens is increasingly using the support of selected Siemens solution partners.

These are highly qualified partner companies which offer professional consulting and services for all relevant safety aspects. They are experts in safety engineering in the process industry, and have:

- Know-how concerning the safety lifecycle of IEC 61511
- Knowledge of safety engineering with S7 F Systems and SIMATIC Safety Matrix
- Comprehensive experience in projects with safety applications in the process industry

A list of certified Siemens solution partners is available on the Internet at: www.siemens.com/process-safety

More details on the Siemens Solution Partner Program are available on the Internet at: www.siemens.com/automation/solutionpartner

Additional information on safety lifecycle management is available on the Internet at: www.siemens.com/processsafety

Information on training courses on safety engineering for process automation is available on the Internet at: www.siemens.com/sitrain
SIMATIC Safety Matrix
The safety lifecycle management Tool

SIMATIC Safety Matrix
The SIMATIC Safety Matrix offered by Siemens is a TÜV-certified Safety Lifecycle Management tool for safety applications up to SIL 3 in accordance with IEC 61508.

SIMATIC Safety Matrix can be used in all phases of the safety lifecycle. The rationalization effects achieved make a significant contribution toward reducing the investment costs and the operational expenses of the plant.

SIMATIC Safety Matrix consists of the following individual products which have different functionalities and fields of application:

- Safety Matrix Editor
- Safety Matrix Engineering Tool
- Safety Matrix Viewer

Consistent use of the SIMATIC Safety Matrix across all phases of the safety lifecycle reduces the investment costs and operational expenses. SIMATIC Safety Matrix offers clear benefits in all phases.

Analysis phase
SIMATIC Safety Matrix does not require programming knowledge. It can therefore be used equally by process, test and planning engineers.

Safety functions are defined using the Cause&Effect method. The Cause&Effect representation is compact, clear, and easy to understand.

Implementation phase
The safety functions defined using SIMATIC Safety Matrix can be imported directly. It is only necessary to carry out the system-specific settings of the SIMATIC S7-400F/FH safety system. Planning engineers, operators and test engineers always have an identical and generally understandable view. The safety functions are represented identically during configuration and operation and in the documentation. Signal states and supplementary information are displayed in different colors during operation. All this results in a significant reduction in engineering, test and acceptance times.

Operating phase
The optimized operator prompting of the SIMATIC Safety Matrix guarantees during operation that operators can react rapidly and specifically to events. They can also simulate sensor and actuator systems, particularly during maintenance. The SIMATIC Safety Matrix Viewer can be used to reduce plant downtimes.

The benefits of Safety Matrix at a glance
- No programming knowledge required
- Uniform view and understanding for all persons involved
- Identical display of matrix in configuration, operation, and documentation
- Reduction in planning, implementation, and acceptance times
- Integrated functions for commissioning and maintenance
- Optimum operator prompting
- Reduced downtimes
SIMATIC Safety Matrix in the analysis phase

It is important in the analysis phase to identify and analyze known and potential safety risks, e.g. using the HAZOP method. This serves to filter out non-tolerable risks, to evaluate the probability of a hazard occurring, and to estimate possible consequences.

The safety concept for the plant is subsequently produced. During this, the safety tasks are assigned to the various protection layers of the plant.

The safety instrumented system (SIS) plays an important role within the safety concept. The SIS requirements defined and described in the form of a specification are the basis for planning, engineering, and acceptance of the plant. Since different people have to work in accordance with this specification during different phases of the safety lifecycle, it is important to formulate the safety requirements in a readily understandable manner.

Safety Requirement Specification (SRS)

The requirements placed on the safety system are defined in the SRS. The SRS includes the functional description of the safety functions as well as all marginal conditions that cause them to be triggered. In addition, determination of the Safety Integrity Level (SIL) is part of the detailed consideration of each individual safety function.

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of failure on demand (PFD) per year</th>
<th>Risk Reduction Factor $= 1/PFD$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>$10 000$ to $100 000$</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
<td>$1 000$ to $10 000$</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
<td>$100$ to $1 000$</td>
</tr>
<tr>
<td>SIL 1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
<td>$10$ to $100$</td>
</tr>
</tbody>
</table>

1) Demand mode of operation

Safety concept and levels of a plant
Cause&Effect matrix

The Cause&Effect method has proven to be an extremely effective option for the description of safety functions and for the definition of marginal and shut-down conditions. The method specified by the American Petroleum Institute in the API RP 14C guideline is currently employed in many sectors of the process industry.

Siemens has implemented the Cause&Effect method defined by the American Petroleum Institute in SIMATIC Safety Matrix.

Already during the analysis phase, SIMATIC Safety Matrix allows safety functions to be consistently recorded, described, and formulated in a format which is easily understood by everyone involved. No special programming knowledge is required for this. This means that process specialists can also directly define their requirements with SIMATIC Safety Matrix.

The causes are defined in the rows of the matrix table. The causes derived from digital and analog signals can result from up to 3 signals. Additional aspects can also be considered, e.g. time delays.

The effects are defined in the columns of the matrix table. A cause can have an effect on up to 4 different actuators.

The linking of several causes and the definition of the response between the causes and effects is carried out at the intersections of the rows and columns. It is also defined here whether an acknowledgment or reset is required.

