System Manual

The Safety System for Industry

5. Edition

SIEMENS

Content

Dear Readers,

Helmut Gierse
A&D Group Board

Applications in the area of machine safety or process technology – state-of-the-art technologies in the automation process - demand the highest degree of safety for man, machine and the environment.

This "Safety Integrated" System Manual, that has already been updated a multiple number of times, indicates that hazards and dangers, caused by functional faults, can either be reduced or removed.

From the sensor through the evaluation equipment up to the safety-related implementation, "Safety Integrated" with the SIRIUS, SIGUARD, SIMATIC, and SINUMERIK/SIMODRIVE product groups provides maximum protection against functional faults.

These product groups have already proven themselves for many years in standard automation solutions and that worldwide. Since the safety-related communications via PROFIBUS and via the actuator-sensor-interface - ASIsafe have been certified, these components can now also be combined in the system.

In addition to the conventional wiring between the individual components, by using standard fieldbus systems, also for safety technology, additional value is added thanks to the overall system integration. This allows more cost-effective engineering, as the same components are used and the plant and system availability is simultaneously increased thanks to improved diagnostics.

Open and integrated

An automation system mainly comprises standard components such as standard PLC, drives etc.

Depending on the application, the component of safety technology of a complete system can vary widely. Independent of the application area, the safety level always comprises a chain of sensors, evaluation devices and actuators for a safety-related condition of the plant or machines. Today, the two levels of a plant or system - standard and safety related technology - are strictly separated. Generally, different engineering techniques and tools are used for these two levels. This not only results in higher costs associated with personnel training, but also in many cases, these two levels can only be linked with considerable expenditure.

The requirements regarding cost-saving potential can be especially fulfilled by selecting the appropriate installation system. In standard technology, the move to distributed concepts and the use of modern fieldbuses have already resulted in significant cost savings. Further cost savings in the future will be achieved by transferring additional safety-related signals along existing standard fieldbuses.

"Safety Integrated" is the practical and consequential implementation of this concept.
By applying this concept, standard as well as the safety components merge together to create a standard, integrated and transparent cost-effective overall system.

Complex wiring for diagnostics and feedback signals can be eliminated. With Safety Integrated, cost-savings are achieved both in the planning as well as in the installation and service/ maintenance phases thanks to standard, integrated engineering tools and techniques as well as visualization concepts.

Changes and revisions in the Standards area mean that mechanical design engineers must modify their methodology when it comes to planning safety-related machine and plant control systems.

We can support this using easy-to-understand documentation and arranging workshops for applying these Standards as well as interpreting these Standards.

As a result of intensive information exchange with users, the required elements will be defined and developed step-by-step but also in the up and coming years, additional products will round-off the portfolio even more.

It goes without saying that trends in the automation technology, that are already influencing today's automation environment, will also soon be found in Safety Integrated. Examples include the PROFINET safety communication protocol that will be introduced in the near future and wireless communications. Further, Safety Integrated will initiate certain trends. As a result of the example set, standards will be set both regarding support as well as qualitative and quantitative proof. And as a result of enthusiastic, convinced users, human responsibility and economic sense will be combined.

Our mission, together with our customers, is to expand the level of competence for functional safety!

Sincerely,

Helmut Gierse

Heinz Gall

Head of the business field
Automation, Software and Information Technology (ASI)
TÜV Industrie Service GmbH, Köln
TÜV Rheinland Group

Automation systems and components are responsible for safety-related tasks in many different applications (machines and conveyor systems, process industry, building technology etc.). This means that the health and safety of persons as well as protecting equipment and the environment depend on the correct functioning of the relevant systems and components.

Today, the correct functioning of systems and components is handled under the term of "Functional Safety". This is especially documented in Standard IEC 61508 "Functional safety of electrical, electronic and programmable electronic safety-related systems" that was ratified in the Spring of 2000. In the meantime, this Standard has also been published as EN 61508 and DIN EN 61508 / VDE 0803.

This standard is considered as a basis standard independent of the application and addresses those parties involved in developing application-specific standards, as well as the contents (describing measures for the safety concept, fault-preventing and fault-controlling measures for hardware and software) – essentially to manufacturers of safety-related systems and components.

This has already been accepted by the Standards groups oriented to specific applications. The first examples include IEC 61511 for the process industry and EN 50156 for the electrical equipment of furnace control systems. In the area of safety of machines, IEC 62061 is expected for safety-related control systems of machines. It goes without saying that in the area of machine safety, application-specific standards - such as e.g. EN 954 - also have to be taken into account. Work is underway for this Standard to integrate the perspectives of IEC 61508 in reference to e.g. quantitative parameters and quantities. A VDMA, Specification sheet 24200-1 has been published for the area of building automation. This also takes into account the perspectives of IEC 61508.

In the future, it can be expected that additional User Associations will use the existing Basis Standard for their work in order to standardize the requirements placed on safety-related systems and components. This especially makes sense, because the principles involved with risk evaluation, risk reduction and the safety-related functions can be applied to the widest range of applications. It would then mean, that from the perspective of the application, only a few aspects would have to be evaluated - such as e.g. the specified response times of the safe condition for the particular process.

This means that manufacturers will be able to develop systems and components which will be able to be used for safety tasks, with comparable degrees of risk, in various applications. To realize this, the following generally applicable data must be available for each particular component:

- Maximum Safety Integrity Level that can be achieved
- Hardware fault tolerance in conjunction with the proportion of safety-related failures (sum of the failures that fail in the safe direction plus the failures, detected and controlled by the internal diagnostics) referred to the sum of all of the failures
- Dangerous probability of failure
- Information and instructions for user programming configuration and operation

These specified criteria then allow safety-related functions to be evaluated in the application; generally, these safety-related functions comprise sensors, logic (e.g. PLC) and actuators as well as communications between these various components.

Field devices, sensors and actuators are increasingly incorporating more "intelligence". This is the reason that bus systems will be increasingly used to establish safety-related communications between the components of a safety-related function.

Over the past couple of years, progress has been made in the area of standardized, safety-related bus systems.

This progress comprises, on one hand, the development of a basis for the "Testing and certification of bus systems to transfer safety-related messages" and on the other hand, conceptual tests of such bus systems have been successfully completed.

In the meantime, safety-related devices/components for operation on these bus systems are available in the marketplace. This means that devices from different manufacturers can be operated on standardized, safety-related bus systems.

In this case, it is up to manufacturers to develop additional devices for these bus systems.

The TÜV Rheinland Group [German Technical Inspectorate, Rheinland Group], especially the business area Automation, Software and Information Technology, supports manufacturers, engineers and users in implementing the above mentioned safety-related tasks - and that worldwide (Europe, US, Japan).

After having been successfully tested, systems and components receive the FS test mark "Functional Safety" in order to document that they are in compliance with the requirements laid-down in the various Standards. Further, management systems associated with functional safety "FSM" - referred to the lifecycle of the components/systems - and experts/engineers of functional safety "FS Exp/ FS Eng" will be qualified and certified.

Engineers and users will be supported in order to achieve the functional safety - also for the application and the implemented safety function.

Cologne, 2nd of September, 2004

Alfred Beer

Management
Automation, Software and Electronics IQSE
TÜV Automotive GmbH,
TÜV SÜD Gruppe, München [German Technical Inspectorate SOUTH Group, Munich]

System certification

The SIMATIC S7 Distributed Safety is, as safety-related programmable system, certified by TÜV SÜD [German Technical Inspectorate, SOUTH]. This means that it is suitable for use in safety-related applications with a high potential hazard risk - e.g. production systems, machinery construction, process technology and offshore processes.

Certification by TÜV SÜD

The testing and certification by TÜV SÜD - as independent and certified third-party - results in some significant advantages such as

- Clear product positioning in the international competitive environment as high-quality sophisticated system, certified by a testing body that has a leading role worldwide
- High degree of security for the future when defining basic testing principles
- Testing is carried-out independently of internal company interest
- High degree of acceptance in the market
- This certification is clearly recognized worldwide.

Advantages of certification for end users

When the engineering guidelines are carefully observed, end users no longer have to give any thought to the functional safety. The control has "integrated" recognized functional safety.

Acceptance authorities therefore only have to evaluate that the control system has been correctly used and that the engineering guidelines have been observed.

The existing certification is used as basis and must no longer be questioned.

Certification procedure

The certification was aligned to IEC 61508. Further, DIN V VDE 0801 was also applied. This is the reason that deterministic as well as probabilistic fault models were used.

A high-quality fault detection and fault controlling are required as a result of the architecture of the processing/evaluation unit.

The proof of this high fault detection rate was not only a challenge for Siemens AG but also for the evaluation carried-out by TÜV SÜD. As a result of the close cooperation and integration into the complete development process, TÜV SÜD was able to make its own detailed picture of the system and the arguments presented. The experience and knowhow of the TÜV SÜD was repeatedly drawn on as a result of the many innovative principles. The reason for this was to ensure that the system remained in basic compliance with IEC 61508.

Another requirement is the management of functional safety in accordance with IEC 61508. Also here, TÜV SÜD was involved in the process as evaluator from the very beginning.

In addition, from the start, the objective was to implement the certification according to the relevant UL standards. This is the reason that the UL were closely involved in the certification process through TÜV SÜD. This meant that work wasn't carried-out twice - time-consuming and cost-intensive work.

Basis of the certification

Several sub-areas must be considered within the scope of successful certification. These don't only involve the functional safety, but also aspects such as primary safety, electromagnetic compatibility and also requirements regarding applications. The user only has a safety-related and available system after all of the requirements of the sub-areas have been fulfilled.

Testing standards

Functional safety

The functional safety was tested based on the IEC 61508 Standard - internationally recognized to represent state-of-the-art technology. UL 1998 was also used in order to be compliant with the requirements relating the US.

Primary safety

The relevant Standards regarding primary safety must be fulfilled to complete and specify the technical requirements from the above listed standards and Directives. Here, it is especially important to mention the generic standard EN 61131-2 and UL 508.

Electromagnetic compatibility

In addition to fulfilling the requirements from the EMC Directive, the specific requirements listed in EN 61131-2 were taken into account.

Application-related Standards

Both European (e.g. EN 60204-1 and EN 954-1) as well as also American (e.g. NFPA 79) Standards regarding machine safety are taken into account. The reason for this is the different application possibilities of the system.

EN 298 was essentially taken into consideration for furnace control systems.

Summary

As a result of its distributed architecture and the use of diverse software structures, the SIMATIC S7 Distributed Safety represents a real milestone when it comes to certified systems. Significant advantages are also obtained due to the fact that safety-related and non-safety-related components can be combined. The system can be used in many different applications due to the widely based basic testing procedures. This was also supported due to the fact that UL Standards are complied with.

Additional information on the services of the TÜV SÜD regarding systems and applications:

www.tuev-sued.de/iqse

Dr. rer. nat. M. Schaefer

Head of "Accident Prevention and Product Safety" in the BG Institute for Occupational Safety and Health – BGIA, Sankt Augustin

New technologies in the name of safety

If you compare the safety controls from the eighties with state-of-the-art products of today, then the advantages of intelligent computer-based systems in safety-related systems become quite clear:

- New sampling-type sensors allow a finely graduated safety technology to be created, optimally adapted to the particular application
- Computer channels, operating with high clock frequencies, result in extremely short response times
- Intelligent software allows aging processes to be identified before they can have a dangerous effect
- Safety fieldbus systems significantly reduce the amount of wiring and therefore potential problems, especially when troubleshooting.

However, new technologies are only beneficial for safety technology, if measures to control and avoid faults are already taken into account at the start of development (refer to IEC 61508). By applying new technologies, not only is a higher degree of safety achieved, but the system availability is also increased even if in some cases it is necessary to significantly intervene in the development process. The experience gained from over 250,000 of our customers' systems in the field clearly indicates that high technology applied in this fashion is also really safe.

Safety technology through dialog instead of checking

Since the middle of the eighties, the BGIA and several other testing bodies have carried-out tests on complex safety systems that accompanied the development process. The testing body no longer comes into play as a checking entity at the end of the development process, but accompanies the creation of the product from a testing-related perspective from the first idea up to when the product goes into series production. Only then can complex systems be certified in the first place. Based on an accepted specification, the testing body checks the measures taken at specific milestones in the lifecycle of a safety system and develops fault-preventing techniques within the scope of the validation. Using these techniques, which are defined in the above-mentioned Standards, the testing body ensures that the development process of a product is perfect. This is the reason why complex safety technology should be considered more a process rather than a product.

Increasing the acceptance of safety technology

The new technology allows safety to be integrated into a machine or plant directly using the functional control. In newly developed CNC control systems with integrated safety technology, reduced speed when setting-up the machine or safe operating stop are implemented using additional software without external monitoring devices. This means, for the user, that safety is embedded in the control and the likelihood of faults is significantly reduced. In the same invisible way, by applying concepts based on standard hardware to safely transfer data, various controls - and even complete production plants and systems - can be safely networked with one another. This therefore eliminates additional manual operations – e.g. parameterizing safety-related devices and equipment. Safety-related data can be centrally managed and made available.

All of these measures eliminate the barriers for the use of safety technology and increase the level of acceptance.

Safety technology from a cost perspective

Especially in the nineties, cost became an increasingly important issue in safety technology. Although the development processes for complex safety technology are extremely cost-intensive, safety, integrated using the software can be realized at a favourable cost for the individual product. Furthermore, downtimes are reduced as a result of the far more efficient diagnostics capability due to the use of safety computer systems.

The German Regulatory Bodies perceive it to be an important task to also accompany the development processes, sketched-out above, also in the future and to also further promote this. And of course, this Manual demonstrates that this is a safe route to take – and a route that is extremely promising.

