Process safety
Safety Integrated for Process Automation with SIMATIC PCS 7

The process industry frequently features complex production sequences where materials and mixtures which are explosive or dangerous to health are produced or processed. A failure or error could have fatal consequences for personnel, machines, plants, and environment.

Therefore the objective of Siemens safety technology is to minimize potential hazards for personnel, plant and environment by means of technical measures, without adversely affecting the production process. This requires a reliable safety instrumented system (SIS) that guides the plant into a safe state whenever necessary.

Safety Integrated for Process Automation provides a comprehensive range of products and services for safe, fault-tolerant applications in the process industry – based on the Siemens safety-related system. It offers complete safety-related functionality – extending from safe instrumentation, to safe and fault-tolerant control, to the actuator (e.g. positioners, valves and pumps).

The enormous potential of Safety Integrated for Process Automation can best be exploited in conjunction with SIMATIC PCS 7. Thanks to the modularity and the flexibility of the safety-related products this combination is extremely variable. It is not just the degree of integration of safety-related systems that can be individually defined in the process control system, it is also the degree of redundancy for controllers, fieldbus and process I/O (Flexible Modular Redundancy). Thanks to the reduced spatial requirements, the scope of hardware and wiring, as well as reduced mounting, installation and engineering overhead, the complete (common) integration of the safety-relevant systems in SIMATIC PCS 7 offers the greatest number of cost advantages - viewed over the entire life-cycle of a plant.

Both the safety technology and the safety applications implemented with it are characterized by great efficiency and comply with both national and international standards, such as:

- IEC 61508 (up to SIL 3) – basic standard for specifications, as well as for the design and operation of safety-related systems
- IEC 61511 – application-specific standard for the process industry
Safety Integrated for Process Automation
with SIMATIC PCS 7

<table>
<thead>
<tr>
<th>Safety Integrated for Process Automation – Product spectrum for SIMATIC PCS 7</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automation systems</strong></td>
</tr>
<tr>
<td>AS 412F/FH</td>
</tr>
<tr>
<td>AS 414F/FH</td>
</tr>
<tr>
<td>AS 417F/FH</td>
</tr>
<tr>
<td><strong>Engineering</strong></td>
</tr>
<tr>
<td><strong>SIMATIC ET 200</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>PROFIBUS with PROFI safe</strong></td>
</tr>
<tr>
<td><strong>Process instruments/process devices</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Applications</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Design versions for safety-related SIMATIC PCS 7 systems

In general, two design versions are differentiated across all architectural levels of a SIMATIC PCS 7 system based on Safety Integrated for Process Automation:

- Single-channel, non-redundant design
- Redundant, fault-tolerant design

These two design versions are very variable and offer a wide scope for design with regard to different customer requirements. Standard (basic process control) and safety-related functions can be combined flexibly, not only in the area of the distributed I/O. Even at the controller level, they can be combined in one system or separate. In addition, there are numerous possibilities arising from the use of flexible modular redundancy.

At the individual architectural levels (controller, fieldbus, distributed I/O), the configuration alternatives shown in the diagram are available, depending on the process I/O used.

Safety-related automation systems

The safety-related SIMATIC PCS 7 automation systems are available in two design versions:

- Single station: AS 412F/AS 414F/AS 417F with only one CPU, safety-related
- Redundant station: AS 412FH/AS 414FH/AS 417FH with two redundant CPUs, safety-related and fault-tolerant

All these systems have multitasking capability, i.e. several programs can be executed simultaneously in one CPU, both basic process control applications and safety-related applications. In interaction with the safety-related signal modules of ET 200M/S distributed I/O systems or safe transmitters connected directly via fieldbuses, they not only detect errors in the process, but also their own internal errors, and will automatically transition the plant to a safe state if an error is detected. Safety programs executed on different automation systems of a plant are also able to carry out safety-related communication with one another over the Industrial Ethernet plant bus.
Safety Integrated for Process Automation with SIMATIC PCS 7

Engineering tools for safety functions

For configuration and programming of the safety-related AS 412F/FH, AS 414 F/FH and AS 417 F/FH, the F-block library in S7 F Systems and the SIMATIC Safety Matrix are available.