Causes can also be combined in selection groups. For example, it is possible to implement a 2 out of 3 (2oo3) vote in this manner.
SIMATIC Safety Matrix
in the implementation phase

The implementation phase starts with the design and planning of the safety-related system and other measures for reducing the risk. This is followed by installation, commissioning, and validation.

The specified safety functions are implemented during the planning. When using the SIMATIC Safety Matrix, the safety functions defined during the analysis phase are presented in the form of a Cause&Effect matrix, which can continue to be used directly without limitations. Conversion of the safety functions described in the SRS into a system-specific programming language, as required with the conventional procedure, is thus omitted. This allows considerable savings in engineering costs to be achieved.

Connection to the plant is established by assigning the causes and effects to the inputs and outputs of the SIMATIC S7-400F/FH. Further extensions and parameter settings can be carried out in SIMATIC Safety Matrix. These include the setting of limits and hysteresis for analog values, as well as the definition of the maximum discrepancy when linking several analog measured values.

Complex calculations can also be integrated into SIMATIC Safety Matrix using function blocks for signal preprocessing, e.g. for conversion of an input value. The corresponding function blocks can be selected in the channel driver of the I/O signal.
It is also possible to configure simulations and bypasses with corresponding access privileges for commissioning and subsequent operation.

A bypass can, for example, be controlled directly using SIMATIC Safety Matrix or via an input signal (key switch).

The option for assigning causes and effects to 3 alarm profiles each improves the overview for displaying alarms and enables plant operators to recognize problems more rapidly and to react accordingly. The reduction in shutdown times makes a significant contribution to increasing plant availability.

The conversion into an executable program logic is carried out automatically. On the basis of the CFC (Continuous Function Chart), the SIMATIC Safety Matrix Engineering Tool generates program logic for each matrix using the function blocks from the F-library in S7 F Systems, and generates the channel drivers for all fail-safe I/O channels. The CFC program logic can subsequently be compiled and downloaded to the controller. Automatic generation of the CFC program logic has been approved and certified by TÜV.

The Safety Matrix Engineering Tool can be switched directly to the online view for test purposes. Alternatively, the Safety Matrix Viewer on the SIMATIC PCS 7 Operator Station can also be used.

SIMATIC Safety Matrix has integrated functions for validity checks, documentation, and simulation as well as for the comparison of files and charts. These functions support configuration, commissioning and test engineers during testing and acceptance of the safety application.

Acceptance of the safety application is usually carried out by authorized bodies or authorities. Since such persons do not normally have special programming knowledge, they greatly profit in their work through the use of the SIMATIC Safety Matrix. The auditor can reproduce the safety functions specified in the SRS almost 1:1 on the screen in online mode. Rethinking or conversion into a specific programming language is unnecessary. This shortens the acceptance times, and production in the plant can be started earlier.
SIMATIC Safety Matrix in the operating phase

During process control it must be possible for the operator to recognize relevant deviations early and to react rapidly. Simple and intuitive operation of the automation plant is therefore necessary. This particularly applies to safety-critical processes where the plant will be shut down if the operator cannot locate the cause of an alarm rapidly enough and initiate appropriate measures.

SIMATIC Safety Matrix can make the operator aware of imminent critical situations by means of a preliminary alarm, and can display the cause and corresponding effect. The operator can then directly recognize an anomalous or faulty sensor and immediately initiate checking or other steps for elimination of the cause.

Maintenance functions integrated in the SIMATIC Safety Matrix support checking of sensors. They allow brief bypassing of the sensor for replacement or external testing. Plant downtimes or shutdowns can be avoided in this manner. A pending proof test can also be the reason for temporarily bypassing sensors or actuators.
Maintenance can be optimized even further through integration of the fail-safe sensor system into the asset management system.

SIMATIC Safety Matrix can be operated and monitored both in the online mode of the Safety Matrix Engineering Tool and by using the Safety Matrix Viewer on the operator station of the SIMATIC PCS 7 process control system.

Operator interventions are documented and can be archived for the safety lifecycle management.

The facilities in the SIMATIC Safety Matrix Viewer which are available to an operator depend on the operator privileges defined in the SIMATIC PCS 7 process control system. This guarantees that only authorized persons can bypass or simulate field devices.

Process-relevant events and alarms are transferred to the operator system of the SIMATIC PCS 7 process control system, and integrated into the signaling system. This enables joint archiving of alarms and messages by the Basic Process Control System (BPCS) and the safety system.

Matrices are called using block symbols positioned on the SIMATIC PCS 7 user interface. These can apply to the complete matrix or just to a specific cause or effect. The view focused on a cause or effect can be switched over to the total view of the matrix at any time, and vice versa.

Group displays on the block symbol for the matrix allow the operator to recognize whether warnings, alarms or maintenance functions are active. The operator can then access further detailed information by opening the corresponding matrix view.

Documentation of operator interventions and events
Get more information

Comprehensive information concerning the SIMATIC PCS 7 process control system:
www.siemens.com/simatic-pcs7

Totally Integrated Automation:
www.siemens.com/tia

SIMATIC Manual Overview:
www.siemens.com/simatic-docu

Information material to download:
www.siemens.com/simatic/printmaterial

Service&Support:
www.siemens.com/automation/support

SIMATIC contacts:
www.siemens.com/automation/partner

Industry Mall for electronic ordering:
www.siemens.com/industrymall

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens’ products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

The information provided in this brochure contains descriptions or characteristics of performance 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. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of 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 whose use by third parties for their own purposes could violate the rights of the owners.