SIMATIC fail-safe controllers
Seamless safety solutions in factory and process automation
Trend to safety systems – Features of SIMATIC Safety Integrated

Increased importance of safety systems

Accidents and damage caused by faults in machines or systems must be prevented to the extent possible. Laws regarding safety at the workplace and protection of the environment are becoming increasingly strict worldwide.

To that goal, many different products and systems for safety-oriented functions (electrical engineering) and standard tasks (classic PLC) are employed. Conventional wiring or the use of special safety buses will not only increase wiring costs and engineering effort, but will also cause error diagnostics to become more expensive and availability to decrease.

That’s why machine manufacturers and plant operators are more and more using automation components for safety-related tasks. The safety of people, machines and the environment thus depends on the correct functioning of the automation systems. The same high demands that are placed on safety-related electromechanical components are therefore placed on safety-related electronic systems as well. Both generic and arbitrary errors must be handled in a safe way.

Safety Integrated as a component of Totally Integrated Automation

Safety Integrated from Siemens, the comprehensive supplier of automation technology, is a complete and uniform safety program. Safety Integrated is a constituent of “Totally Integrated Automation”. As a result, it provides integrated safety technology with its

- sensors (SIGUARD, SIRIUS),
- controllers (SIMATIC), and
- drives (SINUMERIK, MASTERDRIVES, SIMODRIVE, SIMOTION).

Thanks to the integration of safety technology functions into the automation world of Totally Integrated Automation, standard automation and safety automation have become one integrated overall system. This is associated with significant cost savings, both for the mechanical equipment manufacturer and the company operating the plant.

Key features of SIMATIC Safety Integrated

SIMATIC Safety Integrated comprises the fail-safe SIMATIC controllers as well as I/O and engineering modules within the product range of Safety Integrated. If a fault occurs, the application can be flexibly changed into a safe state and remains in that safe state. The fail-safe controllers are based on time-proven standard PLCs.

Both PROFIBUS and PROFINET have been expanded by the PROFIsafe profile for safety-related communication. Standard and safety-related communication are now possible through just one standard bus cable.

The engineering for the safety functions, as well as for the standard functions of the fail-safe SIMATIC controllers, is implemented with the same configuring tools (STEP 7). In a SIMATIC controller the safety technology is thus seamlessly integrated into standard automation. Operation of the complete plant is then made easier. The training requirements are reduced in addition to the engineering costs.

Thanks to the fine-grained structure of the fail-safe I/Os, safety technology is only applied where actually required. Combining safety components and standard components is no problem, as well as the coexistence of safety-related and non-safety-related programs in one controller. As a result of the open PROFIBUS, PROFINET and PROFIsafe standards, interfacing of fail-safe fieldbus devices from other vendors is made easier.

Highlights

SIMATIC Safety Integrated

- One controller
- One engineering
- One bus system
- One distributed I/O system

for standard and safety-related applications
Use of SIMATIC Safety Integrated

For the main applications in factory and process automation, SIMATIC Safety Integrated offers a scalable range of fail-safe controllers, where common I/Os and communication functions are used.

All applicable Standards and directives are fulfilled, e.g.:
- IEC 61508 (up to SIL 3), IEC 61511
- EN 954 (up to Category 4)
- NFPA 79-2002
- NFPA 85

The certificates from the German Technical Inspectorate (TÜV) prove compliance with the respective standards and regulations. SIMATIC Safety Integrated is therefore suitable for global use to protect humans, machines and the environment.

### System architecture of SIMATIC Safety Integrated

<table>
<thead>
<tr>
<th>Controller</th>
<th>Engineering</th>
<th>Communication</th>
<th>Distributed I/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>F-CPUs of ET 200S, S7-300F, S7-400F</td>
<td>STEP 7 (LAD, FBD)</td>
<td>PROFINET with PROFIsafe profile</td>
<td>ET 200S, ET 200pro</td>
</tr>
<tr>
<td>H-CPUs of S7-400</td>
<td>CFC and Safety Matrix</td>
<td>PROFIBUS with PROFIsafe profile</td>
<td>ET 200S, ET 200M, ET 200eco, ET 200pro</td>
</tr>
</tbody>
</table>

1) only for factory automation

### Typical applications in factory automation
- Conveyor systems, presses, processing machines, machine tools, etc.
- Transport of people, e.g. cable cars, lifting platforms, rides in amusement parks, etc.

