

# Safety Integrated for Process Automation

Reliable, Flexible, Easy

Technical Brochure · April 2008

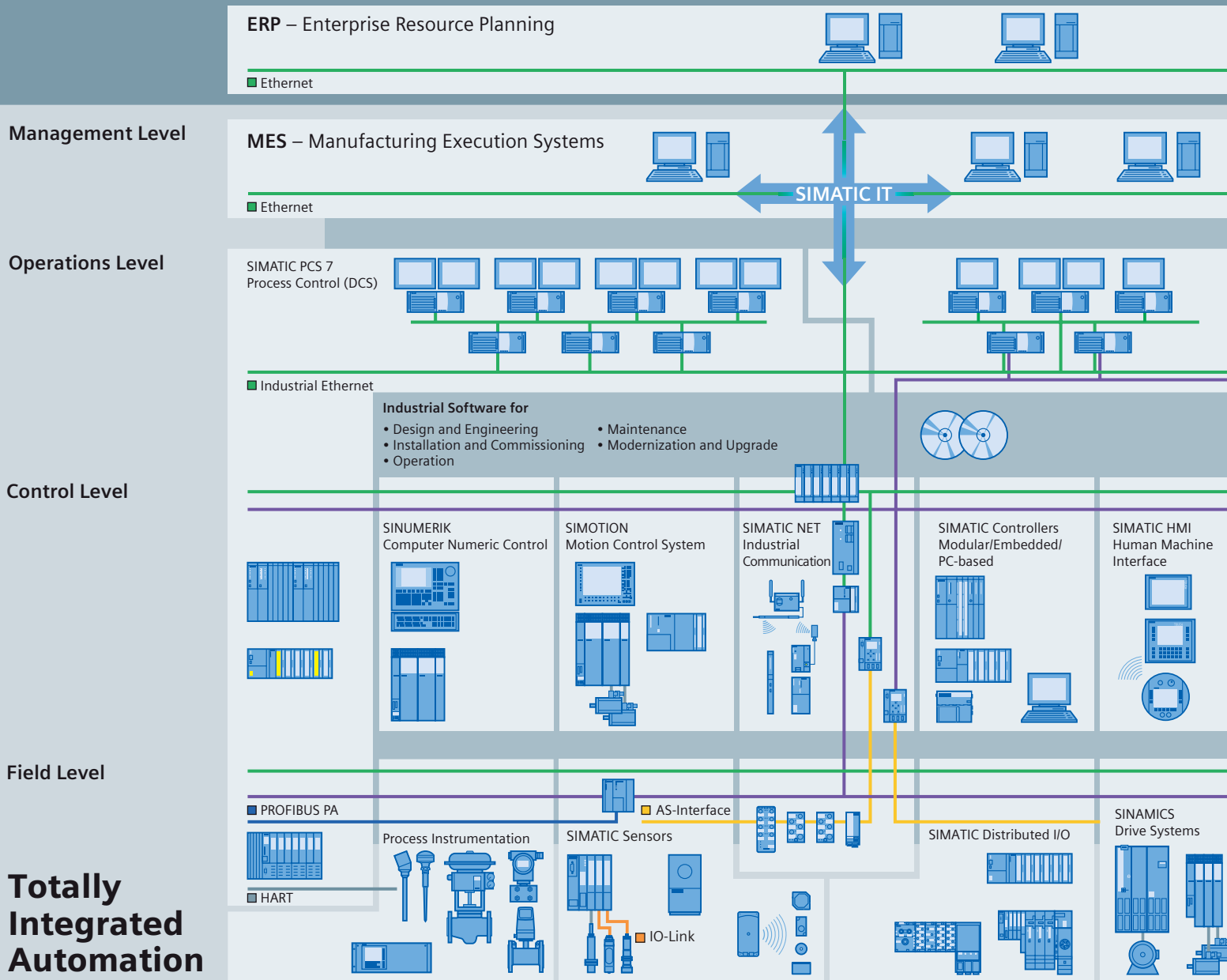


## Safety Integrated

[www.siemens.com/process-safety](http://www.siemens.com/process-safety)

**SIEMENS**

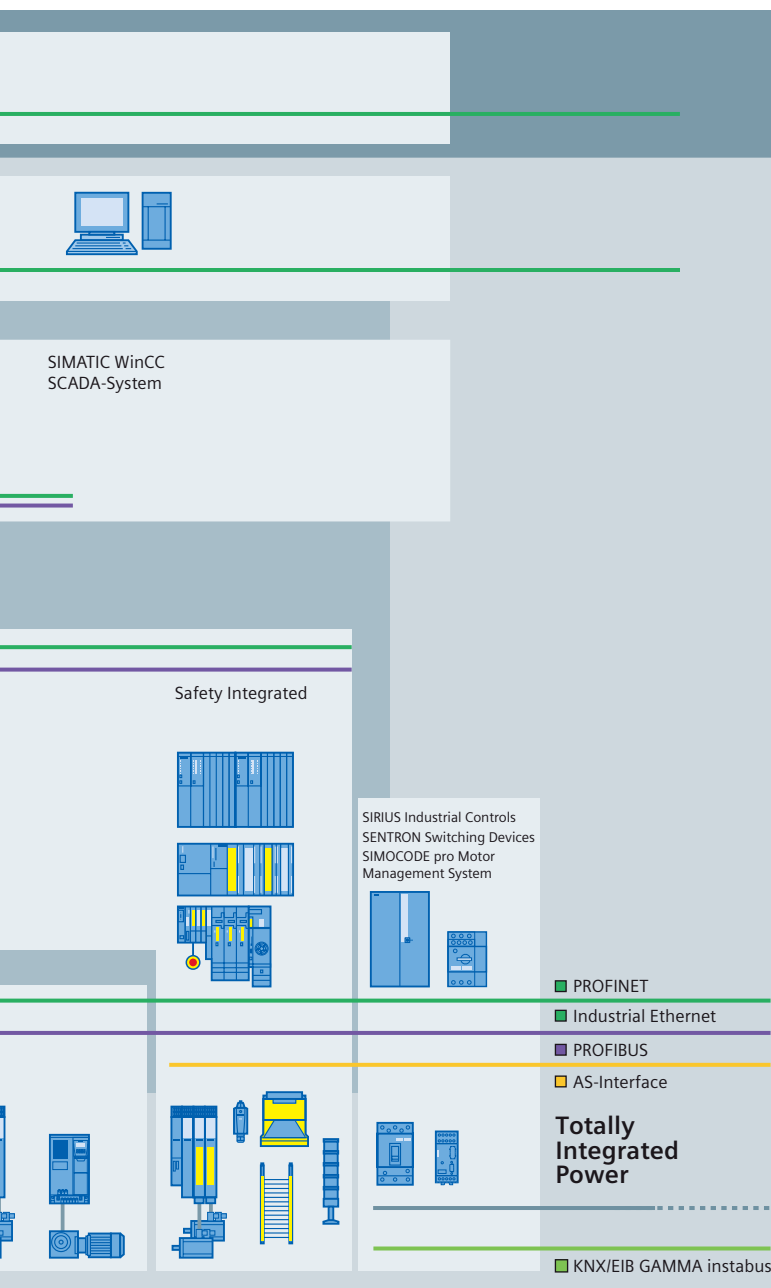
# Totally Integrated Automation



With Totally Integrated Automation (TIA), Siemens is the only provider of a uniform range of products and systems for automation in all sectors – from incoming raw materials to outgoing products, covering the field level, control level and production control level (Manufacturing Execution System, MES), and up to linking to the corporate management level (Enterprise Resource Planning, ERP, e.g. SAP).

Through the integration of safety-related functions in TIA, standard and safety-related automation system components are combined in one uniform overall system. The benefit: significant cost savings for plant constructors and owners.

# Contents



<b>Safety engineering from Siemens</b>	
Process automation with integrated safety . . . . .	4
Standardized, flexible safety products and solutions from a reliable partner . . . . .	6
Safety lifecycle management with support from highly qualified Solution Partners . . . . .	7
Simple control system integration / variable fieldbus communication with integrated safety . . . . .	8
Flexible and scalable fault tolerance / efficient safety lifecycle engineering . . . . .	9
Safety Integrated for process automation – the comprehensive range of products and services . . . . .	10
<b>Integrated control &amp; safety</b>	
SIMATIC PCS 7 – complete integration of the Safety Instrumented System . . . . .	12
<b>Safety Integrated fieldbus technology</b>	
Uniform field communication with flexible PROFIBUS architectures . . . . .	14
PROFIsafe – safety-related PROFIBUS communication . . . . .	15
<b>Flexible Modular Redundancy (FMR)</b>	
Cost-optimized safety through flexible and scalable fault tolerance . . . . .	16
Configuration options with FMR . . . . .	17
SIMATIC controllers for safety-related process applications . . . . .	19
Versatile, distributed I/O systems . . . . .	21
Direct device interfacing via fieldbus with high safety and availability. . . . .	25
Safe field instrumentation on the PROFIBUS PA . . . . .	26
<b>Safety lifecycle management</b>	
Analysis phase . . . . .	27
Realization phase . . . . .	28
Operation and maintenance phase . . . . .	30
<b>Application examples</b>	
Partial Stroke Test (PST) . . . . .	31
High Integrity Pressure Protection Systems (HIPPS), Fire & Gas and Burner Management . . . . .	33
<b>Reference projects</b>	
References in oil & gas and chemical industries . . . . .	34
<b>Overview of product and ordering data</b>	
Controllers, software components, F modules, terminal modules, distributed I/O system, safety packages. . . . .	36

# Safety engineering from Siemens

## Process automation with integrated safety

### Safe at all times

In the process industries it is not uncommon to find hazardous processes. These hazards may arise from the materials being processed being toxic, flammable or even potentially explosive. Alternatively the process itself may be hazardous – involving high pressures, temperatures or exothermic reactions. Any of these hazards, if not properly addressed, could lead to fatalities. When dealing with hazardous processes the safety of personnel, plant equipment and the environment are of utmost importance but it is also paramount that the systems put in place to ensure safety do not themselves compromise the production process through spurious trips.

In order to achieve this combination of safety and fault tolerance a reliable Safety Instrumented System (SIS) is required, which can bring the plant to a safe state when necessary but which can also meet the high availability requirements of the process industries.

### Comprehensive range of Safety Instrumented products and services

Safety Integrated for Process Automation provides a comprehensive range of products and services for fail-safe and fault-tolerant applications in the process industry. Components from the Safety Integrated range are combined in a Safety Instrumented System capable of reacting rapidly to trip conditions to bring the plant to a safe state. All the principal components of a typical Safety Instrumented System are available from Siemens including fail-safe instrumentation, fail-safe and fault-tolerant control, up to the actuators.

### Completely integrated in the standard automation

The SIMATIC S7-400FH controller with its matching I/O offers a maximum degree of safety, fault-tolerance and availability for your applications. From a fail-safe transmitter on PROFIBUS at the field level, up to the SIMATIC PCS 7 process control system: with our offering you can implement efficient and flexible solutions for automation and safety applications in a totally integrated complete system.



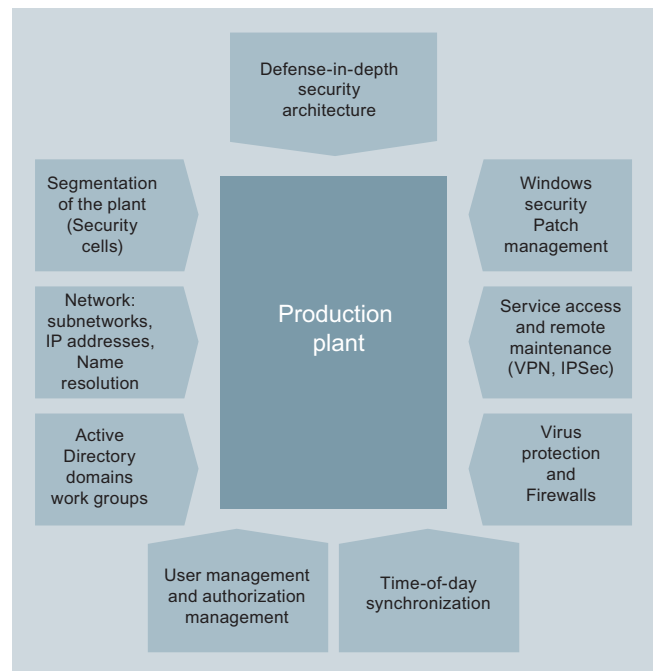
## SIMATIC PCS 7 safety & security

Increased use of open standards and global networking is unfortunately also associated with increased cyber crime. Numerous threats result due to malware or unauthorized access, e.g.:

- Overloading or failure of networks
- Espionage and stealing of passwords or process data
- Unauthorized access to Process Automation Systems
- Direct sabotage

In order to protect plants using 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 which are being continuously upgraded.

However, absolute safety cannot be guaranteed even with all the known security measures. By combining SIMATIC PCS 7 IT security with safety engineering, you can neutralize the effects of cyber crime or limit them to a tolerable degree.



SIMATIC PCS 7 safety and security measures

More information on the Internet at  
[www.siemens.com/pcs7/safety\\_security](http://www.siemens.com/pcs7/safety_security)



## Standardized, flexible safety products and solutions from a reliable partner

### A complex network of standards and directives ...

As a plant owner, you are required by government regulation to ensure safety for personnel and the environment. To achieve this, all rules, directives and orders must be implemented at the plant location. A hazard and risk analysis must be carried out if a potential hazards exist. This describes the existing risks and the current and additional measures required to reduce these risks to a level which is as low as reasonably practicable (ALARP).