For the German Regulatory Bodies, innovation and prevention are important issues in working together. Our society requires ongoing innovation. This secures the competitiveness and facilitates a lifestyle and working methods to help people generally. The German Regulatory Bodies therefore promote such innovation that plays a role in reducing all types of risks and hazards or which improves working techniques and procedures.

In order to present especially outstanding developments for increased safety and health at the workplace to a larger trade public, a German Safety at Work prize in the category of innovative products in the commercial accident prevention & insurance association will be awarded at the "Health and Safety at Work Exhibition in 2005"

(for more detailed information, refer to www.hvbg.de Webcode 860665) .

1

Regulations and Standards

1 Regulations and Standards

1.1 General Information

Objectives

The goal of safety technology is to keep the potential hazards for man and the environment as low as possible by applying and utilizing the appropriate technology. However, this should be achieved without imposing unnecessary restrictions on industrial production, the use of machines and the production of chemicals. By applying internationally harmonized regulations, man and the environment should be protected to the same degree in every country. At the same time, differences in competitive environments, due to different safety requirements, should be eliminated.

In the various regions and countries around the globe, there are different concepts and requirements when it comes to guaranteeing safety. The legal concepts and the requirements regarding what has to be proven and how, regarding whether there is sufficient safety, are just as different as the assignment of the levels of responsibility. For example, in the EU, there are requirements placed both on the manufacturer of a plant or system as well as the operating company which are regulated using the appropriate European Directives, Laws and Standards. On the other hand, in the US, requirements differ both at a regional and even at a local level.

* EUC: Equipment under control

** E/E/PE: Electrical, electronic, programmable electronic

1) corresponds to ISO 13849

2) also EN 61508 and DIN EN 61508 / VDE 0803

However, throughout the US there is a basic principle that an employer must guarantee a safe place of work. In the case of damage, as a result of the product liability laws, a manufacturer can be made liable for his product. On the other hand, in other countries and regions, other principles apply.

What is important for machinery manufacturers and plant construction companies is that the legislation and rules of the location always apply in which the machine or plant is being operated. For instance, the control system of a machine, which is operated and used in the US, must fulfill US requirements, even if the machine manufacturer (i.e. OEM) is based in Europe. Although the technical concepts with which safety is to be achieved are subject to clear technical principles, it is still important to observe as to whether legislation or specific restrictions apply.

Functional safety

From the perspective of the object to be protected, safety cannot be segregated. The causes of danger and also the technical measures to avoid them can vary widely. This is the reason that a differentiation is made between various types of safety, e.g. by specifying the particular cause of a potential hazard. For instance, the term “electrical safety” is used if protection has to be provided against electrical hazards and the term “functional safety” is used if the safety is dependent on the correct function.

This differentiation is now reflected in the most recent Standards, in so much that there are special Standards that are involved with functional safety. In the area of machine safety, EN 954 [1)] and IEC 62061 specifically address the requirements placed on safety-related control systems and therefore concentrate on functional safety. In the basis safety Standard IEC 61508 [2)], IEC addresses the functional safety of electrical, electronic and programmable electronic systems independent of any specific application area.

In IEC 61508, functional safety is defined as “part of the overall safety relating to the EUC* and the EUC control system which depends on the correct functioning of the E/E/PE** safety-related systems, other technology safety-related systems and external risk reduction facilities”.

In order to achieve functional safety of a machine or plant the safety-related parts of the protection and control devices must function correctly and when a fault condition develops, must behave so that the plant or system remains in a safe condition or is brought into a safe condition.

To realize this, proven technology is required, which fulfills the demands specified by the relevant Standards. The requirements to achieve functional safety are based on the following basic goals:

- Avoiding systematic faults,
- Controlling systematic faults,
- Controlling random faults or failures.

The measure for the level of achieved functional safety is the probability of the occurrence of dangerous failures, the fault tolerance and the quality that should be guaranteed by avoiding systematic faults. In the Standards, this is expressed using various terms. In IEC 61508: "Safety Integrity Level" (SIL), in EN 954: "Categories" and ISO 13849-1" Performance Level" (PL) (this has still not been ratified).

Standardization goals

The demand to make plant, machines and other equipment as safe as possible using state-of-the-art technology comes from the responsibility of the manufacturers and users of equipment for their safety. All safety-significant aspects of using state-of-the-art technology are described in the Standards. By maintaining and fulfilling these standards it can be ensured that state-of-the-art technology is applied therefore ensuring that the company erecting a plant or the manufacturer producing a machine or a device has fulfilled his responsibility for ensuring safety.

Note: The Standards, Directives and Laws, listed in this Manual are just a selection to communicate the essential goals and principles. We do not claim that this list is complete.

1.2 Regulations and Standards in the European Union (EU)

Basic principles of the legal requirements in Europe*

Legislation states that we must focus our efforts "... on preserving and protecting the quality of the environment, and protecting human health through preventive actions" (Council Directive 96/82/EC "Seveso II").

It also demands "Health and safety at the workplace" (Machinery Directive, workplace, health and safety legislation, ...). Legislation demands that this and similar goals are achieved for various areas ("Areas which are legislated") in the EU Directives. In order to achieve these goals, legislation places demands on the operators and users of plant, and the manufacturers of equipment and machines. It also assigns the responsibility for possible injury or damage.

The EU Directives

- specify requirements for plants/ systems and their operating companies to ensure the health and safety of personnel and the quality of the environment;

- include regulations regarding health and safety at the workplace (minimum-requirements);

- define product requirements (e.g. for machines) to ensure the health and safety of the user;

* EFTA states also use the concept of the EU.

- different requirements on the implementation of products to ensure the free exchange of goods and requirements on the use of products.

The EU Directives, that involve the implementation of products, based on Article 95 of the EU Contract that regulates free trade. This is based on a new, global concept, ("new approach", "global approach"):

- EU Directives only contain general safety goals and define basic safety-requirements.

- Standards Associations that have the appropriate mandate of the EU Commission (CEN, CENELEC), can define technical details in the appropriate Standards. These Standards are harmonized under a specific Directive and listed in the official EU Journal. When the harmonized Standards are fulfilled, it can be presumed that the associated safety requirements of the Directives are also fulfilled. (For more detailed information, refer to "Safety of machinery in Europe")

- Legislation does not specify that specific standards have to be complied with. However, when specific standards are complied with it can be "assumed" that the associated safety goals of the EU Directives are complied with.

- EU Directives specify that Member States must mutually recognize domestic regulations.

In addition to the Directives that are specific to a device type - e.g. the Low-Voltage Directive or Machinery Directive - that will be discussed in more detail in the following, there is also a general "Product Safety Directive" (2001/95/EC). This handles general questions relating to product safety. In Germany, it is implemented in the new (05.2004) Equipment and Product Safety Law (GPSG).

The EU Directives have the same degree of importance, i.e. if several Directives apply for a specific piece of equipment or device, then the requirements of all of the relevant Directives have to be met (e.g. for a machine with electrical equipment, the Machinery Directive, and Low-Voltage Directive apply).

Other regulations apply to equipment where the EU Directives are not applicable. They include regulations and criteria for voluntary tests and certifications.

The EU Directives of the New Approach with the associated lists of the harmonized Standards are available in the Internet under:

http://www.newapproach.org/

Low-Voltage Directive

The Low-Voltage Directive (73/23/EEC) is valid for electrical equipment with rated voltages in the range 50 - 1000 V AC or 75 - 1500 V DC (for the new Edition that is presently being drawn-up, the lower voltage limits will be eliminated).

This is a New Approach Directive. EN 60204-1 is listed under the Low-Voltage Directive for "Electrical equipment of machines". This means, that if EN 60204-1 is fulfilled, then it can be reasonably assumed that the Directive is fulfilled.

(Note: The requirements to fulfill the Low-Voltage Directive will not be discussed in any further detail in this Manual.)

Health and Safety at the workplace in the EU

The requirements placed on health and safety at the workplace are based on Article 137 (previously 118a) of the EU Contract. The Master Directive "Health and Safety of Personnel at the Workplace" (89/391/EEC) specifies minimum requirements for safety at the workplace. The actual requirements are subject to domestic legislation and can exceed the requirements of these Master Directives. These requirements involve the operation and use of products (e.g. machines, chemical plants), but not their implementation.

In Germany, the requirements are summarized in the operational safety regulations (BetrSichV). More detailed information on these regulations can be found in the internet site of the Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BauA)

(http://www.baua.de/baua/index.htm)

Safety of machinery in Europe

Machinery Directive (98/37/EC)*

With the introduction of a common European market, a decision was made to harmonize the national standards and regulations of all of the EC Member States. This meant that the Machinery Directive, as an internal Directive, had to be implemented in the domestic legislation of the individual Member States. In Germany, the contents of the Machinery Directive were implemented as the 9th Decree of the Equipment Safety law. For the Machinery Directive, this was realized with the goal of having unified protective goals and to reduce trade barriers. The area of application of the Machinery Directive corresponding to its definition "Machinery means an assembly of linked parts or components, at least one of which moves..." and is extremely extensive. With the Change Directives, the area of application has been subsequently extended to "safety components" and "interchangeable equipment." The Machinery Directive involves the implementation of machines.

"Machinery" is also defined as an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole"..

The application area of the Machinery Directive thus ranges from a basic machine up to a complete plant.

* Presently, discussions are taking place in the various Associations of the EU about a new Edition of the Machinery Directive. It is presently not possible to make definitive statements regarding the changes that can be expected and when it will be published.

Machinery Directive

Application area, selling, marketing, freedom of movement, health and safety requirements Art. 1 – Art. 7	Certification procedure Art. 8 – Art. 9	CE marking, protection against arbitrary fulfillment Art. 10 – Art. 12	Coming into force, transitional regulations, cancellation of the regulations Art. 13 – Art. 14

Annex		Article
I	Essential health and safety requirements relating to the design and construction of – machinery, and • interchangeable equipment • safety components	3 5 10
II	Contents of 1. EC Declaration of Conformity for – machinery, and • interchangeable equipment • safety components 2. Manufacturer's declaration for – specific components of the machinery – non-functioning machines	4 5 8 4
III	CE marking	10
IV	Types of machinery and safety components, where the procedure acc. to Article 8 must be applied.	
V	EC Declaration of conformity for – machinery, and • interchangeable equipment • safety components	8
VI	EC type examination for – machinery and • interchangeable equipment • safety components	8
VII	Minimum criteria for testing bodies	9

Fig. 1/1
Overview of the Machinery Directive

The Machinery Directive has 14 Articles and 7 Annexes.

The basic health and safety requirements in the Appendix I of the Directive must be complied with for the safety of machinery. In selecting the most appropriate methods, the manufacturer must apply the following principles (Annex I Paragraph 1.1.2):

a) "Machinery must be constructed that it is **fitted for its function**, **and can be adjusted** and **operated** without putting persons at risk when these operations are carried out under the conditions forseen by the manufacturer." "The measures must exclude any risk of accident..."

b) "When selecting the adequate solutions, manufacturers must apply the following principles, and more specifically in the specified sequence:

- Eliminate or minimize the hazards (integrating the safety-concept into the development and construction of the machine);
- Apply the necessary protective-measures against hazards that cannot be avoided;
- Inform users about the residual hazards as a result of the fact that the safety measures applied are not completely effective.

The protective goals must be responsibly implemented in order to fulfill the demand for conformance with the Directive.

The manufacturer of a machine must prove that the basic requirements have been fulfilled. This proof is made easier by applying harmonized standards.

A certification technique is required for machines listed in Annex IV of the Machinery Directive, which represent a more significant hazard potential. (Recommendation: Machinery, which is not listed in Annex IV, can also represent a high potential hazard and should be appropriately handled.) The precise "technique to define whether compliance exists" with the goals, is defined in Chapter II of the Directive.

Types of machinery and safety components, for which the procedure referred to in Article 8, Paragraph 2, Letters b) and c) must be applied.

A. Machinery

1. Circular saws (single or multi-blade) for working with wood and analogous materials or for working with meat and analogous materials
1.1. Swing machines with fixed tool during operation, having a fixed bed with manual feed of the workpiece or with a demountable power feed
1.2. Sawing machines with fixed tool during operation, having a manually operated reciprocating saw-bench carriage
1.3. Sawing machines with fixed tool during operation, having a built-in mechanical feed device for the workpieces, with manual loading and/or unloading
1.4. Sawing machines with movable tool during operation, with a mechanical feed device and manual loading and/or unloading
2. Hand-fed surface planing machines for woodworking
3. Thicknesses for one-side dressing with manual loading and/or unloading for woodworking
4. Band-saws with fixed or mobile bed and band-saws with a mobile carriage, with manual loading and/or unloading, for working with wood and analogous materials or for working with meat and analogous materials
5. Combined machines of the types referred to in 1 to 4 and 7 for working with wood and analogous materials
6. Hand-fed tenoning machine with several tool holders for woodworking
7. Hand-fed vertical spindle molding machines for working with wood and analogous materials
8. Portable chain saws for woodworking
9. Presses, including press-brakes, for the cold working of metals, with manual loading and/or unloading, whose movable working parts may have a travel exceeding 6 mm and a speed exceeding 30 mm/s
10. Injection or compression plastic-molding machines with manual loading or unloading
11. Injection or compression rubber-molding machines with manual loading or unloading
12. Machinery for underground working or the following types:
    – Machinery or rails: Locomotives and brake-vans
    – Hydraulic-powered roof supports
    – Internal combustion engines to be fitted to machinery for underground working
13. Manually-loaded trucks for the collection of household refuse incorporating a compression mechanism
14. Guards and detachable transmission shafts with universal joints as described in Section 3.4.7.
15. Vehicle-servicing lifts
16. Devices for the lifting of persons involving a risk of falling from a vertical height of more than 3 meters
17. Machines for the manufacture of pyrotechnics

B. Safety components

1. Electro-sensitive personnel protective devices, e.g. light barriers, pressure-sensitive mats, electromagnetic detectors
2. Logic units which ensure the safety functions of bimanual controls
3. Automatic movable screens to protect the presses referred to in 9, 10 and 11 (Letter A)
4. Rollover protection structures (ROPS)
5. Falling-object protective structures (FOPS)

Fig. 1/2
Annex IV of the Machinery Directive

The Machinery Directive defines, in Chapter 1 Article 1 (2):

B. "Safety component"

Means a component, provided that it is not interchangeable equipment, which the manufacturer or his authorized representative established in the Community places on the market to fulfill a safety function when in use and the failure or malfunctioning of which endangers the safety or health of exposed persons.