### Typical applications in process automation
- Chemical, petrochemical
- Burner management systems etc.
Advantages of SIMATIC Safety Integrated

SIMATIC Safety Integrated combines standard automation and safety technology into one innovative overall system.

As a complete supplier, Siemens also offers a complete range of products. Existing SIMATIC and safety technology expertise is sufficient to solve safety-related tasks with SIMATIC.

SIMATIC Safety Integrated provides benefits for:
- machine manufacturers and plant engineers e.g. reduced engineering support and
- plant operators e.g. through higher plant availability and increased flexibility.

When considered individually, advantages result compared to a proprietary fail-safe PLC and also to conventional safety technology.

<table>
<thead>
<tr>
<th>Advantage of SIMATIC Safety Integrated</th>
<th>compared to proprietary fail-safe controllers</th>
<th>compared to conventional safety technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less engineering overhead</td>
<td>· Only one engineering tool required for development of standard and safety programs</td>
<td>· A solution can be easily duplicated by copying the safety program</td>
</tr>
<tr>
<td></td>
<td>· Shared data management for standard and safety programs</td>
<td>· Increased flexibility thanks to programming instead of wiring the safety logic circuit</td>
</tr>
<tr>
<td></td>
<td>· Uniform configuration of standard and safety-related communication</td>
<td></td>
</tr>
<tr>
<td>Commissioning is easier and faster</td>
<td>· Only one PROFIBUS/PROFINET cable for standard and safety-related communication</td>
<td>· Easy modification of the safety logic circuit through program changes with automatic updating of the documentation</td>
</tr>
<tr>
<td></td>
<td>· Same operating philosophy for standard and safety-related automation</td>
<td>· Uniform diagnostics, from sensors to controllers right up to the HMI system</td>
</tr>
<tr>
<td></td>
<td>· All system components are from a single source</td>
<td></td>
</tr>
<tr>
<td>More efficient operating phase</td>
<td>· Shorter downtimes thanks to uniform diagnostics from sensors to controllers right up to the HMI system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Remote diagnostics using Teleservice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Simplified spare parts inventory based on common architecture and fewer components</td>
<td></td>
</tr>
</tbody>
</table>
Comparison: Previous solution versus new fail-safe solution

Previous safety-related PLC solutions required two different PLCs, and for distributed solutions an additional safety bus.

The new solution using SIMATIC Safety Integrated requires only one PLC with uniform engineering and the standard bus PROFIBUS or PROFINET with the PROFIsafe profile for standard and safety-related automation.

If required, the systems can be set up separately as in the past.
Siemens offers you a comprehensive failsafe product range for PROFINET comprising the SIMATIC S7-300 and S7-400 automation systems.

Failsafe distributed field devices from the SIMATIC ET 200 range can be directly connected to PROFINET. Existing failsafe PROFIBUS devices can also be integrated into a PROFINET solution.

The product range is rounded off by a comprehensive selection of active and passive network components, security products for fail-safe Ethernet networks in industry, and the possibility for wireless communication with Industrial Wireless LAN.

### SIMATIC modules

<table>
<thead>
<tr>
<th>Controller</th>
<th>PROFIBUS</th>
<th>PROFINET</th>
</tr>
</thead>
<tbody>
<tr>
<td>ET 200 S</td>
<td>IM 151-7 F-CPU</td>
<td></td>
</tr>
<tr>
<td>S7-300</td>
<td>CPU 315F-2 DP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPU 315F-2 PN/DP</td>
<td></td>
</tr>
<tr>
<td>S7-400</td>
<td>CPU 317F-2 DP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPU 317F-2 PN/DP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPU 416F-2</td>
<td></td>
</tr>
</tbody>
</table>

### Distributed I/O

| ET 200S    |          |          |
| ET 200M    |          |          |
| ET 200pro  |          |          |
| ET 200eco  |          |          |

1) with CP 443-1 Advanced
Configuration example for process automation

**Simple integration into a control system**

SIMATIC Safety Integrated offers a first-class Safety Instrument Solution (SIS) based on innovative and proven products, systems and standards.