Safety lifecycle activities must be comprehensively documented (e.g. safety plans, safety requirement specifications) to ensure that a consistent approach to safety is maintained throughout the analysis, realization and operation phases of the plant.

Maximum availability must be additionally guaranteed depending on the requirements, for example through Flexible Modular Redundancy (FMR). In this manner, flexible and scalable redundancy of up to 100% is simple to achieve.

### ... and a reliable partner which supports you to comply with all requirements.

For more than 25 years already, Siemens as a reliable industrial partner has been implementing first-class automation solutions for process safety in a wide range of sectors. Our solutions feature maximum efficiency, and provide users with significant potential savings whilst complying, of course, with the applicable national and international standards, e.g. IEC 61508 (up to SIL 3) 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 design and operation of Safety Instrumented Systems.

### IEC 61511 – application-specific standard for the process industry

IEC 61511 adapts IEC 61508 to the process industry. It mainly serves as a guideline for planning, implementing and operating Safety Instrumented Systems in process plants. An important component is the demand for documentation of all changes during the complete lifecycle of the plant as part of the Functional Safety Management requirements.

### Safety Integrity Level (SIL)

IEC 61508 and IEC 61511 define four different safety integrity levels (SIL 1-4). The SIL is a measure of the probability that a specific safety instrumented function (SIF) will operate successfully should a demand occur. A higher SIL level corresponds to a greater level of risk reduction. The use of certified safety components is helpful in ensuring each SIF meets its required SIL.

## Safety lifecycle management with support from highly qualified Solution Partners

### The safe way to a reliable plant: Safety lifecycle management

IEC 61511 stipulates the proof of safety for the complete safety loop, covering the sensor, controller up to the actuator. Not only the individual products are considered, but the complete lifecycle of a plant – covering risk analysis, planning, installation and operation up to taking out of operation.

We provide you with support during the complete lifecycle of your Safety Instrumented System – and offer a comprehensive range of products, systems and services:

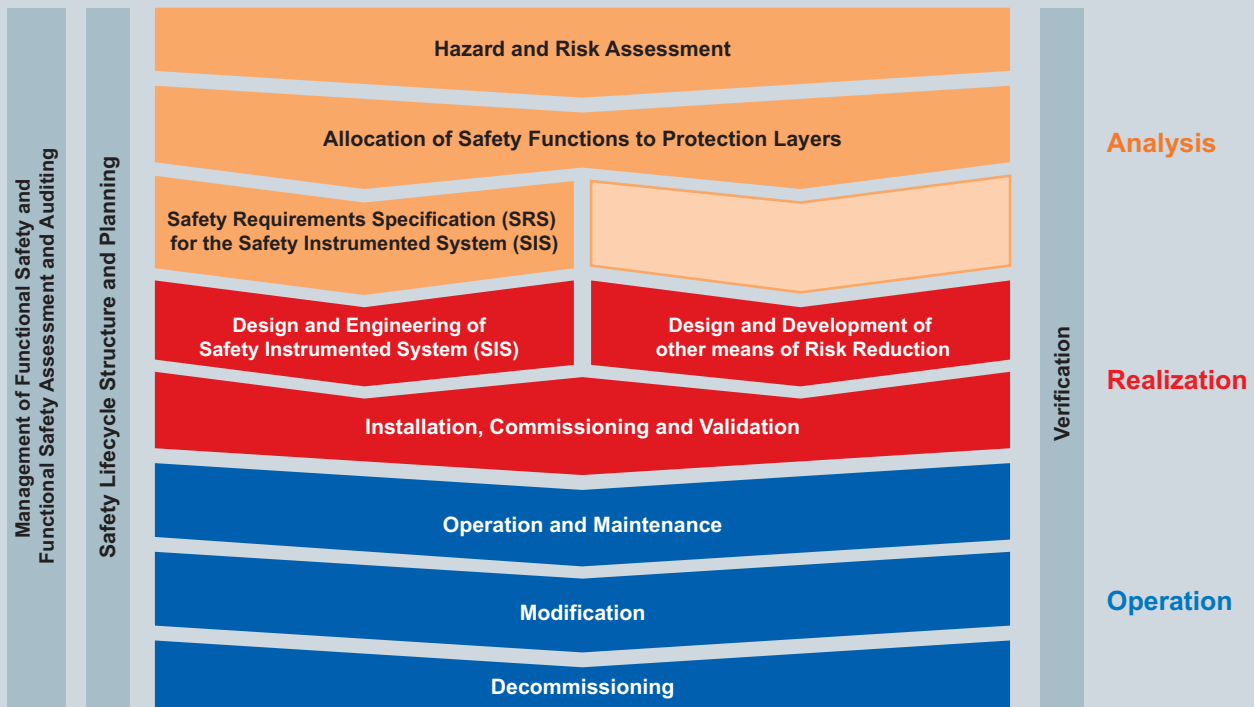
- Complete and uniform Safety Instrumented System: controller, engineering with the safety lifecycle tool "Safety Matrix", and fail-safe process instruments
- Range of services for all lifecycle phases of a Safety Instrumented System – including training, documentation and 24/7 round-the-clock servicing

### The right local support: Solution Partners

In order to cope with the increasing demands in the safety engineering sector, Siemens Automation and Drives – in addition to its standard service & support offering – is also offering selected "Siemens Solution Partners for Automation". These are highly qualified partner companies which offer you professional consulting and support for all relevant safety aspects. The PCS 7 safety specialists are certified Solution Partners for safety within the Process Automation sector. They are fully familiar with safety engineering in the process industries, and provide:

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

You can find more information on our partners on the Internet:  
[www.siemens.com/automation/solutionpartner](http://www.siemens.com/automation/solutionpartner)



The phases of the safety lifecycle

## Simple control system integration / variable fieldbus communication with integrated safety

### Simple integration into control system

Our innovative Safety Instrumented System can be connected to any digital control system (DCS) when using SIMATIC S7-400FH, SIMATIC ET 200M and ET 200S as well as SITRANS P. The facility for integration in our innovative SIMATIC PCS 7 process control system is unique in this context. This combination provides shorter engineering times, a better operating performance, savings from reduced stocking of spare parts, and lower total maintenance costs.

### Common interfacing using proven standards

The proven PROFIBUS DP and PROFIBUS PA fieldbus technology is used when connecting standard and safety-related I/O modules and devices. Safety-related 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 PROFI-safe according to SIL 2 (proven in use).

Safety Integrated fieldbus technology with PROFI-safe permits certified, safety-related communication between controllers, distributed safety I/O and safety-related process instruments. Redundancy or ring structures at all levels of fieldbus communication allow maximum availability.

### Advantages at a glance

- One engineering system for process control and process safety applications
- SIMATIC S7-400FH, one common controller platform for SIMATIC PCS 7 and process safety
- Direct and seamless communication between DCS and SIS
- Automatic integration of various safety-related alarms and messages with time stamping



## Flexible and scalable fault-tolerance / efficient safety lifecycle engineering

### Well thought-out concept for higher availability

The Flexible Modular Redundancy offered by Siemens is an innovative concept for implementing scalable, cost-effective solutions. Multiple fault-tolerance levels can then be implemented exactly where they are required for the respective application.

### Significantly simpler engineering throughout the complete safety lifecycle

The standard and safety programs are generated in the proven SIMATIC Manager – with or without SIMATIC PCS 7. This reduces training requirements in addition to engineering costs. You design the safety section of the program using Continuous Function Chart (CFC) or SIMATIC Safety Matrix, the innovative and convenient tool for safety lifecycle engineering and management. To this end, you use TÜV-certified function blocks from the library in S7 F Systems.

SIMATIC Safety Matrix operating uses the Cause&Effect methodology significantly reducing the overhead for engineering, commissioning and maintenance – with automatic compatibility with IEC 61511.

### Advantages at a glance

- Flexible Modular Redundancy (FMR)
  - I/O and field device redundancy independent of CPU redundancy
  - No time-limited safety operation in event of component failure (degraded mode)
  - Selection of redundancy matching the Safety Instrumented Function (SIF)
  - Safety not a function of redundancy
- SIMATIC Safety Matrix
  - Configuration of safety functions using the proven Cause&Effect methodology
  - Automatic generation of safety logic in CFC
  - User-friendly display of the Safety Matrix on the user interface of SIMATIC PCS 7
  - Simple tracking of modifications
  - Integrated functions for commissioning and maintenance (safety lifecycle)



## 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 safe instrumentation, for example for pressure measurements.

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

Because 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 IEC 61511, S84
- Burner management systems (BMS) according to EN298, NFPA 85
- Fire and gas applications (F&G) according to EN 54, NFPA 72



Range of products for the process industry		
	SIMATIC S7-400FH	Fail-safe, fault-tolerant controllers with a redundant or non-redundant design (up to SIL 3) for the bottom, mid and top performance ranges
	SIMATIC S7-300F	Controller with a non-redundant design (up to SIL 3) for implementing standard and safety-related automation tasks in the bottom and mid performance ranges
	PROFIBUS with PROFIsafe	For standard and safety-related communication on just one bus cable, certified according to IEC 61508 (SIL 3)
	SIMATIC ET 200	<p>ET 200M Modular I/O for multi-channel applications with digital input and output modules as well as analog input modules (up to SIL 3)</p> <p>ET 200S Bit-modular I/O with digital input and output modules as well as safety-related motor starters (up to SIL 3)</p>
	Process instruments/ process devices	<p>Safe process instruments/devices on PROFIBUS PA: SITRANS P DS III (SIL 2) pressure transmitters on PROFIBUS PA with PROFIsafe (proven in use SIL 2)</p> <p>Safe process instruments/devices for connection to ET 200M remote I/Os: Pointek CLS 200/300 analog (SIL 2), Pointek ULS 200 (SIL 1), SITRANS P DS III analog/HART (SIL 2), SITRANS TW series (SIL 1), SIPART PS2, 2/4-wire (SIL 2)</p>
	Engineering	Engineering of safety functions using Continuous Function Chart (CFC) or SIMATIC Safety Matrix (Cause&Effect matrix) and TÜV-certified function blocks (up to SIL 3)
	Applications	<p>Predefined function blocks and faceplates for online valve test to enable preventive valve diagnostics without affecting production</p> <p>Libraries for SIMATIC S7-400FH and S7-300F controllers with TÜV-certified function blocks for burner management systems</p> <ul style="list-style-type: none"> <li>- Partial Stroke Test</li> <li>- Burner libraries</li> </ul>

# 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.

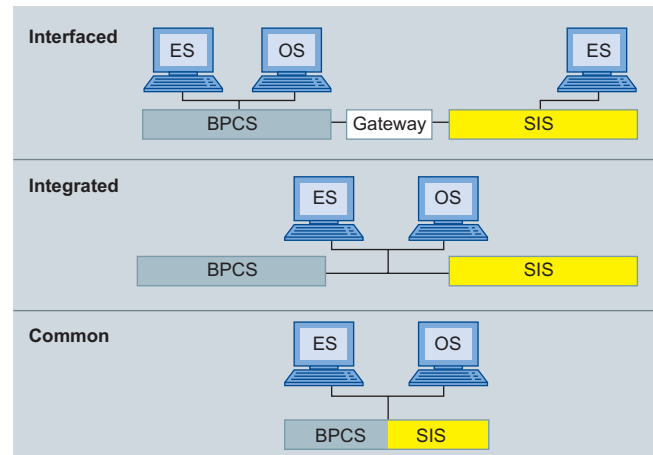
The resulting reduction in required space, scope of hardware and wiring, as well as assembly, installation and engineering overheads results in significant cost savings for the complete lifecycle of the plant.

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. The two systems use separate engineering tools.
- **Integrated**  
The BPCS and the Safety Instrumented System are based on different hardware, but have a uniform communication system and use a common engineering tool.
- **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 process control functions and the safety functions in one controller (automation system) or in separate controllers.