In conjunction with the information regarding the Machinery Directive, this can be interpreted as follows.

"Safety components are characterized by the fact that they must have an appropriate purpose - specified by the manufacturer (as safety component) in the sense of the Directive. In the explanation regarding the Directive, in Section 76 it is defined that components "that must fulfill an operating function" are not safety components. This also applies if their failure would result in a potential hazard and these of course must be safe. An example of a non-safety component is given in Section 81 using the hoisting cable [of a crane]. The main function of the cable is to operationally raise and lower loads, but not to provide "protection against a load dropping". When this sense is transferred, e.g. to drives, this means that generally they are not safety components as their main function is to drive a machine.

On the other hand, components with a double function - for example two-hand switches - are then considered to be a safety component if the safety function (protection of the operator) has far more significance that the operating function (initiating operations) (Section 80 of information on the Machinery Directive).

Individual parts, that must be assembled with additional parts or software programs that are separately purchased, in order to implement a safety function, can themselves not be safety components. This also applies if these individual components are expressly intended to be used in safety components.

Standards

To sell, market or operate products, these products must fulfill the basic safety requirements of the EU Directives. Standards can be extremely helpful when it involves fulfilling these safety requirements. In this case, a differentiation must be made between harmonized European Standards and other Standards, which although are ratified, have still not been harmonized under a specific Directive, as well as other technical rules and regulations which are also known as "National Standards" in the Directives.

Ratified standards define the recognized state-of-the-art technology. This means, that by proving that he has applied them, a manufacturer can prove that he has fulfilled what is recognized to be state-of-the-art technology.

All Standards, that are ratified as European Standards, must be included, unchanged in the National Standards of the Member States. This is independent of whether they are harmonized under one Directive or not. Existing domestic Standards, handling the same subject, must then be withdrawn. This means that over time, a series of standards (without any conflicting statements) will be created in Europe.

Note: IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" is an important Standard that is not harmonized under an EU Directive.
It is ratified as EN 61508. (The preliminary Standards DIN V VDE 0801 and DIN V 19250 and 19251 were therefore withdrawn by August 2004.)
There, where EN 61508 is referenced in a harmonized standard, it is a standard that is "also applicable" to the associated harmonized Standard.

Harmonized European Standards

These are drawn up by the two standards organizations CEN (Comité Européen de Normalisation) and CENELEC (Comité Européen de Normalisation Électrotechnique) as mandate from the EU Commission in order to specify the requirements of the EU Directives for a specific product. These must be published in the official Council Journal of the European communities. These Standards (EN Standards) will be published in the official Council Journal of the European Communities and must be then included in the domestic standards without any changes.

They are used to fulfill the basic health and safety requirements and the protective goals specified in Annex I of the Machinery Directive.

In Germany, the contact partner for CEN/CENELEC is DIN and DKE.

By fulfilling such harmonized standards, there is an "automatic presumption of conformity," i.e. the manufacturer can be trusted to have fulfilled all of the safety aspects of the Directive as long as they are covered in the particular Standard. However, not every European Standard is harmonized in this sense. The listing in the European documentation is definitive The updated lists are also available in the Internet

(Address:
http://www.newapproach.org/)

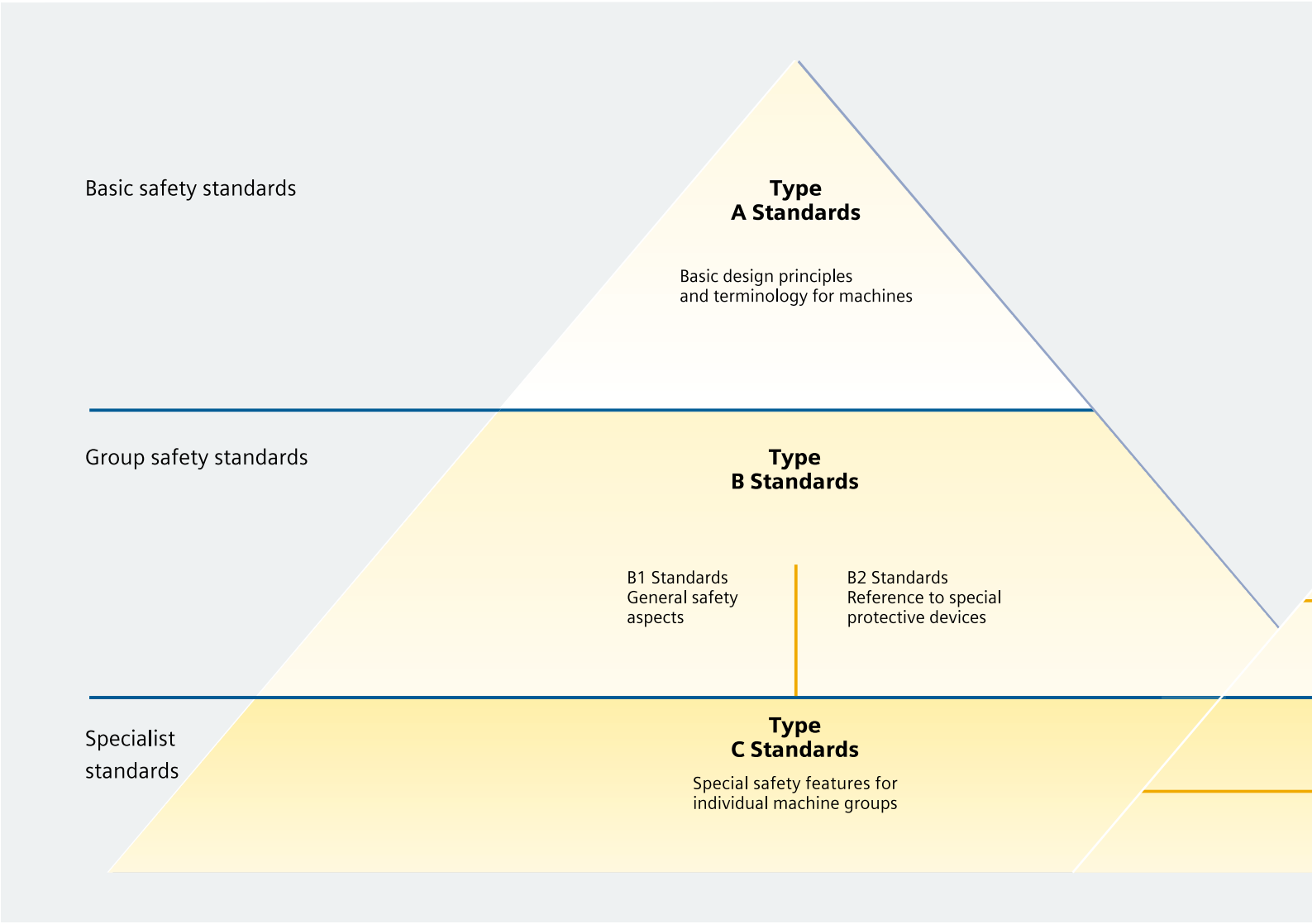


Fig. 1/3
The European Standards for safety of machines

European Standards for the safety of machinery are hierarchically structured as follows

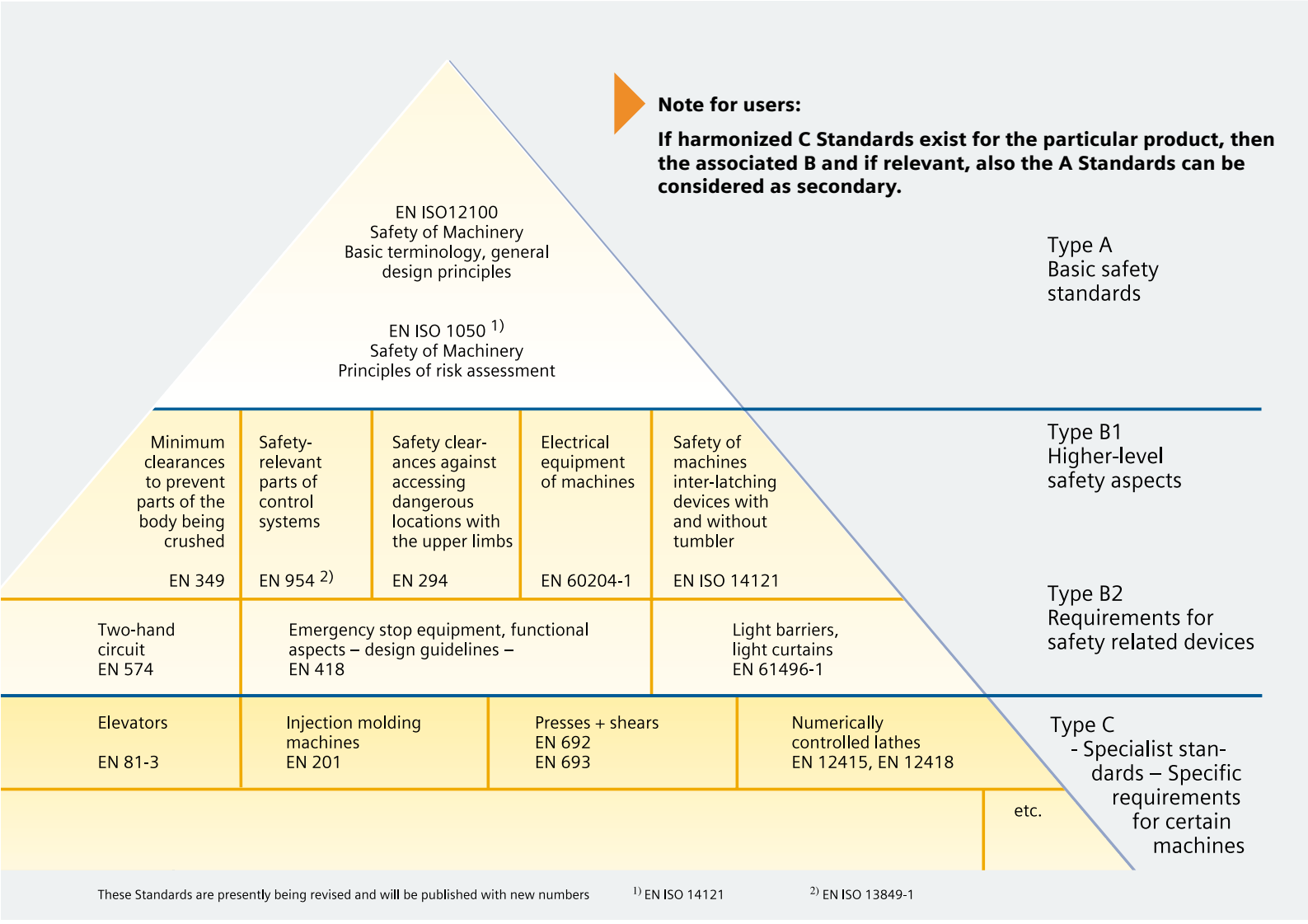
- A Standards,
  also known as Basic Standards.
- B Standards,
  also known as Group Standards.
- C Standards,
  also known as Product Standards.

The structure is shown in the diagram above.

Type A Standards/Basic Standards

Type A Standards contain basic terminology and definitions for all machines. This also includes EN ISO 12100 (earlier EN 292) "Safety of machinery, basic terminology, general design guidelines."

Type A Standards primarily address those parties setting B and C Standards. The techniques and methods discussed there to minimize risks can also be helpful for manufacturers if there are no applicable C Standards.



Type B Standards/Group Standards

These include all Standards with safety-related statements that can address several types of machines.

Type B Standards also primarily address those parties setting C Standards. However, they can also be helpful to manufacturers when designing and constructing a machine if there are no applicable C Standards.

For B Standards an additional subdivision was made:

Type B1 Standards for higher-level safety aspects, e.g. ergonomic design principles, safety distances from potential sources of danger, minimum clearances to prevent crushing of body parts.

Type B2 Standards for safety equipment are for various machine types, e.g. Emergency Stop devices, 2-hand circuits, interlocking functions, contactless protective equipment and devices, safety-related parts of controls.

Type C Standards/Product Standards

These involve Standards for specific machines - e.g. for machine tools, woodworking machines, elevators/lifts, packaging machinery, printing machines and others.

The European Standards are structured so that general statements that are already included in type A or type B standards are not repeated. References to these are made in type C Standards

Product Standards include machinery-specific requirements. These requirements, under certain circumstances, deviate from the Basic and Group Standards. The Type C Standard/Product Standard has absolutely the higher priority for the machinery construction OEM. They (the machinery OEMs) can then assume that they fulfill the basic requirements of Annex I of the Machinery Directive (automatic presumption of conformity).

If there is no Product Standard for a particular machine, then Type B Standards can be applied for orientation purposes when designing and constructing machinery.