You can connect our innovative SIS to any control system (DCS) using SIMATIC S7-400FH and SIMATIC ET 200M/S. A unique feature here is the integration of safe and fault-tolerant functions in the SIMATIC PCS 7 process control system. This combination offers you a number of advantages:

- A single engineering system for standard and critical applications
- Homogeneous integration of safe and fault-tolerant technology in the SIMATIC PCS 7 automation system (AS)
- Comfortable visualization of process values integrated in the SIMATIC PCS 7 Operator Stations (OS)
- Automatic integration of safety-related fault messages in the process visualization, with identical time stamp
- No costly link between DCS and SIS

**Controller**

- Safe and fault-tolerant SIMATIC S7-400FH controllers – configurable like the standard S7-400
- Maximum safety level SIL 3 possible with only one controller
- Standard, safe and fault-tolerant functions either combined in one controller or separate
- FH controllers can be set up separately - up to 15 km apart

**I/O**

- SIMATIC ET 200M with a large number of I/O modules and bit-modular SIMATIC ET 200S
- NAMUR module of the SIMATIC ET 200M for hazardous (Ex) areas
- Standard and fail-safe modules can be added according to requirement
- Fail-safe modules: complete internal redundancy/diversity
- Comprehensive diagnostics functions for detecting internal and external faults
- Safety functions contained in the fail-safe signal modules

**Communication**

- Standard PROFIBUS DP with PROFIsafe profile
Safety-related communication with PROFIsafe profile

PROFIsafe was the first communication protocol approved under the safety standard IEC 61508 that permits both standard and safety-related communication on one bus. This not only results in an enormous savings potential with regard to cabling and the required number of parts, but also adds the advantage of retrofitting.

PROFIsafe is an open solution with safety-related communication via standard field busses. Numerous manufacturers of fail-safe components and end users of safety technology have helped develop this vendor-independent and open standard within PROFIBUS International (PI).

The PROFIsafe profile supports fail-safe communication for the open PROFIBUS and PROFINET standard buses. An IE/PB link guarantees uniform and safety-related communication between PROFIBUS and PROFINET.

As component of SIMATIC Safety Integrated, PROFIsafe is certified to IEC 61508 (up to SIL 3), EN 954 (up to Category 4), NFPA 79-2002, NFPA 85 and thus meets the highest safety requirements of the manufacturing and process industry.

PROFIBUS is the global standard for fieldbuses with approx. 13 million installed nodes. It has such a high level of market acceptance because many vendors offer numerous products for it. With the PA protocol (IEC 1158-2), PROFIBUS DP is extending distributed automation seamlessly into the process world.

PROFINET is the innovative and open Industrial Ethernet standard for automation. It permits short response times and the transmission of large data quantities.

PROFIsafe uses PROFIBUS components and services for fail-safe communication. A fail-safe CPU (F-CPU) and a fail-safe slave (F-slave) exchange useful data as well as status and control information; no additional hardware is required for that purpose.

PROFIsafe counteracts the various possible types of fault when transmitting data in one of the following ways:

<table>
<thead>
<tr>
<th>Action</th>
<th>Consecutive number</th>
<th>Expected time with acknowledgment</th>
<th>Identification for transmitter and receiver</th>
<th>Data protection CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repetition</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Loss</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Insertion</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Incorrect sequence</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Data falsification</td>
<td></td>
<td></td>
<td></td>
<td>■</td>
</tr>
<tr>
<td>Delay</td>
<td></td>
<td></td>
<td></td>
<td>■</td>
</tr>
<tr>
<td>Coupling of safety-related and standard messages (masquerade)</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>FIFO fault</td>
<td></td>
<td></td>
<td></td>
<td>■</td>
</tr>
</tbody>
</table>
Scalable systems for factory and process automation

The product range of the fail-safe SIMATIC controllers comprises widely scalable safety solutions for both factory and process automation.

- **In factory automation**, safety and the protection of people and machines are of prime importance.
- **In process automation**, it is of prime importance to retain system availability. At the same time, protection must be provided against unexpected danger from the process.

If a fault occurs, the application can be flexibly changed into a safe state and kept in that safe condition with the help of fail-safe SIMATIC controllers.

The safety functions are executed by the safety program in the CPU in connection with fail-safe I/O modules. Standard I/O modules and fail-safe I/O modules can also be set up as a combination.

Both safety-related and standard communication between the central processing unit and the I/Os (safety-related or standard) are carried out via PROFIBUS DP or PROFINET and the PROFIsafe profile.

**Factory automation**

The following F-CPU have been designed for factory automation:

- IM 151-7 F-CPU of the ET 200S
- CPU 315F and CPU 317F of the S7-300
- CPU 416F of the S7-400

These CPUs are based on the respective standard CPUs, whose hardware and operating system have been expanded by various protection mechanisms for executing safety programs.