S7 F Systems with F-block library

The S7 F Systems engineering tool allows parameter assignment of the AS 412F/FH, AS 414 F/FH, and AS 417 F/FH as well as the safety-related F-modules from the ET 200M/S series. It supports configuration by means of functions for:

- Comparison of safety-related F-programs
- Detection 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 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 avoid the need for diverse programming tasks for detecting and reacting to errors.

SIMATIC Safety Matrix

The SIMATIC Safety Matrix which can be used in addition to the CFC is an innovative safety lifecycle tool from Siemens that can be used not only for user-friendly configuration of safety applications, but also for their operation and service. The tool, which is based on the proven principle of a cause & effect matrix, is ideally suited to processes where defined statuses require specific safety reactions.

The 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 occurring 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.

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. Special programming knowledge is not required, and the configuration engineer can concentrate fully on the safety requirements of his plant.
PROFIsafe, safety-related I/O modules

**PROFIBUS with PROFIsafe**

The standard PROFIBUS is used together with the PROFIsafe profile for safety-related communication between the CPU of the automation system and the safety-related process I/O. This solution supports operation of standard and safety-related components on the same bus. A separate and expensive safety bus is unnecessary.

The PROFIsafe profile is implemented as an additional software layer within the devices/systems without modifying the communication mechanisms of the standard PROFIBUS. PROFIsafe expands the message frames by additional information with which the PROFIsafe communications partner can recognize and compensate transmission errors such as delays, incorrect sequences, repetitions, losses, faulty addressing or data falsification.

**Safety-related F-modules/submodules**

The safety functions of the F/FH automation systems are perfectly matched to the safety-related I/O modules of the ET 200M and ET 200S distributed I/O systems. The redundant F-signal modules/submodules of ET 200M/S (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.

<table>
<thead>
<tr>
<th>F-signal modules for ET 200M</th>
<th>Digit input SM 326 F</th>
<th>Digital input SM 326 F NAMUR [EEx ib]</th>
<th>Digit output SM 326 F</th>
<th>Digit output SM 326 F</th>
<th>Analog input SM 336 F HART</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of inputs/outputs up to</td>
<td>24 (1-channel for SIL 2 sensors)</td>
<td>8 (1-channel)</td>
<td>10, isolated in groups of 5 P/P switching</td>
<td>6 (1-channel)</td>
<td>15 bit + sign 2-wire or 4-wire connection</td>
</tr>
<tr>
<td>Max. achievable safety class in accordance with IEC 61508/EN 954-1</td>
<td>1-channel: SIL 2 2-channel: SIL 3</td>
<td>1-channel: SIL 2 2-channel: SIL 3</td>
<td>SIL 3</td>
<td>SIL 3</td>
<td></td>
</tr>
<tr>
<td>Input or output voltage</td>
<td>24 V DC</td>
<td>NAMUR</td>
<td>24 V DC</td>
<td>24 V DC</td>
<td>–</td>
</tr>
<tr>
<td>Input or output current</td>
<td>–</td>
<td>–</td>
<td>2 A per channel for &quot;1&quot; signal</td>
<td>2 A per channel for &quot;1&quot; signal</td>
<td>4 ... 20 mA or 0 ... 20 mA</td>
</tr>
<tr>
<td>Short-circuit proof sensor supply</td>
<td>4 for every 6 channels, isolated in groups of 2</td>
<td>8 for each channel, individually isolated</td>
<td>–</td>
<td>–</td>
<td>6 for each channel</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Module redundancy</td>
<td>Module redundancy</td>
<td>Module and channel redundancy</td>
<td>Module and channel redundancy</td>
<td></td>
</tr>
<tr>
<td>Module and channel diagnostics</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Dimensions</td>
<td>80 x 125 x 120</td>
<td>80 x 125 x 120</td>
<td>80 x 125 x 120</td>
<td>80 x 125 x 120</td>
<td>40 x 125 x 120</td>
</tr>
</tbody>
</table>