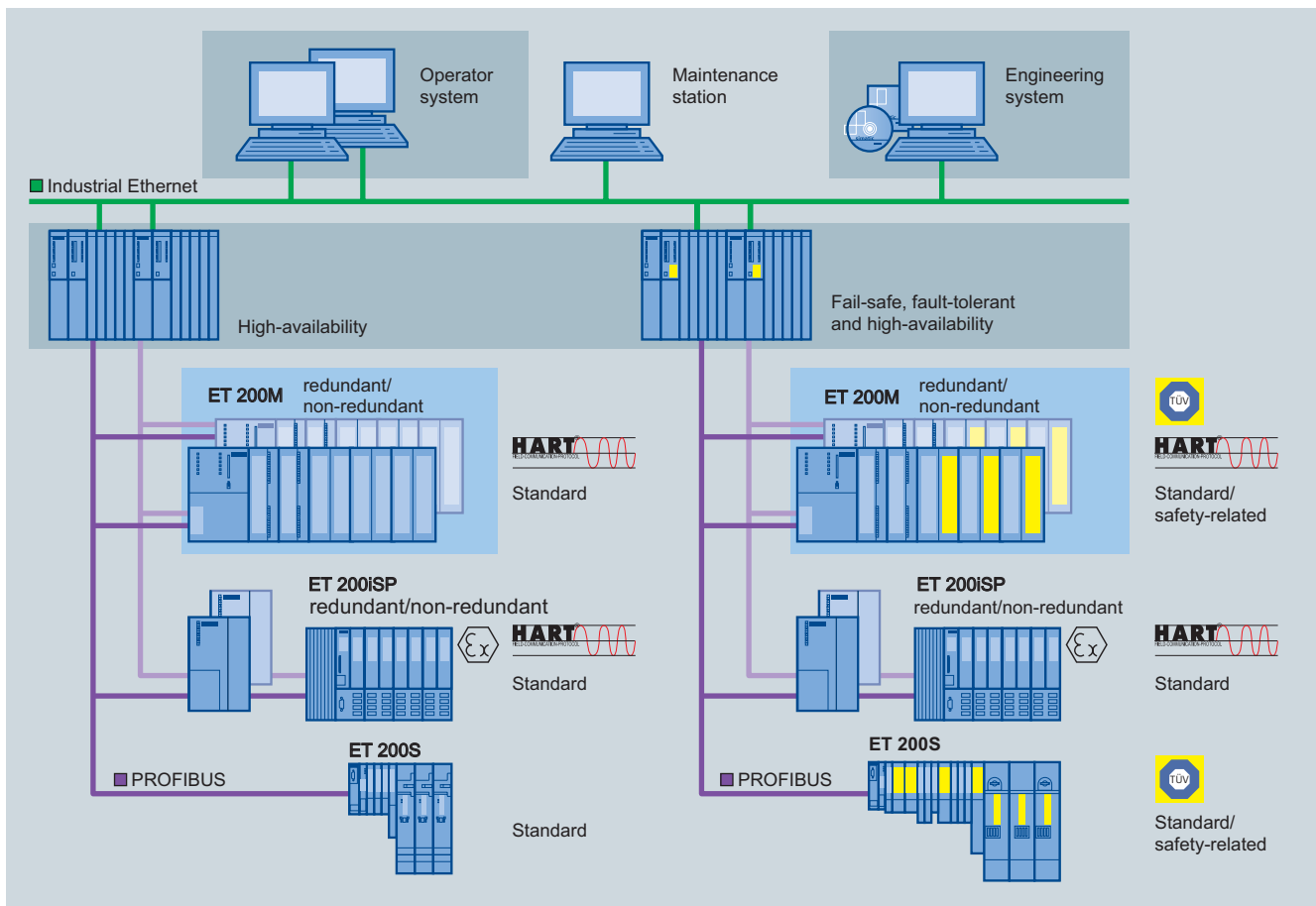
Integration levels of the Safety Instrumented System in the process control system

Many of the benefits of a Siemens Safety Instrumented System can be realized even when it is interfaced to another open control system using standard communication over PROFIBUS. These include:

- Processing of standard and safety functions in one S7-400H controller
- Standard communication and safety-related communication between controller and distributed I/O over PROFIBUS and PROFIsafe instead of a separate safety bus
- Mixed operation of standard and safety-related I/O modules in remote I/O stations of the ET 200M and ET 200S systems

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 engineering system for basic process control and safety-related applications
- Homogenous integration of the safety technology into the automation system of SIMATIC PCS 7
- Integration of the safety-related applications into the convenient process visualization on the SIMATIC PCS 7 operator station
- Automatic consideration of safety-related fault messages in the process visualization, with time stamping



Basic process control system and Safety Instrumented System combined in the SIMATIC PCS 7 process control system

- Uniform data management for basic process control and safety-related automation, including process visualization and diagnostics, therefore no complex data management between BPCS and SIS
- Integration of safety-related hardware into the SIMATIC PCS 7 asset management for diagnostics and preventive maintenance

The safety system usually communicates over the plant bus (with client/server systems also over a terminal bus (OS-LAN) 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 face-plates.

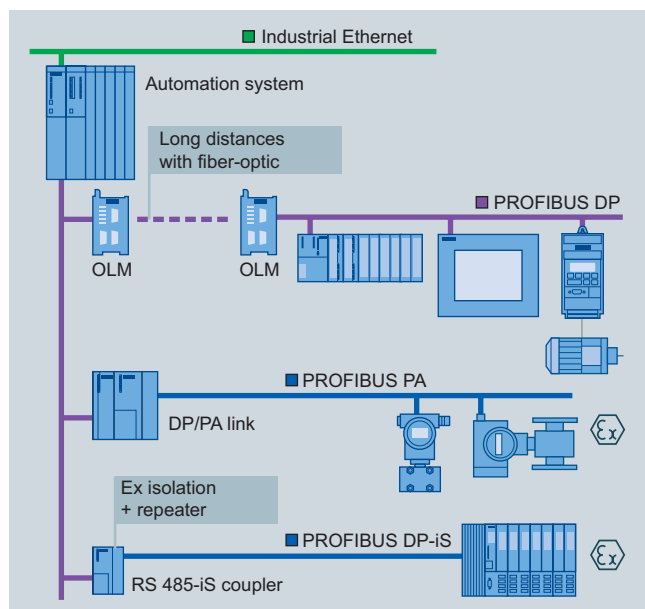
The Safety Integrated System is integrated into the plant bus using rugged Ethernet interface modules in the controllers and Industrial Ethernet Switches such as ESM, OSM or SCALANCE X as suitable for the bus medium used.

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 which are connected together using two pairs of SCALANCE X switches with "standby redundancy".

# Safety Integrated fieldbus technology

## Uniform field communication with flexible PROFIBUS architectures



PROFIBUS transmission systems

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 well suited to these tasks because it enables high-speed communication with the intelligent distributed I/Os by means of a communications protocol (PROFIBUS DP) as well as communication and simultaneous 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

The PROFIBUS PA fieldbus developed for direct linking of sensors and actuators is integrated into 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.

## PROFIsafe – safety-related PROFIBUS communication

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

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

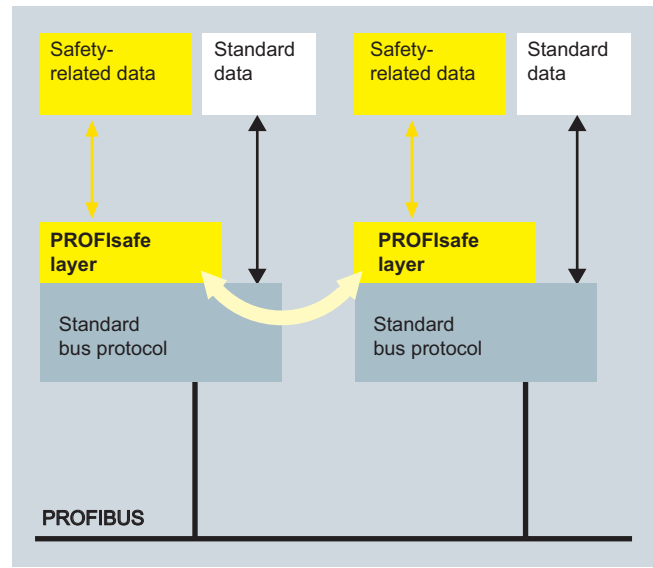
### Further information

For detailed information on PROFIBUS and PROFIsafe, look on the Internet at

[www.siemens.com/profibus](http://www.siemens.com/profibus)

or in the brochure: "PROFIBUS – The perfect fit for the process industry" at

[www.siemens.com/simatic/docu](http://www.siemens.com/simatic/docu)



Standard and safety-related data are transmitted over the same bus line with PROFIsafe. Collision-free communication is possible over a bus system with media-independent network components.

Error	Measure			
	Consecutive number	Time expectation with acknowledgment	Identification of transmitter and receiver	Data security 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 communications partners

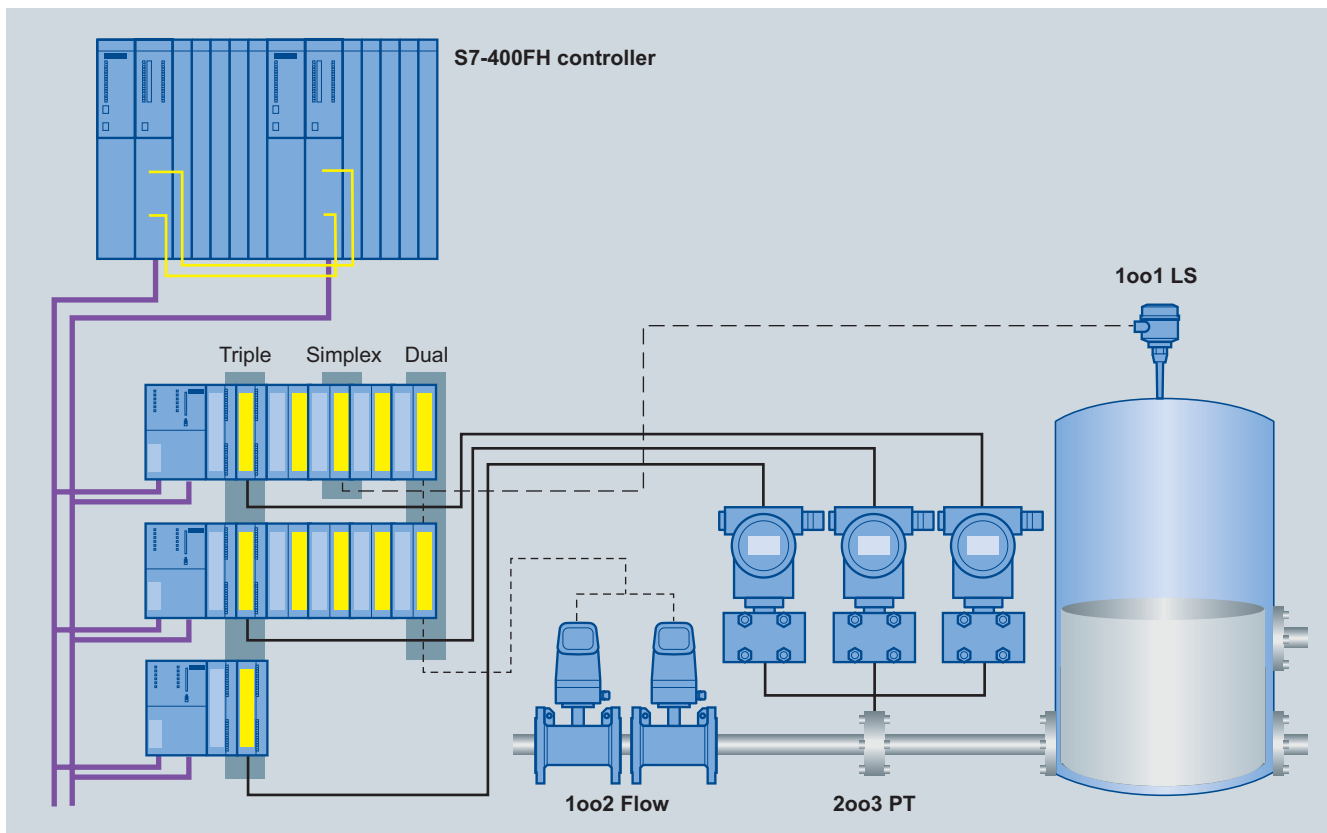
# Flexible Modular Redundancy

## Cost-optimized safety through flexible and scalable fault tolerance

An exceptional feature of Safety Integrated is the Flexible Modular Redundancy (FMR). Depending on the automation task and safety requirements, this allows the configuring engineer to individually define the degree of redundancy for the individual architecture levels comprising 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 additionally comply with the requirements of safety integrity level SIL 3.

You can then implement individual, fault-tolerant architectures exactly tailored to the individual tasks which can tolerate several simultaneously occurring faults. As shown in the example of a plant with ET 200M distributed I/O system, the overall system can accommodate a mixture of different degrees of redundancy within an architecture level (1oo1, 1oo2, 2oo3).

Modeling of the reliability has shown that the Flexible Modular Redundancy from Siemens 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, comparatively more attractive and cost-effective safety applications are possible than with conventional redundancy architectures.