In order to provide a method to harmonize the basic requirements of the Directive, with the mandate of the EC commission, harmonized standards were drawn-up in the technical committees of the CEN and CENELEC for machinery and machinery groups for almost all areas. Drawing-up standards essentially involves representatives from the manufacturer of the particular machinery, the regulatory bodies, such as Trade Associations as well as users. A complete list of all of the listed Standards as well as the activities associated with Standards - with mandated new Standards for the future - are provided in the Internet under:

http://www.newapproach.org/

Recommendation: Technology is progressing at a tremendous pace which is also reflected in changes made to machine concepts. For this reason, especially when using Type C Standards, they should be checked to ensure that they are up-to-date. It should also be noted that it is not mandatory to apply the Standard but instead, the safety objective must be achieved.

Domestic Standards

If there are no harmonized European Standards or they cannot be applied for specific reasons, then a manufacturer can apply the "Domestic Standards". All of the other technical rules fall under this term, e.g. also the accident prevention regulations and standards, which are not listed in the European Council Journal (also IEC or ISO Standards which were ratified as EN). By applying ratified standards, the manufacturer can prove that recognized state-of-the-art technology was fulfilled. However, when such standards are applied, the above mentioned "automatic presumption of conformity" does not apply.

Risk evaluation/assessment

As a result of their general design and functionality, machines and plants represent potential risks. Therefore, the Machinery Directive requires a risk assessment for every machine and, if relevant, risk reduction, so that the remaining risk is less than the tolerable risk. The following Standards should be applied for the techniques to evaluate these risks

- EN ISO 12100 "Safety of machinery – basic terminology, general design guidelines" and
- EN 1050 "Safety of machinery, guidelines to evaluate risks"

EN ISO 12100 mainly describes the risks to be considered and design guidelines to minimize risk, EN 1050 focuses on the iterative process with risk assessment and risk reduction to achieve safety. (refer to Chapter 2 for an explanation of this technique.)

Risk assessment

Risk assessment is a sequence of steps that allows hazards, which are caused by machines, to be systematically investigated. Where necessary, the risk assessment phase is followed by risk reduction. The iterative process is obtained by repeating this procedure (refer to Fig. 1/5). Using this process, hazards, as far as possible, can be eliminated and the appropriate protective measures can be applied.

Risk assessment encompasses

- Risk analysis
  - a) Determining the limits of the machine (EN ISO 12100, EN 1050 Para. 5)
  - b) Identifying the hazards (EN ISO 12100, EN 1050 Para. 6)
  - c) Techniques to assess the risk (EN 1050 Para. 7)
- Risk evaluation (EN 1050 Para. 8)

After risks have been estimated, a risk evaluation is made as part of an iterative process to achieve safety. In this case, a decision has to be made

Fig. 1/4
Risk elements

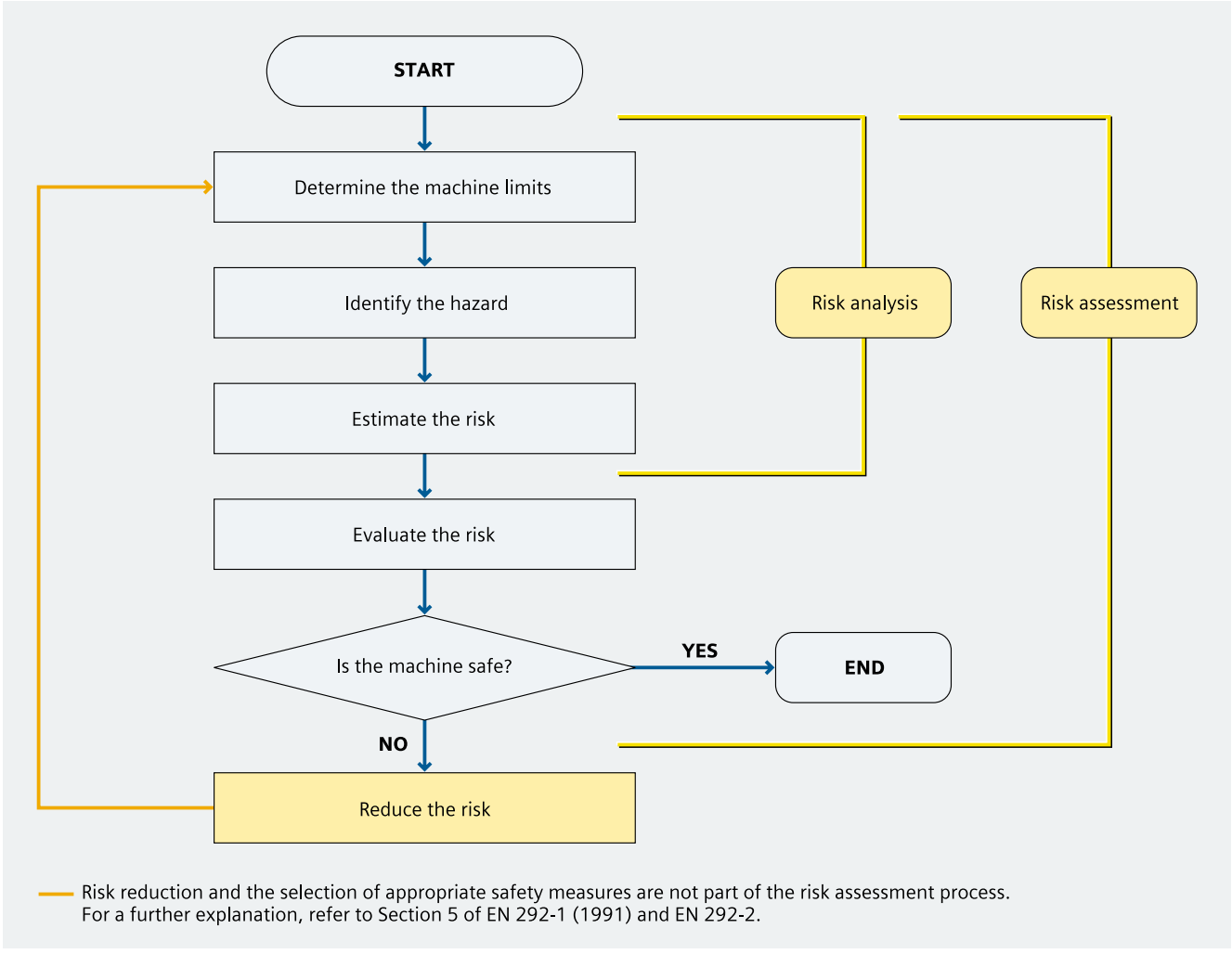


Fig. 1/5
Iterative process to achieve safety in accordance with EN 1050
Note: EN 292-1 /-2 referenced in EN 1050 have in the meantime been replaced by EN ISO 12100-1 /-2.

whether it is necessary to reduce a risk. If the risk is to be further reduced, suitable protective measures must be selected and applied. The risk evaluation process must then be repeated.

Risk elements are defined as a support tool to evaluate risks. Fig. 1/4 clearly shows the interrelationship between these risk elements.

If the required degree of safety has still not been reached, measures are required to further reduce the risk.

The risk must be reduced by suitably designing and implementing the machine. For instance, using suitable control or protective measures for the safety functions (also refer to the Section "Requirements of the Machinery Directive"). If the protective measures involve interlocking or control functions, then these must be configured in accordance with EN 954. Further, electronic control and bus systems must also in compliance with IEC / EN 61508. As an alternative to EN 954, EN 62061 can be used for electrical and electronic control systems.

Residual risk (EN 1050)

Safety is a relative term in our technical environment. Unfortunately, it is not possible to implement the so-called "zero risk guarantee" where nothing can happen under any circumstance. The residual risk is defined as: Risk that remains after the protective measures have been implemented.

In this case, protective measures represent all of the measures to reduce risks.

Reducing risks

In addition to applying structural measures, risk reduction for a machine can also be realized using safety-related control functions. Specific requirements must be observed when implementing these control functions, graduated according to the magnitude of the risk. These are defined in EN 954-1 and, for electrical control systems, especially with programmable electronics, in IEC 61508.

The requirements placed on safety-related parts of control systems are graduated according to the magnitude of the risk and the necessary risk reduction.
For this purpose, EN 954-1 defines "Categories" and in its Annex B describes a technique to select the suitable category to design the safety-related parts of a control. New risk diagrams will be provided in the new Edition (EN ISO 13849-1), that instead of categories, will result in hierarchically graduated levels.

IEC 62061 uses "Safety Integrity Level" (SIL) to achieve this graduation. This is a quantified measure for the safety-related performance of control. The necessary SIL is determined according to the principle of the risk evaluation according to EN 1050. A technique to define the necessary Safety Integrity Level (SIL) is described in Appendix A of the Standard.

It is always important - independent of which Standard is applied - that all parts of the control of the machine that are involved in implementing the safety-related functions clearly fulfill these requirements.

For details, refer to Chapter 2.

Note: The load circuits of drives and motors also belong to the control of a machine.

When designing and implementing the control it is necessary to check whether the requirements of the selected Category or of the SIL are actually fulfilled. The requirements to achieve the necessary Safety Performance are structured differently in EN 954 and IEC. This is the reason that the requirements regarding checking are also structured differently. For a design according to EN 954, the details for the validation and what has to be observed are described in Part 2 (new designation, EN ISO 13849-2). The requirements to validate a design in compliance with IEC 62061 are described in the Standard.

The next table provides a brief summary of the requirements for the Categories according to EN 954-1: 1996.
Basic requirements for configuring control systems are defined in the various categories. These are intended to make the systems tolerant to hardware failures. These requirements will partially change with the new Edition as EN ISO 13849-1 that is scheduled to appear in the immediate future.

Additional aspects must be taken into consideration for more complex control systems, especially programmable electronic systems, so that

- Random hardware failures are controlled,
- Systematic faults/errors in the hardware and the software are avoided and

Category[1]	Summary of requirements	System behavior[2]	Principles to achieve safety
B	The safety-related parts of control systems and/or their protective equipment, as well as their components, shall be designed, constructed selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence.	The occurrence of a fault can lead to the loss of the safety function	Mainly characterized by selection of components
1	The requirements of B shall apply. **Well-proven components** and **well-proven safety principles** must be applied.	The occurrence of a fault can result in the loss of the safety function, but the probability of occurrence is less than in Category B.	
2	The requirements of B and the use of well-tried safety principles shall apply. The safety function shall be checked at suitable intervals by the machine control system.	– The occurrence of a fault can lead to the loss of the safety function between the checks. – The loss of the safety function is detected by the check.	Mainly characterized by structure
3	The requirements of B and the use of **well-proven safety principles** must be fulfilled. Safety-related parts shall be designed, so that: – a single fault in any of these parts does not lead to the loss of the safety function, and – whenever reasonably practicable, the single fault is detected.	– If the individual fault occurs, the safety function always remains. – Some but not all faults will be detected. – Accumulation of undetected faults can lead to the loss of the safety function	
4	The requirements of B and the use of **well-proven safety principles** must be fulfilled. Safety-related parts shall be designed so that: – a single fault in any of these parts does not lead to a loss of the safety function and – the single fault is detected at or before the next demand upon the safety function. If this is not possible, then an accumulation of faults shall not lead to a loss of the safety function	– If faults occur, the safety function always remains. – The faults will be detected in time to prevent the loss of the safety function.	

[1] The categories are not intended to be used in any given order or in any given hierarchy in respect of safety requirements.

[2] The risk assessment will indicate whether the total or partial loss of the safety function(s) arising from faults is acceptable.

- Systematic faults/errors in the hardware and software are controlled,

and sufficient functional safety is achieved for safety-critical tasks.
The international Standard IEC 61508 (identical to IEC 61508) defines the requirements and for contactless (electronic protective devices such as light grids or laser scanners, IEC / EN 61496. The scope of the required measures is also graduated corresponding to the risk reduction required.

The most recent technical developments allows complex systems to be used for safety-related functions as long as these fulfill the requirements of IEC 61508. In order to take this into account, the new Standard IEC 62061 was developed for machine controls and the existing EN 954-1 was revised. The latter will be published with the new designation ISO 13849-1.
Both of these standards are intended to make it possible for the user to configure safety-related controls using suitable electrical and electronic components without having to apply IEC 61508 themselves.

IEC 62061 assumes that the electronic devices used already fulfill IEC 61508 and describes a concept to also implement complex and sophisticated safety functions. This concept specifically addresses companies that integrate machine control systems and allow the Safety Performance that is achieved to be quantified without complicated calculations.

Fig. 1/6
Description of the requirements for Categories acc. to EN 954-1

The concept of the future ISO 13849-1 is restricted to specific, basic architectures and integrates the essential and necessary requirements from IEC 61508. The requirements for safety-related parts of controls based on electro-mechanical components has been supplemented with respect to EN 954-1 so that also here, it is possible to hierarchically graduate the safety performance in a quantifiable fashion.

Please refer to Chapter 2 to decide as to whether ISO 13849 or IEC 62061 should be applied.

Validation

In this case, validation means that the safety functionality to be achieved is checked and evaluated. The purpose of validation is to confirm the definitions and the level of the conformity of the safety-related parts of the control within the overall definition of the safety requirements at the machine. Further, the validation must indicate that each and every safety-related part fulfills the requirements of the relevant Standard. The following aspects are described:

- Fault lists
- Validation of the safety functions
- Validation of the specified and the achieved safety performance (Category, Safety Integrity Level or Performance Level)
- Validation of the environmental/ ambient requirements
- Validation of the service&maintenance requirements

The requirements for carrying-out the validation for the defined safety functions must be described in a validation schedule.

Safety Integrated

The measures which are required to make a complex control adequately and functionally safe for safety tasks are extremely extensive and involve the complete development and production process. This is the reason that devices such as these were specifically designed for safety functions. Examples include SIMATIC S7-300F / S7 400F/FH and SINUMERIK "Safety Integrated" as well as the communication systems PROFIsafe and ASIsafe, the Profibus and AS-Interface that are used to transfer safety-related data.