The entire programming of the safety-related program is done by STEP 7 in the standard languages LAD and FBD.

The software package "S7 Distributed Safety" supports the configuration of the fail-safe I/Os and the programming using preconfigured, certified modules.

There are no restrictions for editing non-safety-related programs.

**Process automation**

The fault-tolerant CPUs 414H and 417H of the S7-400 are available for applications in the process industry.

Safety-related applications in the process industry require a special software package "S7 F-Systems". With one CPU, fail-safe applications can be solved with SIL 3.

Two redundant CPUs can be used for enhanced system availability in order to satisfy the demands for fail-safety and fault tolerance.

The program is developed using the Safety Matrix or Continuous Function Chart (CFC) as well as certified function blocks.

"S7 F-Systems" supports configuration of safety-related I/Os and programming of the logic.
Fail-safe controllers for factory automation
Overview of CPUs

For factory automation, there are four different CPUs available in three different designs. The following table lists the most important technical characteristics of the CPUs.

The fail-safe CPUs have the following functionality:
- Comprehensive self-tests and self-diagnostics to check the fail-safe state of the CPU.
- Execution of standard and fail-safe programs on one CPU.
- Fail-safe internode communication.
- Common diagnostics and signaling functions as for standard SIMATIC S7 CPU.

The ET 200 is used as fail-safe I/O (see Page 15).

<table>
<thead>
<tr>
<th>CPU</th>
<th>IM 151-7 F-CPU</th>
<th>CPU 315F-2 DP</th>
<th>CPU 315F-2 PN/DP</th>
<th>CPU 317F-2 DP</th>
<th>CPU 317F-2 PN/DP</th>
<th>CPU 416F-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus system</td>
<td>PROFIBUS</td>
<td></td>
<td></td>
<td>PROFINET</td>
<td>PROFINET 1)</td>
<td></td>
</tr>
<tr>
<td>Design</td>
<td>ET 200S</td>
<td>S7-300 with central and/or distributed fail-safe I/O</td>
<td>S7-400 with distributed fail-safe I/O</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main memory</td>
<td>96 KB</td>
<td>192 KB</td>
<td>256 KB</td>
<td>512 KB</td>
<td>1,4 MB data</td>
<td>1,4 MB code</td>
</tr>
<tr>
<td>Load memory (plug-in)</td>
<td>64 KB - 8 MB</td>
<td>64 KB - 8 MB</td>
<td>64 KB - 8 MB</td>
<td>256 KB integr., 64 KB - 64 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit memories</td>
<td>2 Kbit</td>
<td>16 Kbit</td>
<td>64 Kbit</td>
<td>128 Kbit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FB/FC/DB</td>
<td>512/512/511</td>
<td>2048/2048/1023</td>
<td>2048/2048/2047</td>
<td>2048/2048/4095</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fail-safe I/O</td>
<td>Up to 28</td>
<td>Up to 320</td>
<td>&gt; 500</td>
<td>&gt; 1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O address area</td>
<td>244/244 Byte</td>
<td>2/2 KB</td>
<td>8/8 KB</td>
<td>16/16 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process I/O image</td>
<td>128/128 Byte</td>
<td>384/384 Byte</td>
<td>1/1 KB</td>
<td>16/16 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td>MPI/DP</td>
<td>MPI and DP</td>
<td>PROFINET and MPI/DP</td>
<td>MPI/DP and DP</td>
<td>PROFINET and MPI/DP</td>
<td>MPI/DP and DP</td>
</tr>
<tr>
<td>Dimensions</td>
<td>60 x 120 x 75</td>
<td>40 x 125 x 130</td>
<td>80 x 125 x 130</td>
<td>25 x 290 x 219</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 151-7FA..</td>
<td>6ES7 315-6FF..</td>
<td>6ES7 315-2FJ..</td>
<td>6ES7 416-2FK..</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1) with CP 443-1 Advanced
Programming

Distributed Safety

When using the “S7 Distributed Safety” software package, no additional know-how is required. Programming of safety-related programs for the fail-safe CPUs is carried out over the well-known STEP 7 standard language ladder diagram (LAD) and function block diagram (FBD). A safety-related program is automatically generated through a special function during compilation.

An additional component of this software package is the F-library with preconfigured, TÜV-certified modules for safety-related functions. S7 Distributed Safety also supports the comparison of safety-related programs. And the generated program printout simplifies the acceptance test of the plant.