Flexible Modular Redundancy shown by an example of a safety-related, fault-tolerant plant configuration

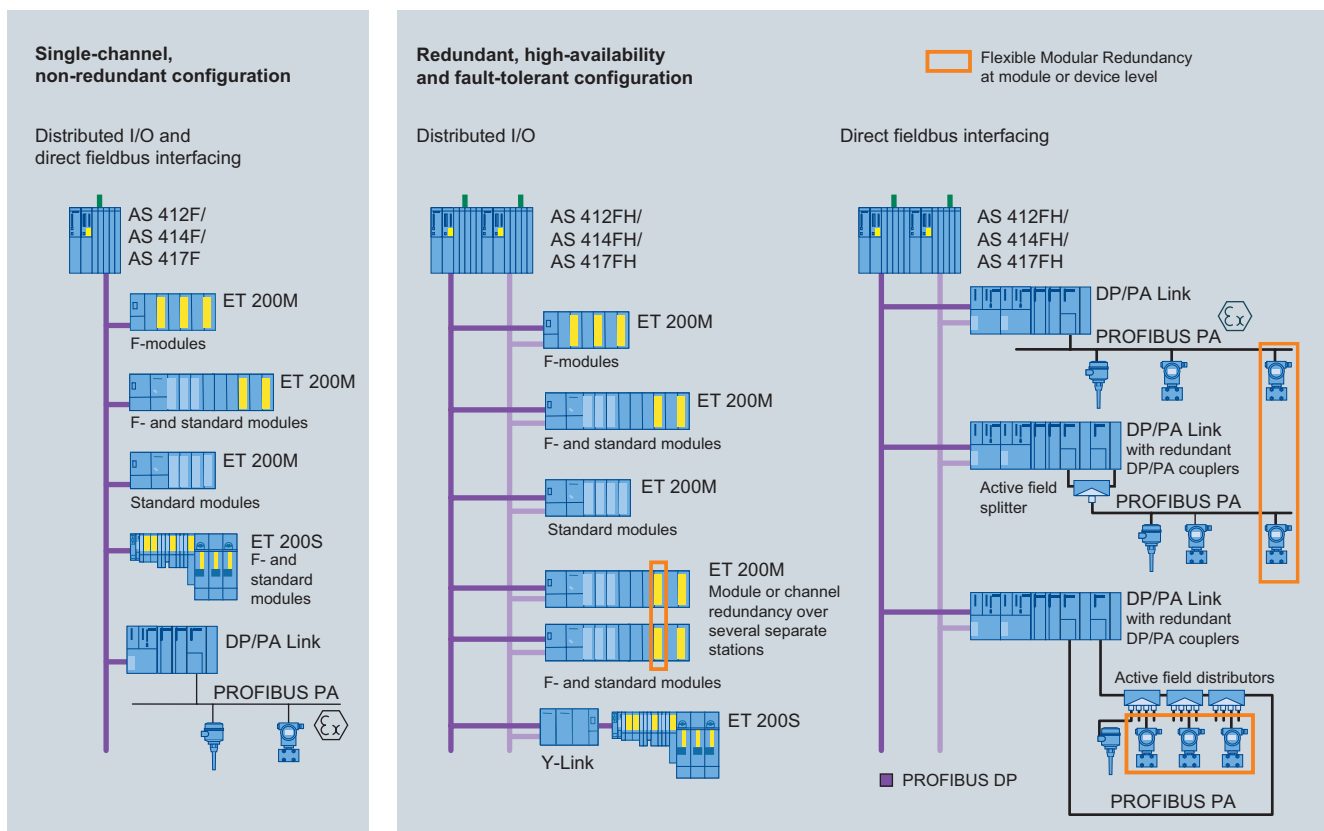
## Configuration options with FMR

Within the overall FMR concept our safety instrumented system configurations can be categorized into two distinct options:

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

The two configuration options are extremely flexible, and offer a wide design scope with respect to different customer specific requirements. You can not only combine standard and safety functions in the I/O area, also in the controller level you are able to combine or separate standard control and safety. The full range of flexibility and scalability is possible with the Flexible Modular Redundancy concept of Siemens.

In the individual architecture levels (controller, fieldbus, I/O) you are offered the configuration alternatives shown in the figure and in the following table depending on the I/O used (remote ET 200M and ET 200S I/O stations or PROFIBUS PA devices according to profile 3.0).



Configuration versions for safety-related systems shown by example of SIMATIC PCS 7 with S7-400H controllers

## Overview of configuration versions

Single-channel, non-redundant configuration		
<b>Controller</b>		Single-channel, equipped with one CPU
<b>Fieldbus</b>	Distributed I/O (remote I/Os)	Individual, single-channel PROFIBUS DP segment with PROFIsafe
	Direct fieldbus interfacing (PA devices)	An individual, single-channel PROFIBUS PA segment is connected to a single-channel PROFIBUS DP segment over a simple router; PROFIsafe is included
<b>Process I/O</b>	Distributed I/O (remote I/Os)	Remote ET 200M and ET 200S I/O stations equipped uniformly with standard or F-modules, as well as those with a mixed configuration on a PROFIBUS DP segment
	Direct fieldbus interfacing (PA devices)	Individual sensors/actuators on a PROFIBUS PA segment with a line or tree topology
Redundant and fault-tolerant configuration		
<b>Controller</b>		High-availability and fault-tolerant, equipped with two redundant CPUs
<b>Fieldbus</b>	Distributed I/O (remote I/Os)	Two redundant PROFIBUS DP segments with PROFIsafe
		Two redundant PROFIBUS DP segments are reduced by a Y-Link to a single-channel PROFIBUS DP segment; PROFIsafe is included
	Direct fieldbus interfacing (PA devices)	An individual, single-channel PROFIBUS PA segment (line/tree) is connected to two redundant PROFIBUS DP segments over a single router; PROFIsafe is included; can be used up to Zone 0 or 1
		An individual, single-channel PROFIBUS PA segment (line) is connected to two redundant PROFIBUS DP segments over an Active Field Splitter (AFS); PROFIsafe is included Automatic switching over of PROFIBUS PA segment to the respectively active coupler of the redundant router per AFS; can be used up to Ex Zone 2
		A PROFIBUS PA ring is connected to two redundant PROFIBUS DP segments over a redundant router; PROFIsafe is included; can be used up to Ex Zone 2
<b>Process I/O</b>	Distributed I/O (remote I/Os)	Remote ET 200M I/O stations equipped uniformly with standard or F-modules, and those with a mixed configuration together on two redundant PROFIBUS segments FMR is possible at the module or channel level using several, separate remote I/O stations
		Remote ET 200S I/O stations equipped uniformly with standard or F-modules, and those with a mixed configuration on two redundant PROFIBUS segments via a Y-Link
	Direct fieldbus interfacing (PA devices)	Individual sensors/actuators on a PROFIBUS PA segment with a line or tree topology FMR possible through grouping of individual devices in different PROFIBUS PA segments
		Individual sensor/actuators are integrated in a PROFIBUS PA ring with automatic bus termination over up to 8 AFDs with 4 short-circuit-proof spur line connections FMR possible through grouping of individual devices on different AFDs

## SIMATIC controller for safety-related process applications

Safety-related SIMATIC controllers are used for critical applications in which an incident can result in danger to persons, plant damage or environmental damage. Working together with the safety-related F-modules of the ET 200 distributed I/O system or directly via fail-safe transmitters connected via the fieldbus, they detect faults both in the process and their own internal faults, and automatically set the plant to a safe state in the event of a fault.

The SIMATIC S7-412FH, S7-414FH and S7-417FH controllers are ideal for implementing safety-related 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 are functionally separate, 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.

SIMATIC S7-300F 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 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 processing is prevented in that the safety-related and BPCS program components remain strictly separated and 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 communications partners are the S7-400FH and S7-300F controllers presented below.



## S7-400FH and S7-300F controllers

### S7-412FH, S7-414FH and S7-417FH controllers

The S7-412FH, S7-414FH and S7-417FH controllers are based on the hardware of the S7-400H controllers, which is extended by the safety functions in the S7 F Systems software package. Single-channel (only one CPU) or fault-tolerant (two redundant CPUs) operation is possible depending on the configuration.

In the context of SIMATIC PCS 7, you can obtain the controllers as preassembled and tested automation systems. These product bundles usually include components such as racks, CPU, power supply, main memory, memory card and Industrial Ethernet interface.

They are available in two configuration versions with the following product names:

- AS 412F, AS 414F or AS 417F as single station with one CPU, safety-related
- AS 412FH, AS 414FH or AS 417FH as redundant station with two redundant CPUs, safety-related and fault-tolerant

The redundant FH systems working according to the 1-out-of-2 principle comprise two subsystems of identical design. To achieve optimum EMC, they are electrically isolated from one another, and 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 present in the same rack, or spatially separated by up to 10 km. Spatial separation provides additional safety gains in the case of extreme effects in the local environment of the active subsystem, e.g. by fire.

The redundancy of the FH systems only serves to increase availability. It is not relevant to processing of the safety functions or the fault detection associated with this.

More information on the Internet:  
[www.siemens.com/fh-cpu](http://www.siemens.com/fh-cpu)



SIMATIC S7-300F controller

### SIMATIC S7-300F controller

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 at the top by the currently most powerful controller S7-319F-3 PN/DP:

- S7-315F-2 DP
- S7-315F-2 PN/DP
- S7-317F-2 DP
- S7-317F-2 PN/DP
- S7-319F-3 PN/DP

Controllers with S7-315F-2 DP or S7-317F-2 DP CPUs are exclusively designed for fieldbus communication over 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 has already become established in the 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 of the ET 200M and ET 200S I/O systems.

More information on the Internet:  
[www.siemens.com/f-cpu](http://www.siemens.com/f-cpu)

## Versatile, distributed I/O systems

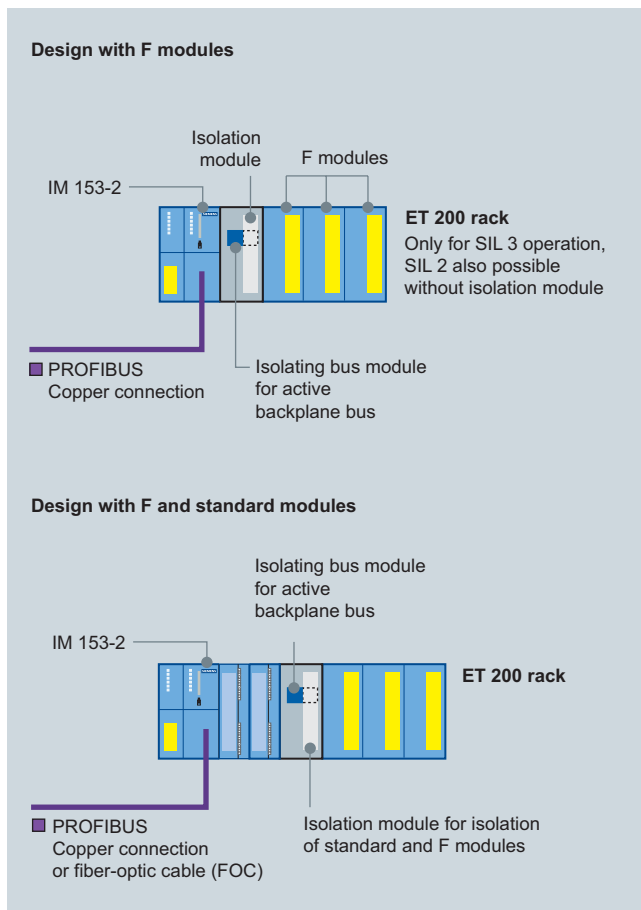
The distributed I/O systems of the Safety Integrated System can be differentiated as follows:

- Modular ET 200M distributed I/O system with IP20 degree of protection, the prime range of remote I/Os for process automation with SIMATIC PCS 7
- Bit-modular ET 200S distributed I/O system with independent wiring and IP20 degree of protection

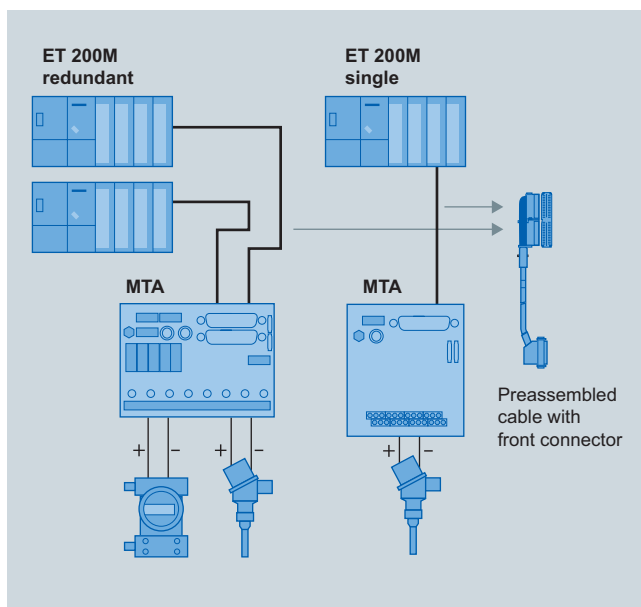
The safety functions of the SIMATIC controllers are perfectly matched to the safety-related F-modules of these I/O systems.

Safety-related, distributed I/O systems	ET 200M	ET 200S
<b>Device characteristics</b>		
For use in hazardous areas	Zones 2 and 22; connected sensors/actuators also in Zones 1 and 21	Zones 2 and 22 (without motor starter)
Redundancy	<ul style="list-style-type: none"> <li>■ PROFIBUS interface</li> <li>■ Module channel (modules in separate stations)</li> </ul>	No
Online modification functions	<ul style="list-style-type: none"> <li>■ Addition of station</li> <li>■ Addition of I/O modules</li> <li>■ Programming</li> </ul>	<ul style="list-style-type: none"> <li>■ Addition of station</li> </ul>
Number of I/O modules	<ul style="list-style-type: none"> <li>■ 12 with IM 153-2 HF</li> <li>■ 8 with IM 153-2 HF FO (fiber-optic)</li> </ul>	63
Mixing of standard and F modules	Station-by-station on the PROFIBUS as well as within a station	Station-by-station on the PROFIBUS as well as within a station
Time stamp functionality	Yes	No
<b>F-modules</b>		
DI	12/24 x 24 V DC 4/8 x NAMUR [EEx ib]	4/8 x 24 V DC
DO	10 x 24 V DC/2 A 8x 24 V DC/2 A	4 x 24 V DC/2 A
AI	6 x 4 to 20 mA, 13 bits + sign 6 x 0 ... 20 mA or 4 ... 20 mA HART, 15 bits + sign	--
Motor starters	--	F-DS1e-x F-RS1e-x
<b>PROFIBUS</b>		
Interface module	IM 153-2 HF IM 153-2 HF FO (fiber optic)	IM 151-1 HF
Order No. stem	6ES7 153-2BA. 6ES7 153-2BB.	6ES7 151-1BA.