Safety-related functions

Safety-related functions include, in addition to conventional functions

- Stopping
- Operator actions in an emergency
- Preventing undesirable starting

In the meantime, also more complex functions such as

- Status-dependent interlocking functions
- Velocity limiting
- Position limits
- Controlled stopping
- Controlled holding etc.

The classic functions are defined in EN 60204-1 and were, up until now, generally implemented using mechanical components. Electronic programmable systems can also be used to implement more complex functions if they fulfill the relevant Standards (IEC 61508, EN 954). Complex functions, e.g. which involve the behavior of variable-speed drives, are described in draft IEC 61800-5-2.

Stop

Stop categories of EN 60204-1

Three stop categories are defined in EN 60204-1 (VDE 0113 Part 1) which define the control sequence for stopping, independent of an emergency:

Stop category 0

Uncontrolled stop by immediately removing the power to the machine drive elements.

Stop Category 1

Controlled stop; the power is only removed after the machine has come to a standstill.

Stop Category 2

Controlled stop, where power is still fed to the machine at standstill.
Note: When shutting down, only the power feed that can cause movement, is interrupted. The plant/system is not brought into a no-voltage condition.

Emergency operations and actions

EN 60204-1/11.98 has defined possible operator actions for emergencies (EN 60204-1, Appendix D). The terminology in brackets corresponds to the version in the final draft, Edition 5.0 of IEC 60204-1).

Operator action in an emergency includes, individually, or a combination of the following:

- Stopping in an emergency (Emergency Stop);
- Starting in an emergency (Emergency Start);
- Power-off in an emergency (Emergency Switching-Off);
- Power-on in an emergency (Emergency Switching-On).

According to EN 60204-1 and EN 418 (new Edition of ISO 13850), these functions are exclusively initiated by a conscious, operator action. In the following text, only "Power-off in an emergency" and "Stopping in an emergency" will be discussed. The latter fully corresponds to the term with the same name in the EU Machinery Directive (Emergency Stop). For reasons of simplicity, EMERGENCY SWITCHING-OFF and EMERGENCY STOP will be used in the following.

EMERGENCY SWITCHING-OFF

This is an action in an emergency, which disconnects power to a complete system or installation or part of it if there is a risk of electric shock or another risk caused by electricity (from EN 60204-1 Annex D).

Functional aspects to disconnect the power in an emergency are defined in IEC 60364-4-46 (this is identical to HD 384-4-46 and VDE 0100 Part 460).

Switching-off in an emergency should be implemented, if

- Protection against direct contact (e.g. with contact wires, contact-assemblies, switching devices in rooms accommodating electrical equipment) can only be achieved through providing the appropriate clearance or the appropriate barriers;
- There is a possibility of other hazards or damage as a result of electrical energy.

Further, the following is specified in 9.2.5.4.3 of EN 60204-1:
In an emergency, the power supply is disconnected from the machine, which results in a Category 0 Stop.

If a Category 0 Stop is not permissible for a machine, then it may be necessary to provide other protection, e.g. against direct contact, so that power does not have to be disconnected in an emergency.

This means that emergency switching-off should be used there where the risk analysis indicates a hazard as a result of the electrical voltage/power and therefore the electric power must be immediately and completely disconnected.

In the EU, EMERGENCY SWITCHING-OFF devices fall under the Low-Voltage Directive 73/23/EEC if they are not used in conjunction with machines.

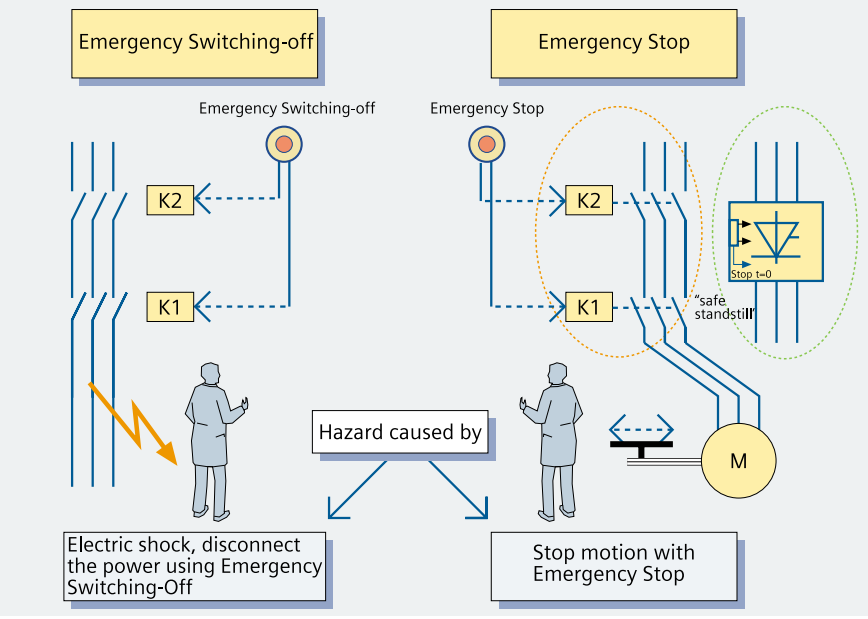


Fig. 1/7
Difference between Emergency Switching-Off and Emergency Stop

If they are used in conjunction with machines, then just like all of other electrical equipment of the machine, they also come under the Machinery Directive 98/37/EC.

Emergency Stop

This is an action in an emergency, which is defined to stop a process or movement which would otherwise have potentially hazardous consequences (from EN 60204-1 Annex D). Further, the following is defined in 9.2.5.4.2 of EN 60204-1:

Stopping

In addition to the requirements for Stop (refer to 9.2.5.3), the following requirements apply for an Emergency Stop:

- This must have priority over all other functions and operator actions in all operating modes;
- The power to the machine drive elements, that could result in a potentially hazardous condition or potentially hazardous conditions, must be disconnected as quickly as possible without creating other hazards(e.g. using mechanical stopping devices, that do not require an external supply, using countercurrent braking for stop Category 1);
- A reset may not initiate a restart.

Stopping in an emergency must either be effective as a Category 0 or Category 1 stop (refer to 9.2.2).

The stop Category in an emergency must be defined as the result of the risk evaluation for the particular machine.

To technically implement Emergency Stop corresponding to the recommended application in the Foreword of EN 60204-1, either the requirements specified in EN 60204-1 or in EN 954 and IEC 61508 can be applied. EN 60204-1 Edition 4 specifies the implementation predominantly using electromechanical components.
The reason for this is that "basic" (programmable) electronic systems are not sufficiently safe. By correctly applying EN 954 - and if required IEC 61508 - electronic and programmable electronic components are functionally safe so that they can also be used to implement an Emergency Stop function for all categories.

The Emergency Stop function specifications will be updated with Edition 5 (this is expected in 2005). In the final draft of 2004 (the final Edition was still not available at the time that this document when to print) the following statement applies:

The Emergency Stop shall function either as a Category 0 stop or as a Category 1 stop (see 9.2.2). The choice of the category of the Emergency Stop depends on the results of a risk assessment of the machine.

In addition to the requirements for stop (see 9.2.5.3), the Emergency Stop function has the following requirements:

- *It shall override all other functions and operations in all modes;*
- *Power to the machine actuators that can cause a hazardous condition(s) shall be either removed immediately (stop Category 0) or shall be controlled in such a way to stop the hazardous motion as quickly as possible (stop Category 1) without creating other hazards;*
- *Reset shall not initiate a restart.*

This new formulation means that there are no longer any restrictions stating that hard-wired, electromechanical equipment must be used to implement safety-related functions.

Devices for EMERGENCY SWITCHING-OFF and EMERGENCY STOP

Devices that are used to stop equipment and machinery in an emergency must be provided at every operator control location and also at other locations where it may be necessary to initiate a stop in an emergency (exception: operator control stations which are not connected through cables).

In order to fulfill the protective goals, specified in EN 60204-1 as well as EN 418, the following requirements apply for both functions (also refer to 10.7 in EN 60204-1):

- When the contacts switch, even when briefly actuated, the command device must positively latch.
- It is not permissible that the machine can be restarted from a remote main operator station without the hazard having first been removed. The emergency switching command must be released locally in the form of a conscious operator action.

Wireless operator control stations must have their own function - that can also be clearly identified - to initiate a machine stop. The operator control station that initiates this stop function may neither be marked nor labeled as a device for emergency stopping.

Implementing safety-related functions

When implementing safety-related control functions, the requirements of ISO 13849 (EN 954) and IEC 62061 (IEC 61508) must be complied with corresponding to the specified risk reduction. When the requirements of these standards are taken into account, it is possible, to even implement complex functions by using electronic and programmable electronic systems, for example, a fail-safe SIMATIC or SINUMERIK. These functions can then be implemented in a safety-related fashion.

Man-machine (color coding for operator control devices and displays)

In order to simplify the interaction between man and machine, Standards EN 60073 and DIN EN 60204 specify the appropriate coding.

Switches, pushbuttons and signaling lamps are predominantly used as the interface between man and the machine. These operator control elements are clearly identified and coded using colors that are assigned a very specific significance. This guarantees that the degree of safety for the operating personnel is increased and it is also simpler to operate and service the equipment/ systems.

The colors of pushbuttons, the significance of these colors, explanations and application examples are shown in Fig. 1/8.
According to DIN EN 60204-1 (VDE 0113 Part 1) the following has to be observed:

WHITE, GREY or BLACK are the colors that can be used for START/ON operator command devices - preferably WHITE. GREEN may be used, RED may not be used.

RED must be used for Emergency Switching-Off and Emergency Stop command devices.

The colors for STOP/OFF operator control devices should be BLACK, GREY or WHITE - preferably BLACK. RED is also permitted. It is not permissible to use GREEN.

WHITE, GREY and BLACK are the preferred colors for pushbuttons, which can be used alternating as START/ON and STOP/OFF pushbuttons. It is not permissible to use RED, YELLOW or GREEN.

WHITE, GREY and BLACK are the preferred colors for pushbutton command devices that result in an operating sequence while they are actuated and operation is terminated if they are released (e.g. jogging).

It is not permissible to use RED, YELLOW or GREEN.

GREEN is reserved for functions that display a safe or normal operating condition.

YELLOW is reserved for functions that display an alarm or a non-standard (abnormal) condition.

BLUE is reserved for functions that require a specific action.

Reset pushbuttons must be BLUE, WHITE, GREY or BLACK. If they also act as STOP/OFF pushbuttons, WHITE, GREY or BLACK are permissible - but preferably BLACK. It is not permissible to use GREEN.

If the same color - white, grey or black - is used for various functions (e.g. white for start/on and stop/off actuator), additional coding means (e.g. in the form of shape, position, symbol) must be used for identification purposes.

The colors of the indicating lamps, their significance with reference to the status of the machine as well as their handling and application examples are listed in Fig. 1/9.

For illuminated pushbuttons, the information in Figs. 1/8 and 1/9 applies. If problems are encountered when assigning suitable colors, then the color WHITE must be used.
For Emergency Switching-Off devices, the color RED may not depend on the illumination.

Color	Meaning	Explanation	Examples of application
RED	Emergency	Actuate in the event of a hazardous condition or emergency	EMERGENCY STOP, Initiation of EMERGENCY STOP functions, conditional for STOP/OFF
YELLOW	Abnormal	Actuate in the event of an abnormal condition	Intervention to suppress an abnormal condition, Intervention to restart an interrupted automatic cycle
GREEN	Normal	Actuate to initiate normal conditions or normal status	START/ON, however WHITE should be preferably used
BLUE	Mandatory	Actuate for a condition requiring mandatory action	Reset function
WHITE	No specific meaning assigned	For general initiation of functions except for EMERGENCY STOP (see note)	START/ON (preferred), STOP/OFF
GREY			START/ON, STOP/OFF
BLACK			START/ON, STOP/OFF (preferred)

Comment: Where a supplemental means of coding (e. g. shape, position, texture) is used for the identification of pushbutton actuators, then the same color WHITE, GREY or BLACK may be used for various functions , e. g. WHITE for START/ON and for STOP/OFF actuators.

Fig. 1/8
Colors for pushbuttons and their significance according to EN 60204-1 (VDE 0113 Part 1): 06.93

Color	Meaning	Explanation	Action by operator	Examples of application
RED	Emergency	Hazardous condition	Immediate action, to deal with a hazardous condition (e. g. by operating EMERGENCY STOP)	Pressure/ temperature outside safe limits, voltage drop, voltage interrupted, passing through a stop position
YELLOW	Abnormal	Abnormal condition impending critical condition	Monitoring and/ or intervention (e. g. by re-establishing the intended function)	Pressure/temperature outside normal operating ranges, tripping a protective device
GREEN	Normal	Normal condition	Optional	Pressure/temperature within the normal operating ranges, per missive signal to continue
BLUE	Mandatory	Indication of a condition that requires action by the operator	Mandatory action	Prompt to enter specified values
WHITE	Neutral	Other conditions: may be used whenever doubt exists about the application of RED, YELLOW, GREEN or BLUE	Monitoring	General information

Fig. 1/9
Colors for indicator lights and their significance acc. to EN 60204-1 (VDE 0113 Part 1): 06.93

Coding cables

The color coding of switches, push-buttons and indicator lamps has been discussed in the previous Section. EN 60204 offers a higher degree of flexibility when coding cables. It specifies that "... cables at every connection must be able to be identified in conformance with the technical documentation..." .