In addition to the fail-safe program, a standard program may coexist and can run on the CPU as well, and is not subject to any limitations.

Burner package

The optional burner package contains an F library with blocks for industrial gas and oil burners. The blocks have been TÜV-certified according to EN 61508 SIL 3 and the TRD standards 411 and 412 for thermal and steam boilers.

Example

The example "Emergency stop" shows how stop functions can be implemented immediately (category 0) or time-delayed (category 1). The acknowledge key is used as start input.

The programming overhead is minimized thanks to distributed error analysis by the ET 200S and ET 200M modules. For example, the discrepancy time is configured by the HW Configuration and analyzed in the module. In the PLC program, only a signal appears. This signal determined by the system can thus be easily processed in the program. Complicated calculations become unnecessary.

<table>
<thead>
<tr>
<th>Option package</th>
<th>S7 Distributed Safety</th>
<th>Burner</th>
<th>Press Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Library</td>
<td>Certified modules, e.g. emergency stop, two-hand control, muting, door monitoring</td>
<td>Certified burner function blocks</td>
<td>Certified function blocks</td>
</tr>
<tr>
<td>Requirements</td>
<td>STEP 7</td>
<td>S7 Distributed Safety</td>
<td></td>
</tr>
<tr>
<td>Engineering package</td>
<td>1 license required per engineering location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Runtime package</td>
<td>1 license required per CPU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 833-1FC...</td>
<td>9AL3 100-1AD...</td>
<td>9AU 1837-0EA...</td>
</tr>
</tbody>
</table>

S7 Distributed Safety: The entire programming process is carried out in a function block diagram (FBD, see above) or ladder diagram (LAD)
Safe and fault-tolerant controllers for process automation
Overview of CPUs

For process automation, there are two CPUs available in the S7-400 family. They are fault-tolerant S7-400 CPUs with software implemented safety functions that permit the configuration of safe systems as well as the configuration of simultaneously safe and fault-tolerant systems. The SIMATIC PCS 7 process control system can very easily integrate the SIMATIC safe and fault-tolerant controllers.

The CPU monitors the proper operation of the system through regular self-tests, instruction tests, as well as program execution monitoring.

The table (see bottom right) lists the most important technical characteristics of the CPUs.
In a distributed configuration, the ET 200M and ET 200S are used as fail-safe I/Os (see Page 15).

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Design</th>
<th>Safety Integrated Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe</td>
<td>Simplex configuration with one CPU</td>
<td>up to SIL 3</td>
</tr>
<tr>
<td>Safe and fault-tolerant</td>
<td>Redundant configuration with two CPUs</td>
<td>up to SIL 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU</th>
<th>CPU 414-4H</th>
<th>CPU 417-4H</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM (integral)</td>
<td>768 KB data</td>
<td>10 MB data</td>
</tr>
<tr>
<td>Load memory</td>
<td>256 KB</td>
<td></td>
</tr>
<tr>
<td>Load memory</td>
<td>Up to 64 MB</td>
<td></td>
</tr>
<tr>
<td>Bit memories</td>
<td>64 Kbit</td>
<td></td>
</tr>
<tr>
<td>FB/FC/DB</td>
<td>2048/2048/4095</td>
<td>6144</td>
</tr>
<tr>
<td>I/O address area</td>
<td>8 KB/8 KB</td>
<td>16 KB/16 KB</td>
</tr>
<tr>
<td>Process I/O image</td>
<td>8 KB/8 KB</td>
<td>16 KB/16 KB</td>
</tr>
<tr>
<td>Interfaces</td>
<td>MPI/DP and DP</td>
<td></td>
</tr>
<tr>
<td>Dimensions</td>
<td>25 x 290 x 219</td>
<td></td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7414-4H...</td>
<td>6ES7417-4H...</td>
</tr>
</tbody>
</table>
Configuring

**S7 F systems**

S7 F systems are used for configuration of safety-related process applications according to IEC 61511, and expand the S7-400FH controller by safety functions. They simplify generation of the safety program by providing an F library with ready-made and TÜV-certified blocks according to SIL 3 IEC 61508. In addition, they facilitate documentation of the safety program, e.g. by management of the signatures.

Configuration of the safety program can be made either using the CFC or the Safety Matrix.