## ET 200M



ET 200M configuration



MTA terminal modules

### 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 safety-related F-modules can be mixed with standard modules within a station.

In the case of applications according to SIL 3 and with mixed configurations with standard modules, an isolating module is required on the left of the F-modules. This protects the F-modules in the event of overvoltages.

### MTA terminal modules

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

When using the MTAs, the requirements and costs for cabling and commissioning are significantly reduced, and wiring errors are avoided. They can of course only be used in the context of SIMATIC PCS 7.

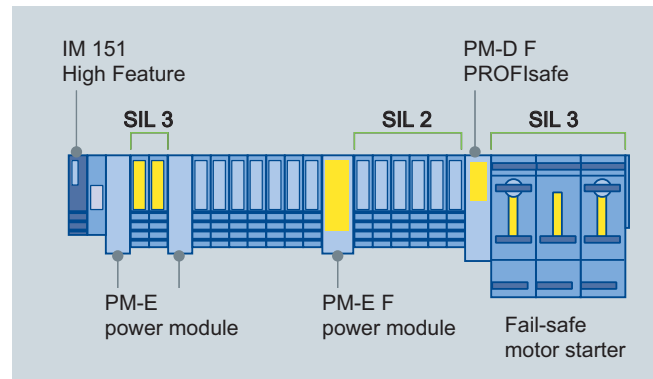
## ET 200S

### ET 200S configuration

With an ET 200S station, up to 63 I/O modules (power modules, electronics modules, motor starters and expansion modules) can be inserted between the interface module and the terminating module. Further configuration limits are the width of up to 2 m, the max. address range of 244 bytes for input data and the same for output data, as well as the limiting of parameters to a maximum of 244 bytes per station.

Power modules are suitable for configuring the I/O modules in potential groups. A power module together with its following I/O modules constitute a potential group in each case, whose scope is limited by the current carrying capacity of the power module (up to 10 A depending on the type). The power module handles the monitoring and also - depending on the version - the fusing of the power supply for this potential group.

The first power module must be positioned directly following the interface module.



ET 200S configuration

Which power module (PM) is used in each case depends on the application and the I/O modules used in it. The power modules listed in the table are relevant to safety-related applications.

An ET 200S station can be configured rapidly and simply using the SIMATIC ET 200 Configurator. This is acquainted with the configuration rules, and provides interactive support for selection of all components and the matching accessories. The SIMATIC ET 200 Configurator is available on the Internet at: [www.siemens.com/et200](http://www.siemens.com/et200)

Power module	Use	Achievable safety (AK/SIL)	Appropriate I/O modules
PM-E F pm DC 24 V PROFIsafe (pm for earth-free loads; ground and earth separated)	Safe shutdown of subsequent standard DO modules 24 V DC	AK4/SIL 2	All non-safety-related standard electronics modules 24 V DC
PM-E F pp DC 24 V PROFIsafe (pp for grounded loads; ground and earth connected together)			
PM-E DC 24 V	Supply of F-DI modules and F-DO modules	AK4/SIL 2	All electronics modules (safety-related and standard modules) in the respective voltage range
PM-E DC 24 ... 48 V/AC 24 ... 230 V		AK6/SIL 3 <sup>1)</sup>	
PM-D F DC 24 V PROFIsafe	Safe shutdown of F-motor starters	AK6/SIL 3	<ul style="list-style-type: none"> <li>■ Safety-related (F) motor starters F-DS1e-x and F-RS1e-x with or without Brake Control xB1 and xB2 expansion modules</li> </ul>
		AK4/SIL 2	<ul style="list-style-type: none"> <li>■ Safety-related (F) motor starters F-DS1e-x and F-RS1e-x with or without Brake Control xB3 and xB4 expansion modules</li> </ul>

<sup>1)</sup> Only AK4/SIL 2 can be achieved when mixing standard and F modules within a potential group.

## Process I/O for ET 200M and ET 200S



F-AI HART analog input module for ET 200M (6 x 0/4 ... 20 mA)

### F-modules

The F-signal modules of ET 200M and ET 200S (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 open-circuit, and automatically monitor the discrepancy time defined in the parameter settings.

Depending on the version, the input modules support 1oo1 and 2oo2 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.

### F-AI HART analog input module for ET 200M

The F-AI HART analog input module with 6 inputs for current measurements in the range from 0 to 20 mA or 4 to 20 mA is the first safety-related ET 200M module with the compact width of 40 mm. All 6 channels of the module are designed for SIL 3. When using F-AI HART modules instead of older F-AI modules with twice the width, the achievable packing density is four times as high.

The module is also suitable for HART communication with HART field devices. The HART communication can be switched off safety-related.

The function example "F Systems: Wiring and Voting Architectures for ET 200M F-AIs" on the Internet shows wiring and evaluation architectures for safety-related analog signals. See [www.siemens.com/process-functional-examples](http://www.siemens.com/process-functional-examples)

### F-motor starters

Initiated by a switch-off signal, safety-related ET 200S motor starters can be selectively switched off by the series-connected PM-D F PROFIsafe power module. In addition to a circuit-breaker/contactors combination, the ET 200S motor starters have a safe electronic evaluation circuit for fault detection. If the contactor to be switched in the case of an emergency stop fails, the evaluation electronics detects a fault and deactivates the circuit-breaker in the motor starter in a safety-related manner.

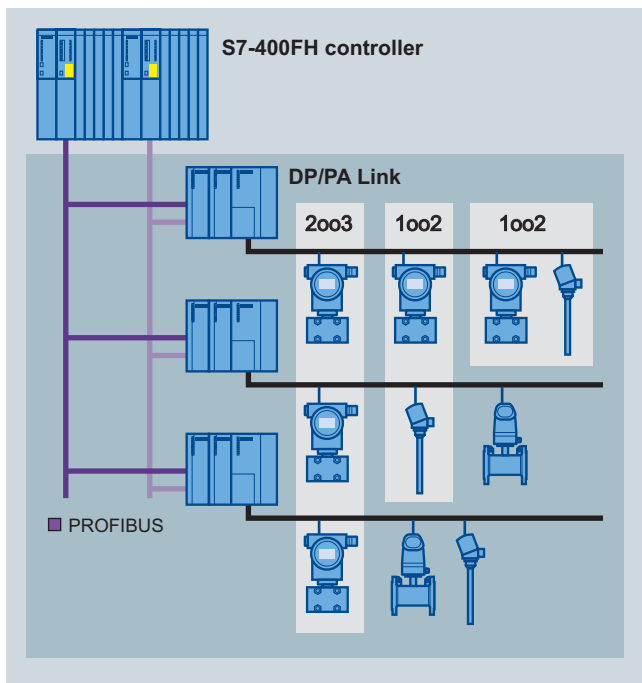
### Safe process instruments and process devices for connection to ET200 remote I/Os

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

Process instrument/ process device	Safety Integrity Level (SIL)
<b>Pressure measurement</b>	
SITRANS P DS III analog/HART	SIL 2
<b>Temperature measurement</b>	
SITRANS TW series	SIL 1
<b>Level measurement</b>	
Pointek CLS 200 analog	SIL 2
Pointek CLS 300 analog	SIL 2
Pointek ULS 200	SIL 1
<b>Position control</b>	
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/fielddevices](http://www.siemens.com/fielddevices)

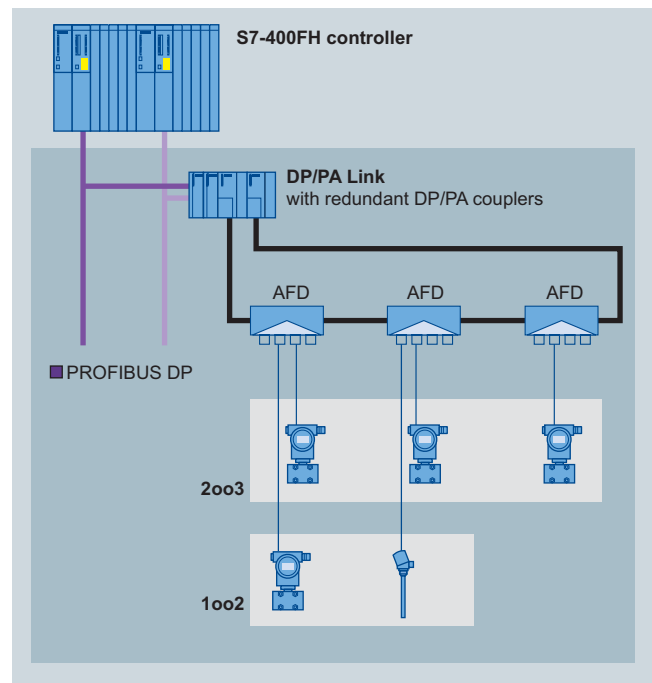
## Direct device interfacing via fieldbus with high safety and availability



Example of previously standard safety-related and fault-tolerant PROFIBUS PA configurations

For plant areas up to hazardous Zone 2, redundant routers together with a PROFIBUS PA of ring topology permit 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. Each of the maximum 8 Active Field Distributors (AFD) in this PROFIBUS PA ring with automatic bus termination has 4 short-circuit-proof spur lines for connection to devices.



Safety-related and fault-tolerant architecture based on a PROFIBUS PA ring topology

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 AFDs expands the existing possibilities for communication and cable diagnostics, and makes fault locating easier in the event of an open-circuit.

The concept of Flexible Modular Redundancy is thus implemented down to the field level.

## Safe field instrumentation on the PROFIBUS PA

### PROFIBUS PA devices for implementation of safety shutdowns

The SITRANS P DSIII digital pressure transmitter is the first PROFIBUS PA device available on the market for SIL 2 safety shutdowns according to IEC 61508/ IEC 61511-1. To this end, Siemens has extended its standard measuring equipment for pressure, absolute pressure and differential pressure by 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 integrity 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.



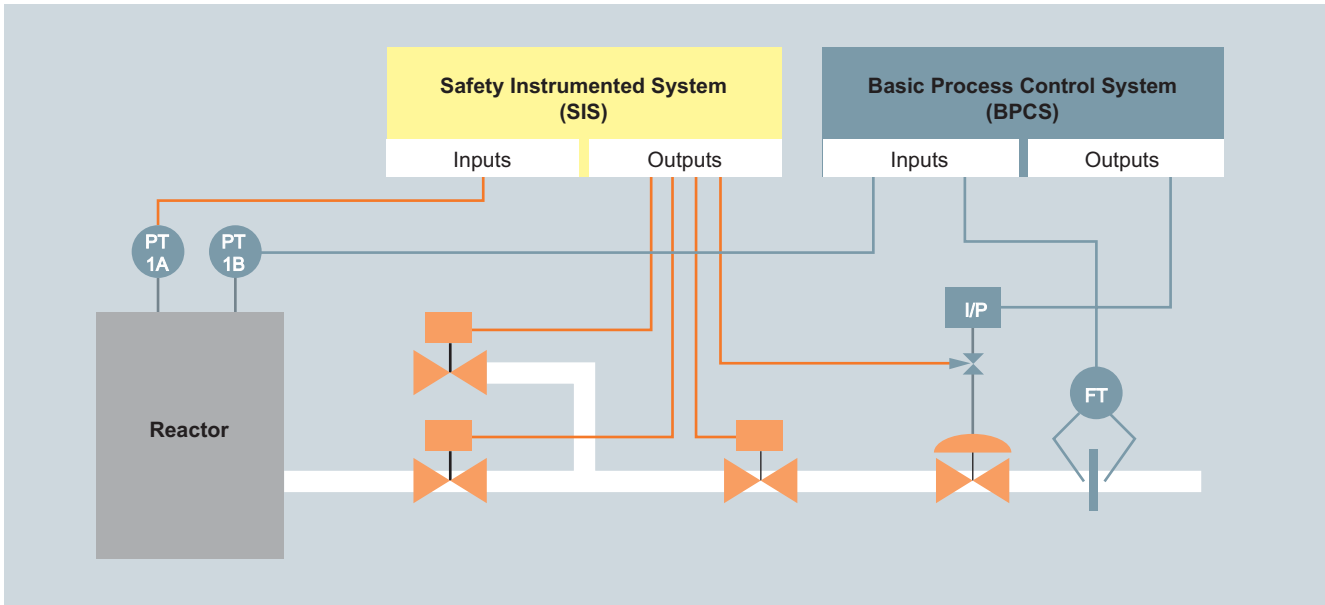
SITRANS P DSIII PROFIsafe pressure transmitter

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](http://www.siemens.com/sitransp)

# Safety lifecycle management

## Analysis phase



Safety Instrumented Function (SIF) in the SIS

The safety lifecycle is divided into three phases according to IEC 61511: analysis, realization and operation/maintenance.

Safety lifecycle management always commences in that the process concept, the functional safety management plan and the historical recordings are examined in order to determine known or potential safety risks.

In a second step, the results are subject to a risk analysis. The objective is to filter out the non-tolerable risks, to rate the probability for the occurrence of a hazard, and to estimate the possible consequences. Various methods are available to this end, e.g.:

- HAZOP
- Danger tree analysis
- Checklists
- FMEA (Failure Modes and Effects Analysis)

Various tools available on the market effectively support the risk analysis through automation of the described procedures.

The result of the risk analysis is documented in the safety requirements specification. This is the basis for subsequent plant planning.

The probability of a safety-relevant event and its effects can be reduced by appropriate protection measures (LOPA, Layer of Protection).