The numbering of terminals matching the circuit diagram is sufficient if it is possible to visually trace the cable. For complex controls, we recommend that the internal cables used for wiring as well as the outgoing cables are coded so that after the cable has been disconnected from the terminal it can be easily reconnected to the same terminal. This is also recommended for terminal locations which have to be disconnected when the equipment is transported.

Using the formulation in IEC 60204-1 1997, Paragraph 14.2.1 conductor coding/identification, the Standards Committee wanted to make the following statement:

1. Each individual conductor must be able to be identified, however, only in conjunction with the documentation. It is not necessary that every cable must be able to be identified without the appropriate documentation.

2. The manufacturer and the operating company should agree on the type of coding and therefore also the identification techniques.

It is not the intention of the Standard to specify a certain coding type that is worldwide.
For instance, for safety reasons, factory-internal specifications may have a higher priority in order to avoid confusion in specific areas that are handled by the same personnel. These definitions cannot be generalized due to the wide application range of the particular Standard - from small individual machines (high unit volume standard products) up to large, complex plants (with unique equipment and systems).

Primarily, appropriate testing should be used to avoid installation/assembly faults.

A standard color coding for the cables should be used. We recommend the following color assignment:

- Black for
  main AC and DC current circuits

- Red for
  AC control circuits

- Blue for
  DC control circuits

- Orange for
  interlocking circuits that are supplied from an external power source.

The above color assignment is recommended if a decision is made to just use color coding. The only mandatory specification is the color coding of the protective conductor and the neutral conductor. For all other cabling and wiring, one of the methods listed in 14.2.4 can be selected (color, numbers or letters; or a combination of colors and numbers or colors and letters).

Protective conductor marking

The protective conductor must be able to be uniquely identified as a result of its shape, location, coding or color. If it is only identified as a result of its color, then a two color-combination of green/yellow must be used along the whole length of the cable. The green/yellow color may only be used for protective conductors.

Neutral conductor marking

If a circuit has a color-coded neutral conductor, then light blue must be used. Light blue may not be used to code other cables if there is a danger of accidentally interchanging them.

If a neutral conductor is not used, a light-blue conductor may be used for other purposes, but not as protective conductor.

Process technology in Europe

Legislative requirements in Europe

The following EU Directives must be essentially applied for process technology:

- Directive 96/82/EC of the Council from the 9th December 96 to control hazards when critical accidents occur with hazardous substances (“Seveso Guideline ” II).
- Low-Voltage Directive
- Machinery Directive (98/37/EC)
- Pressure Equipment Directive (97/23/EC). It is only relevant as the equipment used must fulfill this directive. “The Directive on the other hand is not valid for the assembly of pressurized equipment that is located on the user's grounds, for example, in industrial plants, under his responsibility.”

At the same time, the Health and Safety at Work and Accident Prevention Regulations must always be carefully observed and adhered to.

“Seveso Directive”

An important component of this EU Directive is the fact that companies are responsible in setting-up and implementing a safety management system. This must include an in-depth risk assessment, taking into account all of the possible accident scenarios. It specifies, corresponding to the principles explained in the Introduction, the safety objective,

⇒ using preventive measurements to maintain the quality of the environment and ensure the health and safety of people."

In order to achieve this goal, the following basic requirements have been drawn-up. The Member States must ensure that these are fulfilled.

⇒ Concept to avoid severe accidents

The owner/operating company is responsible for “... drawing-up a document setting-out his major accident prevention policy and appropriate steps to ensure that it is properly implemented. A high degree of protection for man and the environment should be ensured using a concept implemented by the operating company to avoid severe accidents by using suitable measures, organization and management systems” (Article 7 Paragraph 1).

The document must also take into account the following basic principles:

- The concept to avoid severe accidents must be drawn-up in writing.
- A safety management system, in which, among others, the following points are regualted:
  - Determine and evaluate the risks – determine and use methods and techniques to systematically identify risks.
  - Operational checking – determine and use methods and techniques for safety-related operation, including the service&maintenance of plants and systems.
  - Quality assurance – determine and use methods and techniques to continually evaluate and ensure that goals and objectives are achieved.

⇒ Safety report

The operating company is responsible in drawing-up a safety report in which the following is shown

- That a concept was implemented,
- That the hazards have been determined and all of the required measures have been applied to avoid such accidents and to limit the consequences for both man and the environment, and
- Design, construction as well as the operation of all plants and systems is sufficiently safe and reliable.

⇒ Inspection

The regulatory bodies must set up a system of inspections to systematically check the operational, organizational and management-specific systems of the operation which will allow these regulatory bodes to confirm that the user/operating company can prove

- That it has taken all of the required measures to avoid severe accidents, and has provided
- Adequate measures to limit the consequences.

This EU Directive must be nationally implemented.
In Germany this is implemented in the "Störfallverordnung" [regulation that handles responses and escalation stages when an accident occurs].

Note: The "Seveso Directive" is not a Directive of the "New Approach", i.e. the principle that when harmonized standards are applied, it can be automatically assumed that the objectives of the Directive are fulfilled, does not apply here. The exact requirements are regulated at a domestic level.

Plants and systems where these regulations apply - after a new plant has been constructed or significant changes have been made - must be checked by the appropriate regulatory body before commissioning takes place to ensure that state-of-the-art technology has been applied regarding the fulfillment of the safety goals. The assessment is based on the relevant standards.

Technical measures to fulfill legislative goals

The first priority is to design the process so that it is inherently safe. Where this is not possible, additional measures are required to reduce the remaining risk to an acceptable level. Process control technology (PLT) systems can be used to achieve this under the clear condition that they are suitable for the specific task. Electronic controllers are suitable for securing the safety of the plant if they have been specifically designed for this purpose. The requirements are described in the Standards.

Relevant Standards for safety measures using basic process control technology

For safety measures using basic process control technology - up until now the following domestic standards have been applied:

After the IEC 61508 was ratified in Europe as EN 61508, in September 2004 the domestic standards were no longer valid. Instead, EN 61508 must now be applied. The specific standard for the process industry is IEC 61511 "Functional safety: Safety instrumented systems for the process industry sector". IEC 61511 defines the requirements of EN/IEC 61508, specifically for the process industry. At the end of 2004, it can be expected that it will be ratified as EN 61511.

Beyond this, additional Standards apply for the devices and equipment used. These Standards involve the specific safety requirements. Also refer to Chapter Safety of Machinery (refer to Chapter 1.2).

In Germany, there is the VDI/VDE 2180 Directive "Ensuring the safety of process plants using process control technology", for practically implementing plant and system safety. This describes the requirements of the relevant Standard in a simplified form. The new Edition of VDI/VDE 2180 takes into account IEC 61511 and also includes the requirements from NE 31 "Securing plant safety using process control technology" and NE 79: "Micro-processor-based equipment in plant safety systems".

This document is used as a practical guideline. When it comes to selecting safety-related PLCs and other microprocessor-based components (e.g. transmitters), the two standards mentioned above offer a different perspective than the User Directives and when required, should also be taken into account.

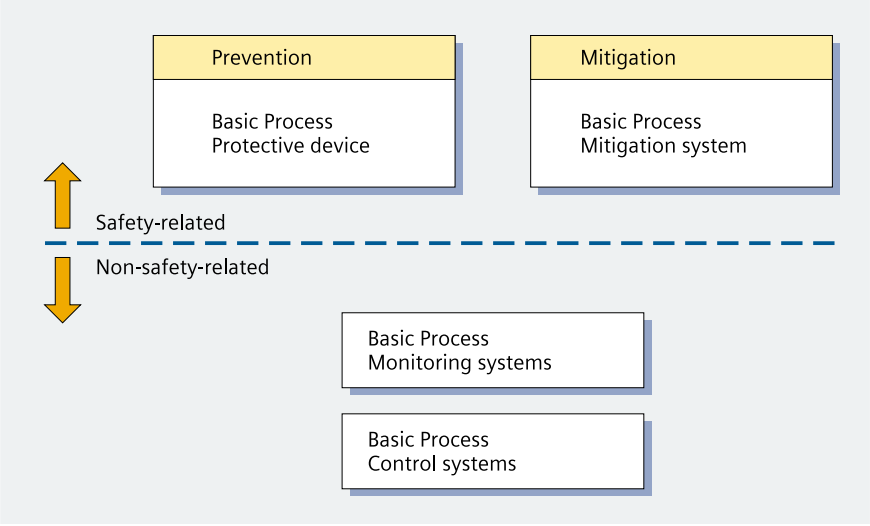


Fig. 1/10
Positioning of process control systems in safety-related/non-safety-related configurations

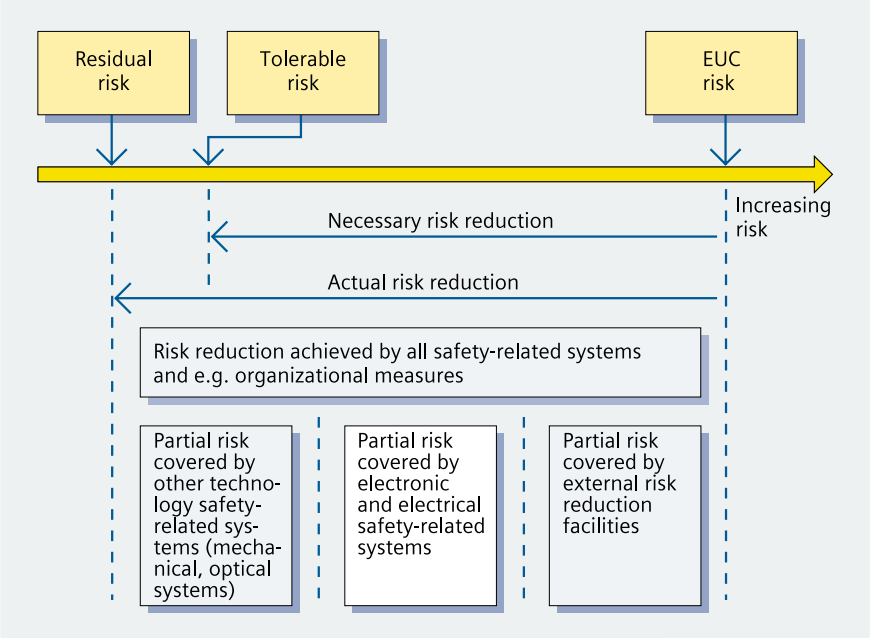


Fig. 1/11
Principle of risk reduction (acc. to IEC 61508)

Reducing risks using basic process control technology

Measures are required to reduce risks if faults or disturbances in the basic process control system and monitoring devices can lead to a dangerous event or can cause the system to go into a hazardous condition and if the resulting risk is unacceptably high. In this case, suitable protective measures must be taken, either to sufficiently reduce the probability of a hazardous event occurring or to reduce the extent of the damage. This can be achieved using basic process control protective equipment and systems if these fulfill the safety requirements.

Risk reduction

As it is not possible to completely exclude certain risks - both from a technical and economic standpoint - it is necessary not only to determine the existing risk, but also to define and specify a risk that can be tolerated. The measure for the safety integrity of the risk-reducing functions is then derived from the difference between these two factors. EN 61508 defines “Safety Integrity Level” (SIL) as a target measure for the probability of failure when executing risk-reducing functions. For safety-related systems in the process industry that operate in the requirement mode, this measure is defined in IEC 61511 as risk reduction factor.

Safety Integrity Level	High demand or continuous mode of operation (probability of a dangerous failure per hour)	Low demand mode of operation (average probability of failure to perform its design function on demand)
4	≥ 10^{-9} to < 10^{-8}	≥ 10^{-5} to < 10^{-4}
3	≥ 10^{-8} to < 10^{-7}	≥ 10^{-4} to < 10^{-3}
2	≥ 10^{-7} to < 10^{-6}	≥ 10^{-3} to < 10^{-2}
1	≥ 10^{-6} to < 10^{-5}	≥ 10^{-2} to < 10^{-1}

Fig.1/12
Safety Integrity levels according to IEC 61508: Target measure for the failure of a safety function, allocated to a safety-related system

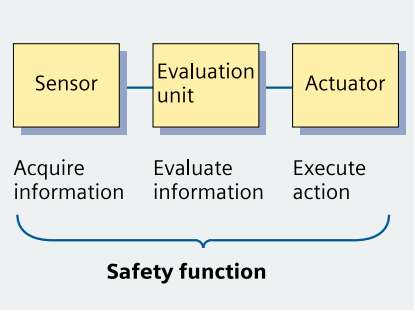


Fig. 1/13
Evaluation unit, e.g. safety PLC

Selecting the equipment and basics of the required features

Safety function

Risk reduction using electronic controllers is realized by defining functions for each possible dangerous event or each possible dangerous condition of the plant or system that prevent the dangerous event occurring. These so-called "safety functions" are used to ensure that the plant/system remains in a safe condition or a safe condition is restored if there is a threat of a hazardous event due to a fault or a disturbance in the plant or system. The safety function can also be used to reduce the extent of any damage due to a hazardous event.

The definition of a safety function always includes the specification of the function itself (e.g. shutting-off the feed to a container if the level has reached its maximum level) and the "Safety Integrity (SIL)" derived from the risk analysis.

Implementing the safety functions

Every safety function always encompasses the complete chain - from the information acquisition through information evaluation up to executing the specific action.

The equipment involved, for example, fail-safe PLCs, sensors and actuators etc. must fulfill, as a total, the determined SIL. If a device is used for various safety functions at the same time, then it must fulfill the highest SIL of the individual functions.

Device characteristics and features

If PLCs are used to process information and data, then these, as "Safety PLC" (SPLC) must fulfill the requirements of the relevant standards (e.g. IEC 61508), corresponding to the specified SIL. Further, they should be certified by an independent testing organization. The essential characteristics and features of fail-safe PLC, that are specified in a graduated scope in the Standards, include:

- In the development, manufacture and service&maintenance, certain measures and techniques must be used, therefore avoiding systematic faults.
- The PLC must be able to control systematic faults that occur in operation.
- The PLC must be able to detect and control random hardware failures in operation.
- Fault control means that when the system detects a fault it must reliably execute the safety function defined for this particular case (e.g. shutdown the plant or system).