**Continuous Function Chart (CFC)**

CFC is particularly suitable for processes with a dynamic response, e.g. in the chemical and petrochemical industries (hydrocracker). CFC can be used to call and link the certified blocks from the F library of S7 F systems or from the optional burner package.

**Burner package**

The optional burner package contains an F library with blocks for industrial gas and oil burners. The blocks have been TÜV-certified according to EN 61508 SIL 3 and the TRD standards 411 and 412 for thermal and steam boilers.

<table>
<thead>
<tr>
<th>Option packages</th>
<th>S7 F Systems</th>
<th>Burner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Library</td>
<td>Approx. 50 certified basic function modules</td>
<td>Certified burner blocks</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>STEP 7 CFC S7-SCL</td>
<td>S7 F-Systems</td>
</tr>
<tr>
<td>Engineering package</td>
<td>1 license required per engineering location</td>
<td></td>
</tr>
<tr>
<td>Runtime package</td>
<td>1 license required per CPU</td>
<td></td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 833-1CC..</td>
<td>9AL3 100-1AA..</td>
</tr>
</tbody>
</table>
Safe and fault-tolerant controllers for process automation
Configuring

Safety Matrix

The Safety Matrix (1) is an innovative configuration tool for processes requiring safety reactions to defined statuses, and can be configured simply using a Cause&Effects matrix. The Cause&Effects analysis is part of the risk analysis of a plant.

The specification of the safety program simultaneously corresponds to the input parameters (2) for the Safety Matrix. Following successful input, the test specification of the plant is derived. Any sources of faults can therefore be reduced to a minimum.

The integrated viewer (3) clearly visualizes the safety matrix at the operator station (OS) using SIMATIC PCS 7.

1) The Safety Matrix generates an executable program from a Cause&Effects table.
Advantages of the Safety Matrix

- Design of safety-related functions (-logic) using cause & effect matrix – also based on process events and process reactions.
- Automatic generation of the safety-related STEP 7 program
- Easy and clear configuration reduces sources of faults to a minimum
- Automatic generation of documentation following safety tests
- No special programming skills necessary, thereby reducing time needed for configuration
- Automatic generation of visualization, and convenient display of the Safety Matrix on the SIMATIC PCS 7 Operator Station
- Automatic management of project versions
- Easy review of changes
- Easy modification of safety function, and simple adaptation of specification in test mode including bypass, reset and override functions

<table>
<thead>
<tr>
<th>Options</th>
<th>Tool</th>
<th>Editor</th>
<th>Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>Windows 2000, Professional, XP Internet Explorer 6.0</td>
<td>S7 F Systems, STEP 7, CFC, S7-SCL</td>
<td>PCS7 OS</td>
</tr>
<tr>
<td>License</td>
<td>1 license per installation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 833-1SM..</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2) Configuration of analog or digital „causes“ and digital „effects“

3) Comfortable visualisation of Safety Matrix on an Operator Station (OS) with SIMATIC PCS 7
Fail-safe I/O system ET 200

A number of fail-safe I/O systems is available for connecting actuators and sensors.

These include:
- ET 200M, the modular I/O for multi-channel applications with up to 24 channels per module
- ET 200S, the bit-modular I/O with up to eight channels per module
and I/O systems for cabinet-free installation with the high degree of protection IP 65/67
- ET 200pro, the modular, multi-functional I/O
- ET 200eco, the economical block I/O

The application of the I/O systems varies according to the different requirements in the manufacturing and process industries:

<table>
<thead>
<tr>
<th>Distributed I/O</th>
<th>Production</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PROFIBUS</td>
<td>PROFINET</td>
</tr>
<tr>
<td>ET 200M</td>
<td>✔</td>
<td>—</td>
</tr>
<tr>
<td>ET 200S</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ET 200eco</td>
<td>✔</td>
<td>—</td>
</tr>
<tr>
<td>ET 200pro</td>
<td>✔</td>
<td>—</td>
</tr>
</tbody>
</table>

**Highlights**

- **Maximum safety level**
  Up to SIL 3/Category 4, TÜV-certified

- **Reduced engineering overhead**
  Self-diagnostics and signal test (short-circuit, open-circuit, discrepancy) without additional programming overhead

- **Cost reductions through saving of material**
  Fail-safe shutdown without additional safety relays

- **Space-saving design**
  Coexistence of standard and fail-safe modules in one station

- **Utilization of existing network infrastructure**
  Connection of standard and fail-safe I/Os via only one PROFIBUS or Ethernet cable

- **Simple conversion to PROFINET**
  Same I/O modules for PROFIBUS and PROFINET
### Supported bus systems and functions with ET 200

The two tables support selection and show which distributed I/O system supports
- which functions with
- which bus systems and which interface modules.