**ET 200S power module PM-E for electronic modules**

- **Supply voltage**: 24 V DC/10 A 24 ... 48 V DC; 24 ... 230 V AC; with fuse
- **Applications**: All electronic module types, including safety-related (4/8 F-DI, 4 F-DO); restrictions due to voltage range
- **Diagnostics**: Load voltage Load voltage and fuse

**Safety-related ET 200S electronic modules (F-modules)**

<table>
<thead>
<tr>
<th>Module types</th>
<th>Digital input 4/8 F-DI</th>
<th>Digital output 4 F-DO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of I/Os</td>
<td>4 (2-channel SIL 3-sensor) 8 (1-channel SIL 2-sensors)</td>
<td>4 for 24 V DC/2 A, current sinking/sourcing, up to SIL 3 P/M: for ungrounded loads (mass and ground separated)</td>
</tr>
<tr>
<td>Input or output voltage</td>
<td>24 V DC</td>
<td></td>
</tr>
<tr>
<td>Module and channel diagnostics</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
Safety-related I/O modules

Safety-related F-motor starter for ET 200S

- PM-D F PROFIsafe power module for fail-safe motor starters
- Safety-related motor starters up to 7.5 kW, can be expanded by brake control module
  - F-DS1e-x direct-on-line starter
  - F-RS1e-x reversing starter

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/contactor combination, the safety-related 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 detect a fault and deactivate the circuit-breaker in the motor starter in a safety-related manner.

PROFIBUS PA devices for safety shutdowns

- SITRANS P DS III PROFIsafe

The SITRANS P DS III digital pressure transmitter is the first commercially available PROFIBUS PA device for SIL2 safety shutdowns conforming to IEC 61508/IEC 61511-1. For this reason, Siemens has extended its standard measuring instrument for pressure, absolute pressure, differential pressure to include a PROFIsafe driver.

In a safety application, the pressure transmitter can be connected via PROFIBUS PA to an AS 412F/FH, AS 414F/FH or AS 417 F/FH. For safe shutdown, the digital input of SIPART PS2 PA, the electropneumatic PROFIBUS PA positioner, can be used.

In the case of a diverse redundant design, measuring circuits up to safety level SIL3 can be implemented.

Process safety highlights

- Safety Integrated for Process Automation – the comprehensive product and service offering for safe, fault tolerant, and high-availability applications in the process industry
  - Easy implementation, operation, and maintenance of safety applications
  - Innovation safe thanks to high-level adaptability to changed conditions
  - Reliable in elimination of dangers and risks

- Homogenous integration of safety technology in the SIMATIC PCS 7 Process Control System
  - Processing of basic process control functions and safety functions in one controller: Safety level SIL 3, AK 6 with only one CPU is possible
  - Standard and safety-related communication between controller and I/O via a common fieldbus PROFIBUS with PROFIsafe – no separate safety bus
  - Mixed operation of standard and safety-related F-modules in ET 200M/S stations
  - Uniform data storage for basic process control and safety related automation, including process visualization and diagnostics - no cumbersome data handling

- Configuration of safety functions is part of the uniform system configuration with the PCS 7 Engineering System
  - 57 F systems, CFC, and SIMATIC Safety Matrix are anchored in the engineering toolset
  - Configuration of basic process control functions and safety functions with one engineering tool, the CFC
  - Safety Matrix for creation of safety functions without special programming skills - even faster, easier, and with more convenience than is possible with the CFC

- Automatic consideration of safety-related fault messages in process visualization, with identical time tagging

- Uniform diagnostics and maintenance from sensor/actuator via automation system up to the operator system

- Integration of safety-related technology in diagnostics and maintenance with the PCS 7 Asset Management system

- Minimization of total lifecycle costs
  - Reduction of costs for hardware, mounting, wiring, installation, engineering, and commissioning as the level of integration increases
  - Low acquaintance and training requirements as result of uniform system/tool landscape
  - Cost-effective stocking of spare parts through reduction of types and parts