A possible protective measure is the use of a Safety Instrumented System (SIS). The SIS is an independent safety system comprising components ranging from sensor over controller to final element. It is suitable for the following purposes:

- Shutdown: a process or plant is automatically driven to a safe state when a predefined condition is violated.
- Tolerance: under defined conditions, the plant can still be operated safely.
- Reduction: possible consequences of a safety event are minimized and thus limited.

The achievable risk reduction factor will increase with higher SIL level

Safety Integrity Level	Probability of failure on demand (PFD) per year <sup>1)</sup>	Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	10 000 to 100 000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	1 000 to 10 000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	100 to 1 000
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	10 to 100

<sup>1)</sup> Low demand mode of operation

## Realization phase

The realization phase is characterized by selection of the technology and architecture, definition of the proof test interval, the design and installation of the SIS, as well as commissioning.

Siemens provides the F-block library in S7 F Systems and the SIMATIC Safety Matrix for configuration and programming of the S7-400FH controllers.

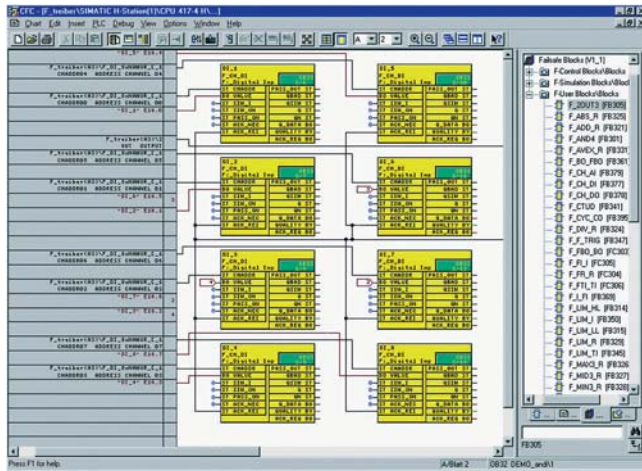
### S7 F Systems with F-block library and Safety Matrix

The S7 F Systems engineering tool permits parameterization of the S7-400FH systems and the safety-related F-modules from the ET 200 series.

It supports configuration by means of functions for:

- Comparison of safety-related F-programs
- Recognition of changes in the F-program using the checksum
- Separation of safety-related and standard functions

Access to the F-functions can be password-protected. The F-block library integrated in S7 F Systems contains predefined function blocks for generation of safety-related applications with the CFC or the SIMATIC Safety Matrix based on it. The certified F-blocks are extremely robust and intercept programming errors such as division by zero or out-of-range values. They save the necessity for performing diverse programming tasks for detecting and reacting to errors.



Engineering of safety-related applications using CFC

### SIMATIC Safety Matrix

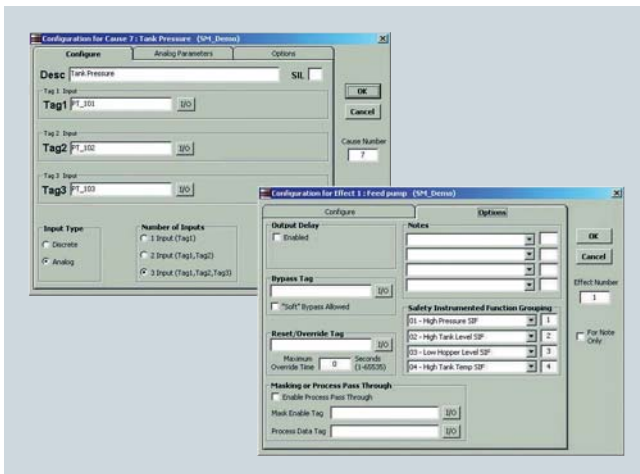
The SIMATIC Safety Matrix which can be used in addition to CFC is an innovative safety lifecycle tool from Siemens which can be used for convenient configuration of safety applications and also for their operation and servicing. Based on the proven principle of a Cause&Effect matrix, the tool is highly suitable for processes where defined statuses require specific safety reactions.

Input Tag	Func	Limit/Trip	EngUnit	Cause Description	Action	Output Tag	Effect Description
PS_100		FALSE		Feed Pump High Pressure Switch	1	N	Feed pump
LSH_100		TRUE		Tank_100 Level switch high	2	2S	Feed block valve
LSL_200		TRUE		Hopper_200 Level switch Low	3	N	Feed block valve
PSH_200		TRUE		Hopper_200 High Pressure	4	N	Hopper Feed block valve
PT_100		H 38.00	PSIG	Feed pressure	5	S	Tank Drain block valve
LT_100		H 50.00	Feet	Tank Level	6	2S	ESD Shutdown
PT_101		H 26.00	D 3.0	Tank Pressure	7	N	Tank restrainer
PT_102	Vote	H 26.00	in_H2O	Tank Pressure	7	N	Tank restrainer
PT_103		H 26.00	in_H2O	Tank Pressure	7	N	Tank restrainer
LT_200		H 50.00	FI	Hopper Level	8	2S	Tank restrainer
TS_101		FALSE		Tank_100 High Temperature switch	9		Tank restrainer
TS_102	AND	FALSE		Tank_100 High Temperature switch	9		Tank restrainer
TS_103		FALSE		Tank_100 High Temperature switch	9		Tank restrainer

Safety Matrix: assignment of exactly defined reactions (effects) to occurring events (causes)

The SIMATIC Safety Matrix not only means that programming of the safety logic is significantly simpler and more convenient, but also much faster than in the conventional manner. During the risk analysis of a plant, the configuration engineer can assign exactly defined reactions (effects) to events (causes) which may occur during a process.

The possible process events (inputs) are initially entered in the horizontal lines of a matrix table comparable to a spreadsheet program, and then their type and quantity, logic operations, any delays and interlocks as well as any tolerable faults are configured. The reactions (outputs) to a particular event are then defined in the vertical columns.

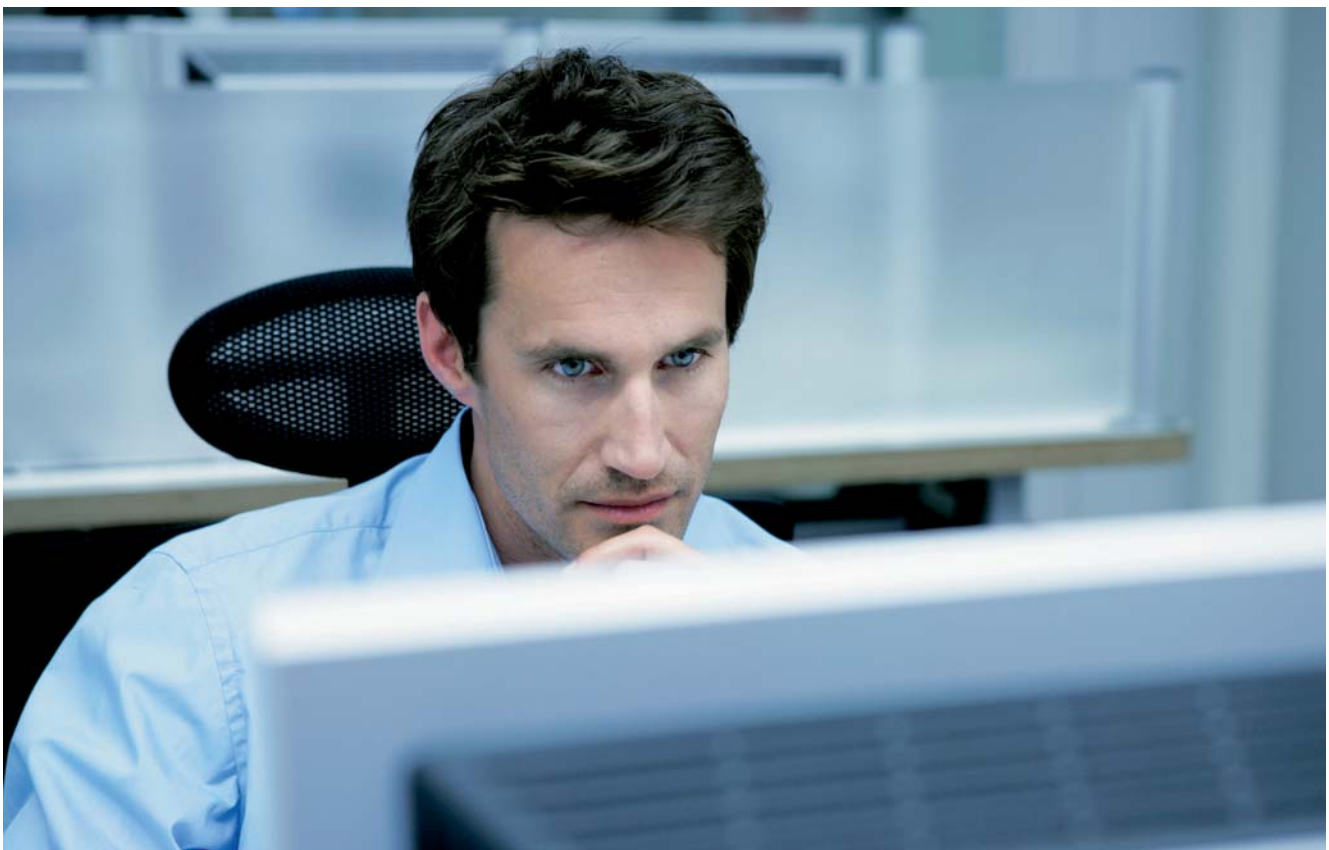


Input window for configuration of analog or digital causes as well as their digital effects

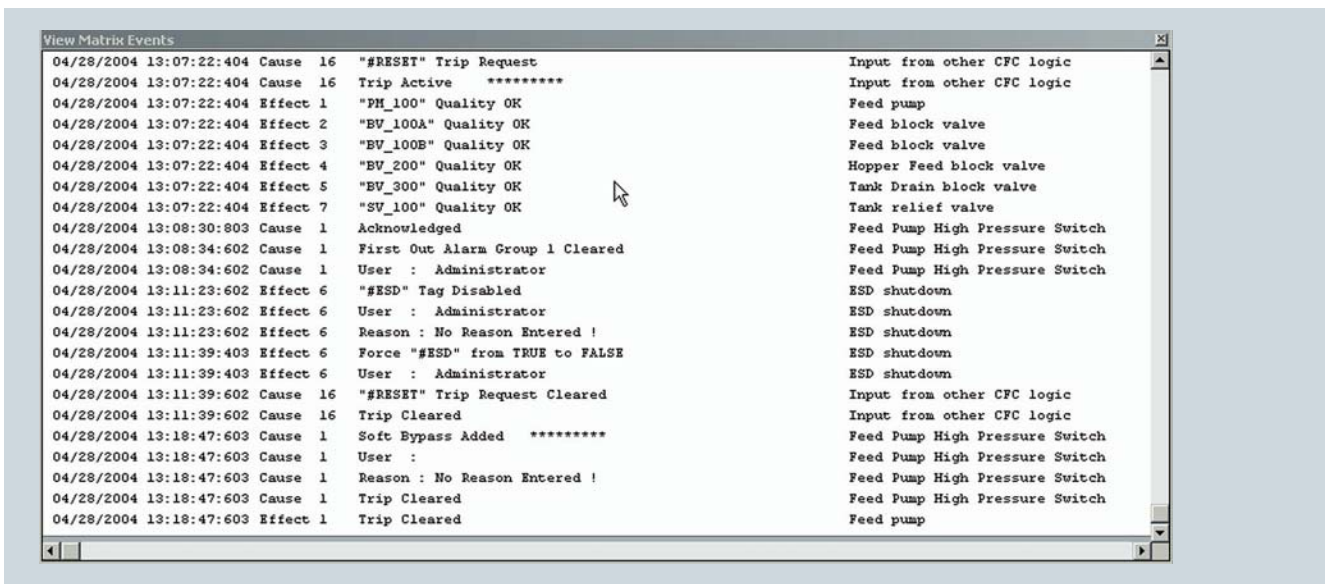
The events and reactions are linked by simply clicking the cell at the intersection point of line and column. Using this procedure, the Safety Matrix automatically generates complex, safety-related CFC programs. Configuration engineers require no special programming knowledge, and can concentrate fully on the safety requirements of their plants.

### Advantages of the Safety Matrix in the realization phase

- Simple programming using Cause&Effect method
- No programming knowledge required
- Automatic generation of CFCs including driver blocks
- Automatic version tracking
- Integral tracking of changes
- 1-to-1 printout of Cause&Effect matrix



## Operation and maintenance phase



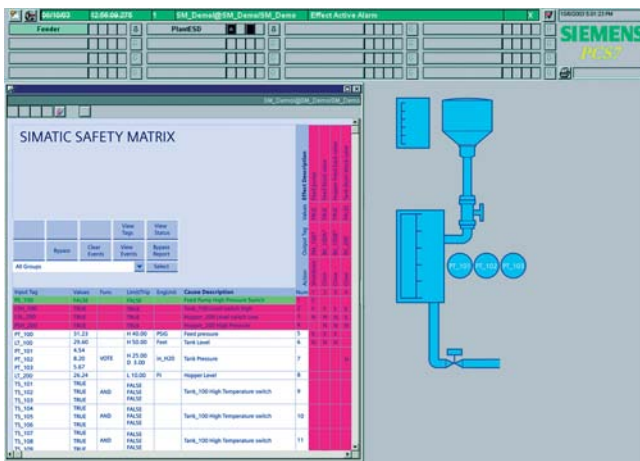
Documentation of changes with the Safety Matrix

The third and final phase of the safety lifecycle comprises operation, maintenance and modification of the safety application as well as plant decommissioning.