<table>
<thead>
<tr>
<th>Fail-safe I/O</th>
<th>PROFIBUS</th>
<th>PROFINET</th>
</tr>
</thead>
<tbody>
<tr>
<td>ET 200S</td>
<td>IM 151-1 HF</td>
<td>IM 151-3 PN HF</td>
</tr>
<tr>
<td>ET 200M</td>
<td>IM 153-2 HF</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>IM 153-2 FO HF</td>
<td>–</td>
</tr>
<tr>
<td>ET 200pro</td>
<td>IM 154-2 DP HF</td>
<td>IM 154-4 PN HF</td>
</tr>
<tr>
<td>ET 200eco</td>
<td>Through a terminal block</td>
<td>–</td>
</tr>
</tbody>
</table>

### Fail-safe I/O Properties

<table>
<thead>
<tr>
<th>Fail-safe I/O</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>ET 200S</td>
<td>The bit-modular I/O with up to eight channels per module.</td>
</tr>
<tr>
<td></td>
<td>DI</td>
</tr>
<tr>
<td>ET 200M</td>
<td>The modular I/O for multi-channel applications with up to 24 channels per module.</td>
</tr>
<tr>
<td></td>
<td>DI</td>
</tr>
<tr>
<td>ET 200pro</td>
<td>The modular, multi-functional I/O with high IP65/67 degree of protection.</td>
</tr>
<tr>
<td></td>
<td>DI</td>
</tr>
<tr>
<td>ET 200eco</td>
<td>The low-cost block I/O with high IP65/67 degree of protection.</td>
</tr>
<tr>
<td></td>
<td>DI</td>
</tr>
</tbody>
</table>
Technical specifications ET 200

ET 200S

<table>
<thead>
<tr>
<th>Fail-safe ET 200S modules</th>
<th>Digital input module 4/8 F-DI</th>
<th>Digital output module 4 F-DO</th>
<th>Power module PM-E F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of inputs and outputs</td>
<td>4 (2-channel for SIL 3 sensors) 8 (1-channel for SIL 2 sensors)</td>
<td>4 at 24 V/2 A</td>
<td>Up to 2 SIL 3 outputs for 24 V/2 A, 1 relay output (10 A max.)</td>
</tr>
<tr>
<td>Input or output voltage</td>
<td>24 V DC</td>
<td>24 V DC</td>
<td>24 V DC</td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 138-4FA..-.....</td>
<td>6ES7 138-4FB..-.....</td>
<td>6ES7 138-4CF..-.....</td>
</tr>
</tbody>
</table>

Fail-safe motor starter

In addition to a circuit-breaker/contactor assembly, the fail-safe motor starters process a safe electronic evaluation circuit for fault detection.

If the contactor to be switched fails during an emergency stop event, the evaluation electronics recognizes a fault and switches off the circuit-breaker in the motor starter in a safety-related manner.

Performance at 500 V | 7.5 kW |
Rated operating current Ie | 16 A |
Short-circuit breaking capacity | 50 kA at 400 V |
Coding | Can be assigned to 1 of 6 disconnection groups |
Order No. group motor starter | 3RK1301-0.B13-.AA2 |
Order No. group terminal module | 3RK1903-3A... |

Power module PM-D F

Number of int. disconnection groups | 6 |
Aggregate current of outputs | 5 A |
Diagnostics | Can be read out |
Order No. group | 3RK1903-3B.. |

F-CM fail-safe contact multiplier

Contacts | 4 NO |
Diagnostics | Voltage failure, PLC device malfunction |
Making/breaking capacity | 1.5 A/24 V |
Order No. group | 3RK1 903-3CA.. |

Fail-safe power module (infeed terminal module) PM-D F X1

Operation | Standalone with external safety technology |
Double terminals for disconnection groups | 6 |
Diagnostics | Voltage failure |
Order No. group | 3RK1 903-3DA.. |

Fail-safe frequency converter

The fail-safe frequency converters permit safety functions with variable-speed asynchronous motors:
- Safe stop
- Safe braking ramp
- Safe reduce speed.