Similar requirements also apply for complex field devices. Details on this are described in IEC 61511.

Application

When using a fail-safe PLC, the conditions, defined in the associated safety manual must be carefully complied with and any additional requirements associated with the certificate.

For the peripheral devices to be connected (e.g. sensors and actuators), in addition, the requirements listed in the Standards (IEC 61508 and IEC 61511) must be carefully observed regarding the following aspects:

- Avoiding systematic faults such as, e.g. configuring/engineering, installation and handling faults.
- Detecting and controlling random faults (failures).
- Necessary fault tolerance. This depends on the percentage of the failures that fail in the safe direction.
- Required service & maintenance (repeated tests and checks).

IEC 61511 limits the maximum permissible SIL for which the field devices may be used, depending on their fault tolerance. The fault tolerance, shown in Fig. 1/14 can be reduced by 1, if:

- The devices have been well-proven in operation,
- The devices only allow the setting of process-related parameters, and
- The setting of process-related parameters is protected.

In order to achieve the higher hardware fault tolerance necessary to achieve the SIL level for specific applications, field devices can be redundantly used - as long as the devices are suitable for this SIL as far as their other features and characteristics are concerned.

Test and monitoring functions can be integrated in the PLC in order to detect faults in the peripheral devices (I/O devices). A response that may be required must be performed within a suitably short time.

These time requirements depend on the fault tolerance. The precise requirements are defined in IEC 61511.

When using more complex peripheral devices (e.g. transmitter with microprocessor), it must be ensured that these devices themselves are in compliance with the relevant Standards (EN 61508 and IEC 61511).

The complete basic process control protective system must be configured so that it fulfills the relevant standards for all of the safety-related functions. Regarding functional safety, these are EN 61508 and IEC 61511.

SIL	Minimum hardware fault tolerance if the main failure direction is towards the safe condition
1	0
2	1
3	2

Note: Those failures are designated as “safe” where a safe plant condition is maintained.
Note: A fault tolerance of N means that N+1 faults cause the function to fail.

Fig. 1/14
Maximum permissible SIL for field devices dependent on their fault tolerance (acc. to IEC 61511-1)

Furnace systems in Europe

EU Directives

Furnaces and burners must fulfill the relevant Directives as a result of their application and the devices and equipment which are used (e.g. Machinery Directive, Pressured Equipment Directive (...), Directive for Gas Burners (90/396/EEC)). There are no specific EU Directives for furnace systems. Furnaces are subject, where relevant, to application-specific Directives. Industrial thermo-processing equipment is, for example, classified as machinery under the Machinery Directive.

Standards

Industrial thermo-processing equipment and systems

The European series of standards EN 746-x "Industrial thermo-process systems ...", apply for these types of plants and systems; these Standards are harmonized under the Machinery Directive.

EN 746 can be applied to industrial thermal-processing equipment, for example

- Plants that produce and finish metal,
- Glassworks,
- Ceramic plants,
- Cement, lime and gypsum plants,
- Chemical plants,
- Incinerators etc.

Part 1: "General safety requirements for industrial thermo-process plants" makes reference to EN 60204-1 and EN 954-1 for the implementation of the electrical equipment.

Furnaces

The following is applicable as general standard for furnace systems that do not belong to the industrial thermal-process systems and are not used to heat process fluids and gases in the chemical industry:

- EN 50156 "Electrical equipment for furnaces Part 1: Requirements for application design and installation"

The German Standard DIN VDE 0116 "Electrical equipment for furnace systems". EN 50156 specifies that EN 60204-1 must be complied with. The requirements for safety relevant systems is based on IEC 61508.

The following standards are presently in force for burners

- EN 676 gas burners;
- EN 230 oil vaporization burners in a mono-block design;
- EN 267 oil burners;
- EN 298 automatic furnace systems for gas burners and gas devices with and without blower.

1.3 Legal requirements and standards regarding safety at work in North America

Note: *The following description is intended to provide an overview of the principles and basic requirements. It should not be considered as a complete description of the situation. The reader of this document must, in addition, inform himself about the precise requirements as well as the domestic and local regulations for his particular application.*

An essential difference between the legislation associated with safety at work between North America and Europe is the fact that in the US there is no standard legislation regarding machinery safety that addresses the responsibility of the manufacturer/supplier. There is a general requirement that the employer must provide a safe place of work.

US - general

The Occupational Safety and Health Act (OSHA) from 1970 is responsible in regulating the requirements for employers to ensure safe working conditions. The core requirements of OSHA are listed in Section 5 "Duties":

(a) Each employer -
(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;
(2) shall comply with occupational safety and health standards promulgated under this Act.

The requirements from the OSH Act are administered and managed by the Occupational Safety and Health Administration (also called OSHA). OSHA deploys regional inspectors who check whether workplaces (places of employment) fulfill the applicable regulations.

The regulations, relevant for safety at work of the OSHA are defined and described in OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health"). (CFR: Code of Federal Regulations).

Also refer to www.osha.gov.

The following is stated at the beginning of the regulations for the Safety and Health Program (29 CFR 1900.1):

"(b)(1) What are the employer's basic obligations under the rule? Each employer must set up a safety and health program to manage workplace safety and health to reduce injuries, illnesses and fatalities by systematically achieving compliance with OSHA standards and the General Duty Clause."

And later

"(e) Hazard prevention and control.

(e)(1) What is the employer's basic obligation? The employer's basic obligation is to systematically comply with the hazard prevention and control requirements of the General Duty Clause and OSHA standards.

(e)(2) If it is not possible for the employer to comply immediately, what must the employer do? The employer must develop a plan for coming into compliance as promptly as possible, which includes setting priorities and deadlines and tracking progress in controlling hazards. Note: Any hazard identified by the employer's hazard identification and assessment process that is covered by an OSHA standard or the General Duty Clause must be controlled as required by that standard or that clause, as appropriate."

The application and use of various Standards is regulated in 29 CFR 1910.5 "Applicability of standards." The concept is similar to that in Europe. Product-specific standards have priority over general standards as long as the associated aspects are actually handled there. When the standards are fulfilled, the employer can assume that he has fulfilled the core requirements of the OSH Act regarding the aspects actually handled in the standard.

1910.5 (f) "An employer who is in compliance with any standard in this part shall be deemed to be in compliance with the requirement of section 5(a)(1) of the Act, but only to the extent of the condition, practice, means, method, operation, or process covered by the standard."

Machine safety

Minimum requirements of the OSHA

The OSHA Regulations under 29 CFR 1910 include general requirements for machines and machinery (1910.121) and a series of specific requirements for certain types of machines. The requirements specified are extremely specific but have little technical detail. Excerpt from 29 CFR 1910.212 "General requirements for all machines":

"(a)(1)

Types of guarding. One or more methods of machine guarding shall be provided to protect the operator and other employees in the machine area from hazards such as those created by point of operation, ingoing nip points, rotating parts, flying chips and sparks. Examples of guarding methods are barrier guards, two-hand tripping devices, electronic safety devices, etc." An example of the requirements for the control of presses is the following excerpt from 29 CFR 1910.217 "Mechanical Power Presses":

"(b)(13)

Control reliability. When required by paragraph (c)(5) of this section, the control system shall be constructed so that a failure within the system does not prevent the normal stopping action from being applied to the press when required, but does prevent initiation of a successive stroke until the failure is corrected. The failure shall be detectable by a simple test, or indicated by the control system. This requirement does not apply to those elements of the control system which have no effect on the protection against point of operation injuries."

"(h)(6)(xvii)

Controls with internally stored programs (e.g., mechanical, electro-mechanical, or electronic) shall meet the requirements of paragraph (b)(13) of this section, and shall default to a predetermined safe condition in the event of any single failure within the system. Programmable controllers which meet the requirements for controls with internally stored programs stated above shall be permitted only if all logic elements affecting the safety system and point of operation safety are internally stored and protected in such a manner that they cannot be altered or manipulated by the user to an unsafe condition."

The OSHA regulations define minimum requirements to guarantee safe places of employment. However, they should not prevent employers from applying innovative methods and techniques, e.g. "state of the art" protective systems in order to maximize the safety of employees
(refer to e.g.: www.osha.gov/ ...Standard Interpretations ... 06/05/2001 - Use of Electro Sensitive Protection Equipment ...)

In conjunction with specific applications, OSHA specifies that all electrical equipment used to protect employees, must be certified for the intended application by a nationally recognized testing laboratory (NRTL) authorized by OSHA (refer to e.g.: www.osha.gov/ ...Standard Interpretations ... 08/11/1994 - Presence sensing devices (PSDs) for power presses.: "...OSHA requires that all electrical products used by employees must be treated and approved for their intended use by an OSHA Approved Nationally Recognized Testing Laboratory (NRTL)....").

Application and use of additional standards

In addition to OSHA Regulations, it is just as important to carefully observe the current standards of organizations such as NFPA and ANSI as well as the extensive product liability legislation which is in force in the US. As a result of the product liability, it is in the interest of manufacturers and operating companies to carefully observe and maintain the regulations - and they are more or less forced to fulfill the state-of-the-art technology requirement".

Third-party insurance contracts generally demand that the parties fulfill the applicable standards of the standardization organizations. Companies who are self-insured initially do not have this requirement. However, in the case of an accident, they must prove that they had applied generally recognized safety principles.

NPFA 70 (known as the National Electric Code (NEC)) and NFPA 79 (Electrical Standard for Industrial Machinery) are two especially important standards regarding safety in industry. Both of these describe the basic requirements placed on the features and the implementation of electrical equipment. The National Electric Code (NFPA 70) predominantly applies to buildings, but also to the electrical connections of machines and parts of machines. NFPA 79 applies to machines. This results in a grey area (somewhat undefined) in the demarcation between both standards for large machines and machinery that comprise partial machines. For instance, large conveyor systems can be considered to be part of the building so that NFPA 70 and/or NFPA 79 should be applied.

NFPA 79

This Standard applies to the electrical equipment of industrial machines with rated voltages less than 600 V (a group of machines that operate together in a coordinated fashion is considered as a machine).
The new Edition NFPA 79 - 2002 includes basic requirements for programmable electronics and fieldbuses if these are used to implement safety-related functions. When these requirements are fulfilled, specifically qualified electronic controls and fieldbuses may only be used for Emergency Stop functions, stop Categories 0 and 1 (refer to NFPA 79 - 2002 9.2.5.4.1.4). Contrary to EN 60204-1, NFPA 79 specifies that for Emergency Stop functions the electrical power must be disconnected using electromechanical devices.

The core requirements placed on programmable electronics and buses include:
System requirements
(refer to NFPA 79 - 2002 9.4.3)

- Control systems that contain software-based controllers must,
  (1) if a single fault occurs, bring the system into a safe condition so that it can be shut down
    - prevent restarting until the fault has been removed
    - prevent unexpected starting

  (2) offer protection that is comparable to hard-wired controls

  (3) be implemented to correspond to a recognized Standard that defines the requirements for such systems

  In a Note, it is stated that IEC 61508 is a suitable standard.

Requirements placed on programmable equipment (refer to NFPA 79 - 2002 11.3.4)

- Software and firmware-based controllers that are used in safety-relevant functions must be listed for such an application (i.e. certified by an NRTL).

  In a note, it is stated that IEC 61508 provides requirements for the design of such a controller.

Listing files of electronic devices for safety-related functions

In order to implement the requirements in NFPA 79: 2002, UL has defined a special category for "Programmable Safety Controllers" (code NRGF). This category addresses control devices that contain software and are intended to be used for safety-related functions.

A precise description of the categories as well as the list of the devices that fulfill these requirements is provided in the Internet:

www.ul.com –> certifications directory –> UL Category code / Guide information –> search for category "NRGF"

TUV Rheinland of North America, Inc. is also an NRTL for these applications. The products listed there can also be called-up in the Internet: With the "ID" of the device (Enter TUVdotCOM ID), the description, entered in the listing, can be called from the products listed there. (http://www.tuv.com.

URL: http://www.tuv.com

ANSI B11

The ANSI B11 Standards are consensus Standards, that have been developed by associations - e.g. the Association for Manufacturing Technology (AMT), National Fire Protection Association (NFPA) and the Robotic Industries Association (RIA)for various types of machine tools.

The potential hazards of a particular machine are assessed using the risk analysis. Risk analysis is an important requirement according to NFPA79-2002, ANSI/RIA 15.06 1999, ANSI B11.TR-3 and SEMI S10 (semiconductors). A suitable safety technology/ system can be selected using the documented results of a risk analysis - based on the specified safety class of the particular application.

ANSI B11.TR-4 was approved in 2004 for the application of programmable electronic systems for the safety rated functions of machines covered by the B11 series. This Technical Reference refers to NFPA 79: 2002 and provides guidance for the application of safety PLC technology for the safety rated functions identified by the Risk Analysis.

The current list of ANSI Standards is provided below. This list is intended as a reference and if an authorized revision is to replace these, then the revised Standard applies.