The Viewer of the SIMATIC Safety Matrix which can be used on the SIMATIC PCS 7 operator station permits simple and intuitive operation and monitoring of the safety application during runtime. The signal status is displayed online in the Cause&Effect matrix.

The operator can display and save first-up signals and also record safety-relevant events. Changes in parameters are supported, as are bypass, reset and override functions.

Safety lifecycle management functions for version management and for documentation of operator interventions and program modifications effectively supplement the configuration, operation and servicing functions of the SIMATIC Safety Matrix and also the safety lifecycle management.

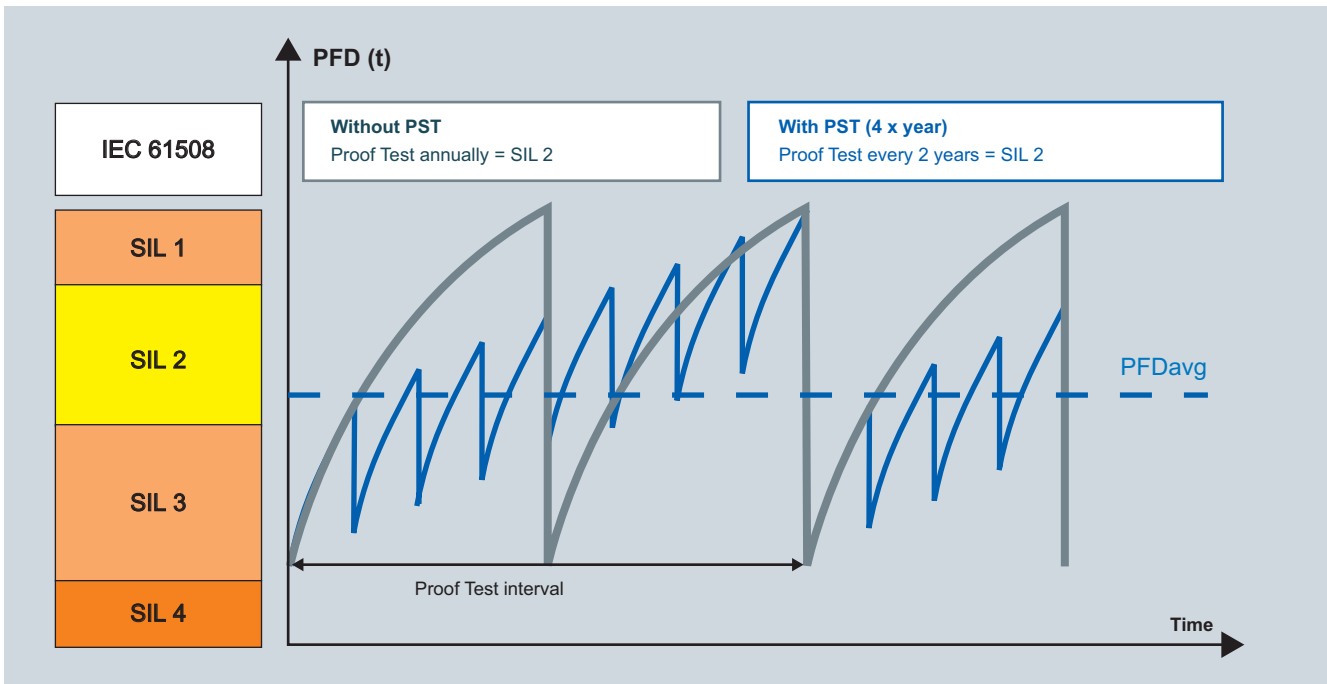


Viewer of the Safety Matrix on a SIMATIC PCS 7 operator station

### Advantages of the Safety Matrix in the operation phase

- Complete integration in SIMATIC PCS 7
- First-up alarm display and saving
- Integral operating functions such as bypass, reset, override and parameter modification
- Sequence of event display and saving
- Automatic saving of operator interventions for the safety lifecycle management
- Automatic version tracking
- Automatic documentation of modifications





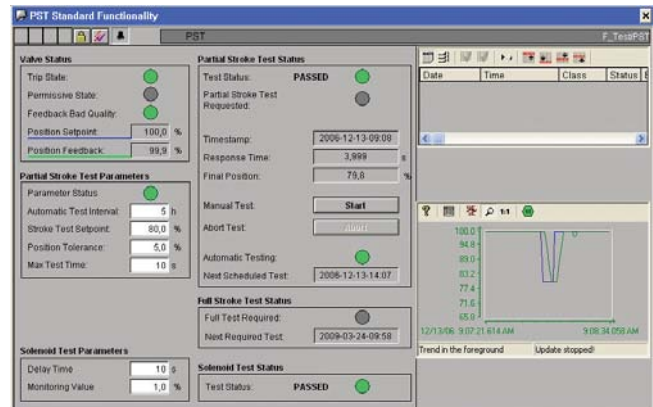
Partial Stroke Test extends the test interval for the Full Stroke Test from one to two years

#### Function blocks

- F\_PST carries out the Partial Stroke Test
- PST provides the alarms and events for the operator station
- Option: F\_SOLENOID tests the solenoid valve
- Option: PST\_CALC calculates the time of the next Full Stroke Test

#### Advantages of the Partial Stroke solution from Siemens

- Online valve test without interfering with production
- Test covering different types of failure
- Preventive diagnostics
- More flexible tests and longer test intervals
- Minimization of duration for bypassing the ESD valve or for process shutdown
- Lower failure probability of valve when required
- Feedbacks concerning Full Stroke Tests required to retain the SIL



Faceplate for the SIMATIC PCS 7 operator system

# High Integrity Pressure Protection Systems (HIPPS), Fire & Gas and Burner Management

## High Integrity Pressure Protection System (HIPPS)

The High Integrity Pressure Protection System is the specific application of a Safety Instrumented Systems (SIS) for protection against overpressure. It can be used as an alternative to pressure reducers according to API 521 and ASME code 2211, Section VIII, Paragraphs 1 and 2.

On the basis of the Safety Integrated Systems, Siemens has developed complex HIPPS solutions for various applications in cooperation with solution providers:

[www.siemens.com/process-safety](http://www.siemens.com/process-safety)

## Burner Management Systems

Burner Management Systems (BMS) are defined according to EN 298 and NFPA 85 (2001) as "Control systems for safe combustion, for supporting operating personnel when starting-up and shutting-down fuel conditioning and firing plants, and for preventing malfunctions and damage on these plants".

Their wide range extends from very small systems for boilers with single burners up to very large systems for power plant boilers.

Siemens offers burner libraries as well as complete solutions with TÜV-certified function blocks for the SIMATIC S7-400FH and S7-300F controller platforms.



Example of a control cabinet configuration

## Fire and gas

Systems for protection against fire and gas play an important role in the total protection concept of industrial plants for exploitation, processing and transportation of petroleum, petrochemicals or dangerous gases.

They must reliably detect and signal fires and/or gas leakages, even under adverse conditions such as failure of the main power supply. To reduce subsequent damage, they are also partially able to automatically initiate appropriate counter-measures such as firefighting or drawing out of a gas. The Safety Integrated System is certified for this in line with the required safety standards EN 54 and NFPA 72.

# Reference projects

## References in the oil & gas and chemical industries

Whether during power generation, oil and gas exploitation, in refineries, in the chemical, petrochemical or pharmaceutical industries: on the basis of our sound know-how and comprehensive experience, we have already implemented a large number of turnkey process safety solutions. These have proven themselves in everyday use worldwide.

### Energy:

#### Afam gas purification plant of the Shell Petroleum Development Company (SPDC) Nigeria

SPDC has installed a gas conditioning plant to guarantee the quality of gas supply to an existing State owned 270 MW power station, subject to a sale & purchase agreement with SPDC, and to an SPDC new build 650 MW power station due on stream in Mid 2007.

SPDC Nigeria chose the integrated, fault-tolerant and redundant safety and process control system PCS 7 for the 190 mmscf/d gas conditioning plant. The system controls all emergency shut downs as well as the fire detection system and gas leak detection system and has to comply strictly to safety standards.

### The solution

- Process control system SIMATIC PCS 7 with SIMATIC Safety Integrated
- Fault-tolerant and highly available SIMATIC S7-400FH controller – with two fiber optic cables connected CPUs – Type 417-4H, as well as communication processors for the connection with PROFIBUS and Ethernet
- Over two interface modules IM 153-2 High Feature, decentralized I/Os of the periphery system ET 200M are connected to PROFIBUS: seven I/O lines for measuring field signals out of the Safety Instrumented System, Fire and Gas as well as out of the common process automation
- Safety-engineering and Safety Lifecycle Management via SIMATIC Safety Matrix
- Foot print optimized and cost-effective system architecture thanks to Flexible Modular Redundancy

Especially important was the application of the SIMATIC Safety Matrix. This efficient engineering tool simplifies the design and implementation of the safety relevant application. Furthermore it supports important parts of the Safety Lifecycle of the system – from design and realization through to the operation and maintenance phase.



Afam gas purification plant of the Shell Petroleum Development Company (SPDC) Nigeria

### Refinery:

#### Hydrocracker at Repsol YPF in Tarragona, Spain

A further project in which Siemens could prove its sector competence was the automation of the hydrocracker for Repsol YPF in the refinery in Tarragona, Spain. The hydrocracker converts the impressive quantity of 24 000 barrels of petroleum into higher-quality products every day. The demands placed on the SIS were correspondingly high. The tasks: interlocking of the two furnaces, motor control and monitoring of tank levels, as well as emergency shutdown of five compressors for controlling the exhaust stack and the furnaces.

### The solution

- SIMATIC PCS 7 process control system with SIMATIC Safety Integrated
- Two SIMATIC S7-400FH controllers
- 1 900 safety-related inputs and outputs with SIMATIC ET 200M remote I/Os
- Plant configuration

The two SIMATIC S7-400FH controllers ensure that the plant operates within the approved range at all times. Using the new hydrocracker, Repsol YPF could significantly increase its production of petrol, diesel and other high-quality petrochemical products. The fuels from Tarragona of course also satisfy the EC environmental directives.



Bayer in Dormagen, Germany

### Chemical industry: production of pesticides at Bayer in Dormagen, Germany

In their new multipurpose plant in Dormagen, it was particularly important for Bayer Crop Science AG to produce a uniformity with SIMATIC PCS 7 from the field level up to the ERP level (SAP). Bayer decided in favor of a control system solution with integral safety technology – for 35 process plants, 240 sub-systems and 4 500 measuring points.

#### The solution

- SIMATIC PCS 7 process control system with SIMATIC Safety Integrated
- 53 SIMATIC S7-400FH controllers
- 1 000 safety-related inputs and outputs with SIMATIC ET 200M remote I/Os
- Plant configuration

Safety Integrated results in a reduction in engineering costs over the complete lifecycle of the multipurpose plant. Thanks to its high degree of flexibility, production can be adapted to modified requirements significantly simpler and faster. Maintenance and modification work has become much more simple as a result of the unit-specific assignment of the controllers (one controller per plant unit).



Statoil offshore platform, Norway

### Oil and gas: Statoil offshore platform, Norway

In order to completely satisfy all safety-critical requirements for its Huldra unmanned offshore oil platform in the North Sea, Statoil, the largest Norwegian mineral oil company, relies on fire and gas warning systems as well as emergency shut-down systems. One of the reasons: The SIMATIC S5 system already installed proved its excellence in the past.

#### The solution

- Five SIMATIC S7-400FH controllers
- 3 000 safety-related inputs and outputs via SIMATIC ET 200M
- Plant configuration

The project was the beginning of a new controller generation with integral safety engineering at Statoil. Since then, 20 further platforms have been equipped with SIMATIC S7-400FH. The large economical advantage: the user programs could be reused for all platforms.

# Overview of product and ordering data

## S7-400FH controllers

**SIMATIC S7-400FH controllers as AS bundles for SIMATIC PCS 7**  
(preferred configurations including S7 F Systems RT license)

AS types	AS 412F	AS 414F	AS 417F	AS 412FH	AS 414FH	AS 417FH
CPU redundancy	No, 1 CPU			Yes, 2 CPUs (fault-tolerant)		
Basic hardware	AS 412-3-1H	AS 414-4-1H	AS 417-4-1H	AS 412-3-2H	AS 414-4-2H	AS 417-4-2H
Order No. stem of hardware	6ES7 654-8AB01-3BX. / -3GX. 6ES7 654-8AB02-3BX. / -3GX.	6ES7 654-8CF01-3BX. / -3GX. 6ES7 654-8CF02-3BX. / -3GX.	6ES7 654-8EN01-3BX. / -3GX. 6ES7 654-8EN02-3BX. / -3GX.	6ES7 656-8AB31-1EX. / -1GX. 6ES7 656-8AB32-1EX. / -1GX.	6ES7 656-8CF31-1EX. / -1GX. 6ES7 656-8CF32-1EX. / -1GX.	6ES7 656-8EN31-1EX. / -1GX. 6ES7 656-8EN32-1EX. / -1GX.

In the context of SIMATIC PCS 7, the SIMATIC S7-400FH controllers are available as completely assembled and tested AS bundles. By selecting preconfigured ordering units, you can define the configuration of the AS bundles and their order numbers in interactive mode.