Power | Up to 4.0 kW |
Order No. group | 6SL3 244-05... |
ET 200M

<table>
<thead>
<tr>
<th>Fail-safe ET 200M modules</th>
<th>Digital input module SM 326 F</th>
<th>Digital input module SM 326 F (NAMUR)</th>
<th>Digital output module SM 326 F</th>
<th>Digital output module SM 326F (PM)</th>
<th>Analog input module SM 336 F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of inputs and outputs</td>
<td>24 (1-channel for SIL 2 sensors) 12 (2-channel for SIL 3 sensors)</td>
<td>8 (1-channel) 4 (2-channel)</td>
<td>10</td>
<td>8 x current sourcing/sinking</td>
<td>6 (2-channel for SIL 3 sensors) 13 bits</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>24 V DC</td>
</tr>
<tr>
<td>Alarms</td>
<td>Diagnostic alarm</td>
<td>Diagnostic alarm</td>
<td>Diagnostic alarm</td>
<td>Diagnostic alarm</td>
<td>4-20 mA</td>
</tr>
<tr>
<td>Input current/output current</td>
<td>--</td>
<td>--</td>
<td>2 A per channel at signal &quot;1&quot;</td>
<td>2 A per channel at signal &quot;1&quot;</td>
<td></td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 326-1BK-.....</td>
<td>6ES7 326-1RF-.....</td>
<td>6ES7 326-2BF-.....</td>
<td>6ES7 326-2BF-.....</td>
<td>6ES7 336-1HE-.....</td>
</tr>
</tbody>
</table>

ET 200eco

<table>
<thead>
<tr>
<th>Digital block I/O ET 200eco</th>
<th>Fail-safe ET 200pro modules</th>
<th>EM 16/8 F-DI</th>
<th>EM 8/4 F-DI/F-DO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of inputs</td>
<td>4 (2-channel with SIL 3 sensors) 8 (1-channel with SIL 3 sensors)</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Input voltage</td>
<td>24 V DC</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 148-3FA-.....</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

ET 200pro

<table>
<thead>
<tr>
<th>Fail-safe ET 200pro modules</th>
<th>EM 16/8 F-DI</th>
<th>EM 8/4 F-DI/F-DO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of inputs</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>2-channel with SIL 3 sensors 1-channel with SIL 2 sensors</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>Input voltage</td>
<td>DC 24 V</td>
<td>4 current sourcing/sinking SIL 3</td>
</tr>
<tr>
<td>Number of outputs</td>
<td>--</td>
<td>4</td>
</tr>
<tr>
<td>Output current</td>
<td>--</td>
<td>24 V DC / 2 A</td>
</tr>
<tr>
<td>Order No. group</td>
<td>6ES7 148-4FA-.....</td>
<td>6ES7 148-4FC-.....</td>
</tr>
</tbody>
</table>
Additional information

SIMATIC Safety Integrated in the Internet:
SIMATIC Safety Integrated for production industry
www.siemens.com/f-cpu
SIMATIC Safety Integrated for process industry
www.siemens.com/fh-cpu

Additional printed documentation:

- PROFINET, the open Industrial Ethernet standard
  E20001-A11-M116-V1-7600
- SIMATIC ET 200pro
  E20001-A120-P240-V1-7600
- SIMATIC ET 200 – Overview
  6ZB5310-0MF02-0BA0
- Safety Integrated – Overview
  E20001-A150-M103-X-7600
- Process Safety with SIMATIC Safety Integrated
  E20001-A550-P210-X-7600
- Fail-safe due to High- Availability fault-tolerant SIMATIC S7 PLCs
  6ZB5310-0FW02-0BA6
- SIMATIC Safety Integrated System manual
  6ZB5000-0AA02-0BA0

Multimedia:

- CD-ROM Fail-safe controllers for Factory Automation including ‘Getting Started’, S7 Distributed Safety evaluation version and comprehensive documentation
  E20001-W480-P210-X-7400
- CD-ROM SIMATIC Safety Matrix with an introduction to the Cause&Effect tool, ‘Getting Started’ and references
  E20001-W450-P210-X-6400

You can find more detailed information in the SIMATIC Guide documentation:
www.siemens.com/simatic-docu

You can order further documents on the topic SIMATIC at:
www.siemens.com/simatic/printmaterial

To get in touch with your contact person near you, look in the Internet under:
www.siemens.com/automation/partner

You can place a direct order electronically over the Internet at the A&D Mall:
www.siemens.com/automation/mall

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.

© Siemens AG 2005
Subject to change without prior 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.