A configurator available in the catalog and in the online ordering system on the Internet ([www.siemens.com/automation/mall](http://www.siemens.com/automation/mall)) provides you with effective support. In order to help you when selecting preferred configurations, these are listed additively together with their complete order number.

The ordering units of the AS bundles and the preferred configurations are also listed in the SIMATIC PCS 7 Catalog ST PCS 7. The ordering data of the individual components are listed in the Catalogs ST PCS 7 and ST 70. Both catalogs are available on the Internet at:

**[www.siemens.com/simatic/printmaterial](http://www.siemens.com/simatic/printmaterial)**

### SIMATIC CPU S7-400H

CPU type	CPU 412-3H	CPU 414-4H	CPU 417-4H
Component of the AS bundle	AS 412F (1 x) / AS 412FH (2 x)	AS 414F (1 x) / AS 414FH (2 x)	AS 417F (1 x) / AS 417FH (2 x)
Technical setup	S7-400 with distributed I/O	S7-400 with distributed I/O	S7-400 with distributed I/O
Load memory, RAM (integrated / memory card)	256 KB / up to 64 MB	256 KB / up to 64 MB	256 KB / up to 64 MB
Main memory <ul style="list-style-type: none"> <li>■ Total</li> <li>■ For program</li> <li>■ For data</li> </ul>	768 KB 512 KB 256 KB	2.8 MB 1.4 MB 1.4 MB	30 MB 15 MB 15 MB
Execution time	75 ns	45 ns	18 ns
Number of F I/Os	Approx. 100	Approx. 600	Approx. 3 000
Bit memories	8 KB	8 KB	16 KB
Integrated interfaces <ul style="list-style-type: none"> <li>■ Number and type</li> <li>■ Number of DP segments</li> </ul>	1 (MPI/DP) 1	2 (MPI / DP and DP) 2	2 (MPI / DP and DP) 2
Dimensions (WxHxD) in mm	50 x 290 x 219	50 x 290 x 219	50 x 290 x 219
Order No. stem	6ES7 412-3H.	6ES7 414-4H.	6ES7 417-4H.

## S7-300F controllers / software components

### SIMATIC S7-300F controller

CPU type	CPU 315F-2 DP	CPU 315F-2 PN/DP	CPU 317F-2 DP	CPU 317F-2 PN/DP	CPU 319F-3 PN/DP
Technical setup	S7-300 with distributed I/O or central, safety-related I/O				
Load memory (plug-in)	64 KB to 8 MB		64 KB to 8 MB		8 MB
Main memory	192 KB	256 KB	1 MB		1.4 MB
F operations	36 K	50 K	200 K		280 K
Number of F I/Os	Approx. 300		Approx. 500		Approx. 1 000
Bit memories	2 KB		4 KB		8 KB
Fieldbus connection	PROFIBUS (DP)	PROFIBUS (DP), PROFINET (PN)	PROFIBUS (DP)	PROFIBUS (DP), PROFINET (PN)	PROFIBUS (DP), PROFINET (PN)
Integrated interfaces ■ Number and type ■ Number of DP segments	2 (MPI and DP) 1	2 (DP/MPI and PN) 1	2 (DP/MPI and DP) 2	2 (DP/MPI and PN) 1	3 (DP/MPI, DP, PN) 2
Dimensions (WxHxD) in mm	40 x 125 x 130		80 x 125 x 130		120 x 125 x 130
Order No. stem Standard version	6ES7 315-6FF.	6ES7 315-2FH.	6ES7 317-6FF.	6ES7 317-2FK.	6ES7 318-3FL.
Order No. stem SIPLUS version <sup>1)</sup>	6AG1 315-6FF.	–	6AG1 317-6FF.	–	–

<sup>1)</sup> As SIPLUS component also for extended temperature range -25 to +60°C and corrosive atmosphere/condensation ([www.siemens.com/siplus](http://www.siemens.com/siplus))

### Software components for engineering, runtime mode and safety lifecycle management

Name	Order No. stem
S7 F Systems / S7 F Systems upgrade	6ES7 833-1CC01-0.
S7 F Systems RT license (part of the AS bundles)	6ES7 833-1CC00-6.
Safety Matrix Editor including Safety Matrix Viewer Safety Matrix Tool Safety Matrix Viewer	6ES7 833-1SM0. 6ES7 833-1SM4. 6ES7 833-1SM6.
Partial Stroke Test function blocks and faceplates ■ Engineering license and RT license for one AS ■ RT license for a further AS	6BQ2 001-OCA. 6BQ2 001-OCB.
Burner libraries, function blocks ■ For SIMATIC S7-400FH controllers ■ For SIMATIC S7-300F controllers	9AL3 100-1AA1. 9AL3 100-1AD5.

## ET 200M F signal modules MTA terminal modules

### F signal modules for ET 200M on S7-300F and S7-400FH

Module types	Digital input		Digital output		Analog input
	SM 326F	SM 326F NAMUR [Ex ib]	SM 326F		SM 336F HART
Max. number of inputs/outputs	24 (1-channel for SIL 2 sensors) 12 (2-channel for SIL 3 sensors)	8 (1-channel) 4 (2-channel)	10, electrically isolated in groups of 5 P/P switching	8, electrically isolated in groups of 4 P/M switching	6 (1-channel) 15 bits + sign 2-wire or 4-wire connection
Max. achievable safety class to IEC 61508 / EN 954-1	1-channel: SIL 2 2-channel: SIL 3	1-channel: SIL 2 2-channel: SIL 3	SIL 3	SIL 3	SIL 3
Input or output voltage	24 V DC	NAMUR	24 V DC	24 V DC	–
Input or output current	–	–	2 A per channel with "1" signal	2 A per channel with "1" signal	4 ... 20 mA or 0 ... 20 mA
Short-circuit-proof sensor supply	4 for 6 channels each, electrically isolated in groups of 2	8 for 1 channel each, electrically isolated- from each other	–	–	6 for 1 channel each
HART communication	–	–	–	–	● (optional)
Redundancy mode	● Module redundancy	● Module redundancy	● Module and channel redundancy	–	● Module and channel redundancy
Module and channel diagnostics	●	●	●	●	●
Dimensions (WxHxD) in mm	80 x 125 x 120	80 x 125 x 120	80 x 125 x 120	80 x 125 x 120	40 x 125 x 120
Order No. stem	6ES7 326-1BK.	6ES7 326-1RF.	6ES7 326-2BF0.	6ES7 326-2BF4.	6ES7 336-4GE.

### MTA terminal modules for the sensor/actuator connection to F modules of the ET 200M

MTA type	Input/output range	IO redundancy	Order No.		
			MTA	ET 200M module	Connection cable
6 channels F AI HART (safety-related)	4 ... 20 mA or 0 to 20 mA	●	6ES7 650-1AH61-5.	6ES7 336-4GE00-0.	6ES7 922-3BD00-0AU. (3 m) 6ES7 922-3BJ00-0AU. (8 m)
6 channels F AI (safety-related)	4 ... 20 mA	●	6ES7 650-1AH51-5.	6ES7 336-1HE00-0. (as of pr. version 6)	6ES7 922-3BD00-0AS. (3 m) 6ES7 922-3BJ00-0AS. (8 m)
24 channels F DI (safety-related)	24 V DC	●	6ES7 650-1AK11-7.	6ES7 326-1BK00-0. and 6ES7 326-1BK01-0. (as of pr. version 1)	
10 channels F DO (safety-related)	24 V DC, 2 A	●	6ES7 650-1AL11-6.	6ES7 326-2BF01-0. (as of pr. version 2)	
10 channels F DO relays (safety-related)	110 ... 220 V AC, 5 A; 24 V DC, 5 A	●	6ES7 650-1AM31-6.	6ES7 326-2BF01-0. (as of pr. version 2)	

# ET 200S distributed I/O system

## SIMATIC PCS 7 safety packages

### Power modules and safety-related electronics modules (F modules) for ET 200S on S7-300F and S7-400FH

Power modules for electronics modules		
Module types	PM-E	
Supply voltage	24 V DC/10 A	24 ... 48 V DC; 24 ... 230 V AC; with fuse
Application	All types of electronics module, including safety-related (4/8 F DI, 4 F DO); limitations through voltage range	
Diagnostics	Load voltage	Load voltage and fuse
Order No. stem of power module	6ES7 138-4CA.	6ES7 138-4CB.
Order No. stem of terminal module	6ES7 193-4CC. (2 x 3 terminals), AUX1 with through-connection to left 6ES7 193-4CD. (2 x 3 terminals), AUX1 interrupted to left 6ES7 193-4CE. (2 x 2 terminals)	

Safety-related electronics modules (F modules)		
Module types	<b>Digital input module 4/8 F DI</b>	<b>Digital output module 4 F DO</b>
Number of I/Os	4 (2-channel for SIL 3 sensors) 8 (1-channel for SIL 2 sensors)	4 with 24 V DC/2 A, P/M switching <sup>1)</sup> , up to SIL 3 <sup>1)</sup> P/M: for ungrounded loads (mass and ground separated)
Input or output voltage	24 V DC	
Module and channel diagnostics	●	●
Order No. stem of electronics module	6ES7 138-4FA.	6ES7 138-4FB.
Order No. stem of terminal module	6ES7 193-4CF. (4 x 4 terminals) 6ES7 193-4CG. (4 x 6 terminals)	6ES7 193-4CF. (4 x 4 terminals) 6ES7 193-4CG. (4 x 6 terminals)
Order No. stem of power module (see table of power modules for associated terminal modules)	6ES7 138-4CA. 6ES7 138-4CB.	

### SIMATIC PCS 7 safety packages

SIMATIC PCS 7 Safety ES Packages		Order No. stem
SIMATIC PCS 7 Safety ES Package for AS/OS, 250 POs	<ul style="list-style-type: none"> <li>■ SIMATIC PCS 7 Engineering Software with AS/OS engineering and runtime license for 250 POs</li> <li>■ S7 F Systems</li> </ul>	6ES7 651-6AA07-0.
SIMATIC PCS 7 Safety ES Package for AS/OS, unlimited POs	<ul style="list-style-type: none"> <li>■ SIMATIC PCS 7 Engineering Software with AS/OS engineering license for unlimited POs and AS runtime license for 600 POs</li> <li>■ S7 F Systems</li> </ul>	6ES7 651-6AF07-0.
SIMATIC PCS 7 Safety Matrix ES Package for AS/OS, 250 POs	<ul style="list-style-type: none"> <li>■ SIMATIC PCS 7 Engineering Software with AS/OS engineering and runtime license for 250 POs</li> <li>■ SIMATIC Safety Matrix Tool</li> <li>■ S7 F Systems</li> </ul>	6ES7 651-6BA07-0.
SIMATIC PCS 7 Safety Matrix ES Package for AS/OS, unlimited POs	<ul style="list-style-type: none"> <li>■ SIMATIC PCS 7 Engineering Software with AS/OS engineering license for unlimited POs and AS runtime license for 600 POs</li> <li>■ SIMATIC Safety Matrix Tool</li> <li>■ S7 F Systems</li> </ul>	6ES7 651-6BF07-0.
SIMATIC PCS 7 Safety Matrix ES Extension Package	<ul style="list-style-type: none"> <li>■ SIMATIC Safety Matrix Tool</li> <li>■ S7 F Systems</li> </ul>	6ES7 651-6BX07-0.
SIMATIC PCS 7 Safety Matrix OS Packages		
SIMATIC PCS 7 Safety Matrix OS Single Station Package	<ul style="list-style-type: none"> <li>■ SIMATIC PCS 7 OS Software Single Station, 250 POs</li> <li>■ SIMATIC Safety Matrix Viewer</li> </ul>	6ES7 652-6AA07-0.
SIMATIC PCS 7 Safety Matrix OS Client Package	<ul style="list-style-type: none"> <li>■ SIMATIC PCS 7 OS Software Client</li> <li>■ SIMATIC Safety Matrix Viewer</li> </ul>	6ES7 652-6CX07-0.
SIMATIC PCS 7 Safety Matrix OS Extension Package	<ul style="list-style-type: none"> <li>■ SIMATIC Safety Matrix Viewer</li> </ul>	6ES7 652-6BX07-0.

## Get more information

You can find more detailed information in the SIMATIC Guide manuals:  
[www.siemens.com/simatic-docu](http://www.siemens.com/simatic-docu)

You can order further documents on the topic of SIMATIC at:  
[www.siemens.com/simatic/printmaterial](http://www.siemens.com/simatic/printmaterial)

More detailed technical documentation can be found at our  
Service & Support Portal:  
[www.siemens.com/automation/support](http://www.siemens.com/automation/support)

For a personal discussion, you can locate your nearest contact at:  
[www.siemens.com/automation/partner](http://www.siemens.com/automation/partner)

In the A&D Mall you can place orders electronically via the Internet:  
[www.siemens.com/automation/mall](http://www.siemens.com/automation/mall)

Visit our Process Automation Portal with comprehensive information on  
process control engineering and process instrumentation from Siemens:  
[www.siemens.com/processautomation](http://www.siemens.com/processautomation)

Siemens AG  
Industry Sector  
Industrial Automation Systems  
P.O. Box 48 48  
D-90327 NUREMBERG  
GERMANY

[www.siemens.com/process-safety](http://www.siemens.com/process-safety)

Subject to change without prior notice  
Order No.:  
E86060-A4678-A181-A3-7600  
Dispo 09508  
KB 0408 5. ROT 40 En / 815207  
Printed in Germany  
© Siemens AG 2008

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.