General perspectives

ANSI B11.TR-1 (1993)
Ergonomic Guidelines for the design, installation and use of machine tools

ANSI B11.TR-2 (1997)
Mist control considerations for the design, installation and use of machine tools using metalworking fluids

ANSI B11.TR-3 (2000)
Risk assessment and risk reduction – A guide to estimate, evaluate and reduce risks associated with machine tools

ANSI B11.TR-4
Application of programmable electronic systems for the safety related functions of machines covered by the B11 safety standard series

ANSI Z244.1 (2003)
Control of hazardous energy- Lockout/tagout and alternative methods

ANSI Z535.1 (2002)
Safety Color Code

ANSI Z535.3 (2002)
Criteria for Safety Symbols

ANSI Z535.4 (2002)
Product Safety Signs and Labels

ANSI Z535.5 (2002)
Accident Prevention Tags and Labels

Additional reference standards with special definitions and additional information:

OSHA 29CFR 1910.147
Control of hazardous energy ("lockout/tagout")

IEC 61496 (2003)
Safety of machinery; Electrosensitive protective equipment

Standards for the particular machine type

ANSI B11.1 (2001)
Safety requirements for Mechanical Power Presses

ANSI B11.2 (1995)
Safety requirements for Hydraulic Power Presses

ANSI B11.3 (2002)
Safety requirements for Power Press Brakes

ANSI B11.4 (2003)
Safety requirements for Shears

ANSI B11.5 (2002)
Iron Workers - Safety requirements for construction, care and use

ANSI B11.6 (2001)
Safety Requirements for Manual Tuning Machines

ANSI B11.7 (2000)
Cold Headers and Cold Formers - Safety requirements for construction, care and use

ANSI B11.8 (2001)
Safety requirements for Manual milling and boring Machines

ANSI B11.9 (1997)
Grinding machines - Safety Requirements for Construction Care and Use

ANSI B11.10 (2003)
Metal Sawing Machines - Safety Requirements for Construction Care and Use

ANSI B 11.11 (2001)
Safety Requirements for Gear & Spline Cutting Machines

ANSI B11.12 (1996)
Roll Forming and Roll Bending machines – Safety Requirements for Construction Care and Use

ANSI B11.13 (1998)
Automatic Screw/Bar and Chucking machines- Safety Requirements for Construction Care and Use

ANSI B11.14 (1996)
Coil Slitting Machines - Safety Requirements for Construction Care and Use

ANSI B11.15 (2001)
Safety Requirements for Pipe. Tube and Shape Bending Machines

ANSI B11.17 (1996)
Horizontal Hydraulic Extrusion Presses - Safety Requirements for Construction Care and Use

ANSI B11.18 (1997)
Coil Processing Systems - Safety Requirements for Construction Care and Use

ANSI B11.19 (2003)
Performance Criteria for Safeguarding

ANSI B11.20 (1996)
Manufacturing systems / Cells - Safety Requirements for Construction Care and Use

ANSI B11.21 (1997)
MachineTools Using Lasers - Safety Requirements for Construction Care and Use

ANSI B11.22 (2002)
Safety Requirements for Numerical Controlled Turning Machines

ANSI B11.23 (2002)
Safety Requirements la Machine Centers

ANSI B11.24 (2002)
Safety Requirements for Transfer Machines

Process industry in the US

The basic safety requirements of the OSHA for the process industry are defined in OSHA's Process Safety Management of Highly Hazardous Chemicals, Explosives and Blasting Agents Standard (PSM), 29 CFR 1910.119. (Refer to www.osha.gov).

Excerpt from 29 CFR 1910.119:

Purpose. This section contains requirements for preventing or minimizing the consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals. These releases may result in toxic, fire or explosion hazards.
Section (d) with its sub-sections contain the basic requirements placed on process instrumentation.

1910.119(d)
Process safety information. ... the employer shall complete a compilation of written process safety information ... This process safety information shall include information pertaining to the hazards of the highly hazardous chemicals used or produced by the process, information pertaining to the technology of the process, and information pertaining to the equipment in the process.

1910.119(d)(3)
Information pertaining to the equipment in the process.

1910.119(d)(3)(i)(F)
Design codes and standards employed;

1910.119(d)(3)(ii)
The employer shall document that equipment complies with recognized and generally accepted good engineering practices.

OSHA provides guidelines on this with: CPL 2-2.45A "Process Safety Management of Highly Hazardous Chemicals-Compliance Guidelines and Enforcement Procedures.

OSHA specifies that the process instrumentation must be implemented in accordance with generally accepted "good engineering practice." With a letter, dated March 2000, OSHA clarified an inquiry from ISA, that ANSI/ISA 84.01 is a standard that is applicable nationwide and which OSHA recognizes as generally accepted "good engineering practice." However, in the same letter, OSHA clearly stated that ISA 84.01 is not the only standard which is considered when fulfilling the requirements of 1910.119 (PSM).

CFR 1910.119 doesn't clearly state whether the requirements refer to the complete instrumentation. Two types of instrumentation are generally used in the process industry. "Safety Instrumented Systems" (SIS) and "Basic Process Control System" (BPCS). ANSI/ISA 91.01 defines that only the SIS is to be handled under the OSHA regulations.

IEC 61511 "Functional safety: Safety Instrumented Systems for the process industry sector" is the IEC standard with the same scope as ISA 84.01. It was developed, with significant involvement of the ISA and is to be included in the new Edition of the ISA 84.

A large proportion of processes falls within the scope of ISA 84.01, but does not formally fall under 29 CFR 1910.119 (PSM). Also in this case, the Standard should be applied in order not to violate the basic requirements of the "Duties" section of the Occupational Safety and Health Act (OSHA).

Safety Regulations and Standards in Canada

Canada Labour Code is the law for all industries in Canada. Part 2 of the Canada Labor Law governs Occupational Health and Safety in the workplace. Under the Canadian constitution, labour legislation is primarily a provincial responsibility. The Occupational Health and Safety Act (OHSA) sets out the rights and duties of all parties in the workplace. Its main purpose is to protect workers against health and safety hazards on the job. The OHSA establishes procedures for handling risks at the workplace and it provides for enforcement of the law where compliance has not been achieved voluntarily. Regulations issued under the OSHA identify specific requirements that must be complied with, set standards that must be met and prescribe procedures that must be followed to reduce the risk of accidents at work.

Officials appointed by the federal, provincial and territorial governments have the power to inspect workplaces and enforce the law by use of all enforcement tools necessary, including stop work orders, fines and prosecutions directed at the employers and workers. These are for example Ministry of Labor (MoL) in Ontario or the Commission de la santé et de la sécurité du travail (CSST) in Quebec. The officials work closely with its agencies, safe workplace associations (SWAs), worker training centers and clinics and the Canadian Center for Health and Safety. Some of these key organizations include Industrial Accident Prevention Association (IAPA) in Ontario and The Institut de Reherche Robert-Sauvé en Santé et en Sécurité du Travail (IRSST) in Quebec. Insurance Boards are also the key element in workplace safety. For example, The Workplace Safety and Insurance Board (WSIB) oversees Ontario's workplace safety education and training system, provides disability benefits by administering safety insurance program, monitors the quality of health care through financial interventions etc.

Government of Canada, Occupational Health and Safety in Canada (www.hrsdc.gc.ca)

Ministry of Labour(www.gov.on.ca/lab/)

Commission de la santé et de la sécurité du travail (www.csst.qc.ca)

Industrial Accident Prevention Association (www.iapa.on.ca)

The Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (www.irsst.qc.ca)

Workplace Safety and Insurance Board (www.wsib.on.ca)

The Regulation for Industrial Establishments under OHSA in Ontario, Regulation 528/00 Section 7 (PSHSR - Pre Start Health and Safety Review) has been in effect since the 7th of October 2000. The 2nd item in the table is specific to machinery safety. The employer is responsible for ensuring that all requirements of the OHSA and the regulations are complied with in the workplace. The regulation is, to a large extent, a performance-based standard. This means that the regulation defines what level of protection is to be provided and the objective to be achieved, but does not state how to achieve the required level of protection.

Section 7 or Reg. 528/00 refers to current applicable standards in Canada. In order to fully comply with the requirements of Section 7, it is necessary to refer to other recognized applicable codes and standards, such as the Ontario Fire Code, the National Fire Code, NFPA codes and standards, CSA codes and standards, ANSI standards etc. The table shown summarizes the applicable standards specific to the machine safety circumstances listed to support compliance with Section 7 of the Regulation.

"Guidelines for Pre-Start Health and Safety Reviews, April 2001, Ministry of Labour

Applicable provisions of the regulations	Circumstances	Ontario Codes	Generic Codes ('A' & 'B')	Machine-specific standards'C'
Sections 24, 25, 26, 28, 31 and 32	Applies when any of the following are used as protective elements in conjunction with an apparatus: 1. Safeguarding devices that signal the apparatus to stop, including but not limited to safety light curtains and screens, area scanning safeguarding systems, radio frequency systems, two-hand control systems, two-hand tripping systems and single or multiple beam systems 2. Barrier guards that use interlocking mechanical or electrical safeguarding devices	Ontario Electrical Safety Code	CSA-Z432* ANSI B11.19 ISO 14121 ISO 12100 Parts 1&2 ISO 13851 ISO 13852 ISO 13853 ISO 13854 ISO 13855 ISO 13856 ISO 14119 ISO 14120 IEC 61496 Parts 1,2,3 ISO 4413 ISO 4414	CSA Z142* CSA Z434* CSA Z615i ANSI B11.1* ANSI B11.2 ANSI B11.3 ANSI B11.6 ANSI B11.8 ANSI B11.10 ANSI B11.20 ANSI B11.21 ANSI B65.1 ANSI B65.2 ANSI B65.5 ANSI 15.06 ANSI B151.1 ANSI Z245.1 +MOL Guide ANSI Z245.2 ANSI Z245.5

* Latest revision is applicable

A & B standards are generic safety standards that give basic concepts and principles for design and general aspects, or deal with one safety aspect or one type of safety related device that can be applied to machines/ processes.

C standards are safety standards that deal with detailed safety requirements for a particular machine or process.

The following are the **key machine safety standards in Canada** that accept the use of safety-related software and firmware-based controllers under their latest revisions:

- CSA Z432-04 "Safeguarding of Machinery" accepts the use of programmable safety under Section 8.3.
  This Standard applies to the protection of persons from the hazards arising from the use of mobile or stationary machinery.
  It provides the criteria to be observed and the description, selection and application of guards and safety devices. Where a CSA Standard exists for a specific type of machinery, it is to be used in conjunction with this Standard to provide the most effective protection to the particular situation.

- CSA Z434-03 "Industrial Robots and Robot Systems-General Safety Requirements" accepts the use of programmable safety under Section 6.5.
  The purpose of this Standard is to provide requirements for industrial robot manufacture, remanufacture, and rebuild; robot system integration/

installation and safeguarding methods to enhance the safety of personnel associated with the use of robots and robot systems.

- CSA Z142-02 "Code for Power Press Operation:
  Health, Safety and Guarding Requirements" accepts the use of a programmable safety under Section 8.1.3.
  This Standard covers the occupational health and safety requirements for all classes of power presses that are fitted with a ram (plunger or slide) and dies for the purpose of blanking, cutting, trimming, drawing, punching, forming (bending), stamping, assem bling, or processing metal and other materials.

- NFPA 79 2002 "Electrical Standard for Industrial Machines" accepts the use of programmable safety under Section 9.4.3. and Section 11.3.4.
  This standard provides detailed information about the the application of electrical/electronic equipment, apparatus, or systems supplied as part of industrial machines that will promote safety to life and property. The provisions of this Standard apply to the electrical/electronic equipment, apparatus, or systems of industrial machines, operating from a nominal voltage of 600 volts or less, and commencing at the point of connection of the supply to the electrical equipment of the machine.

The CSA safety standards require safety-related software and firmware-based controllers to be certified by Nationally Recognized Testing Laboratory (NRTL) or Standards Council of Canada (SCC)-accredited testing laboratory to an approved standard applicable for safety devices.

Safety Negligence is a Criminal Offense

- Bill C-45 is a new Act under the Criminal Code, enforceable effective March 31, 2004.

- Canadian Labour Code imposes a legal duty, under the Criminal Code, on employers and those who direct work to take reasonable measures to protect worker and public safety.

- An organization can now be charged with criminal negligence concerning health & safety and therefore be investigated and; charged under both the Occupational Health and Safety Act and the Criminal Code.

- Bill C-45 increases the maximum fine for a summary conviction offense from $25,000 to $100,000.
  And there is no limit on the fine for more serious offenses.

- The maximum penalty for an individual convicted of criminal negligence is life imprisonment.

Government of Canada, Occupational and Health Safety in Canada (www.hrsdc.gc.ca)

Government acts to increase enforcement of workplace health and safety

The addition of 200 new Health and Safety Inspectors in Ontario was announced by the government on the 8th of July 2004. This measure targets workplaces with poor health and safety records. The government's goal is to reduce workplace injuries by 20% in four years. Based on the average cost of a workplace injury, eliminating 60,000 injuries annually will also translate into savings for businesses of up to $960 million per year. Recruitment of 100 new inspectors began immediately, marking a major expansion of the current force of 230 inspectors. Inspectors will initially target 6000 workplaces with the highest injury rates.

04-78, July 8, 2004, Ministry of Labour (www.gov.on.ca/lab/)

1.4 Safety requirements for machines in Japan

For applications in Japan

The situation in Japan was previously different than in Europe and the US. Contrary to Europe and the US, where the employer is responsible for safety at the workplace, in Japan, the employee must take every precaution that nothing happens to him/her. This is the reason that he may only use appropriately trained personnel on a machine.

Comparable, legal requirements regarding functional safety - as in Europe - therefore do not exist. Further, product liability does not play such a role as in the US. However, in the meantime, it has been recognized that today, this concept is no longer adequate. In Japan, a transition is being made over to the basic principle that applies in both Europe and the US.

There is no legal requirement to apply standards. However, an administrative recommendation to apply JIS (Japanese Industrial Standards) exists:
Japan bases its standards on the European concept and has included basic standards as national standards (refer to the Table)

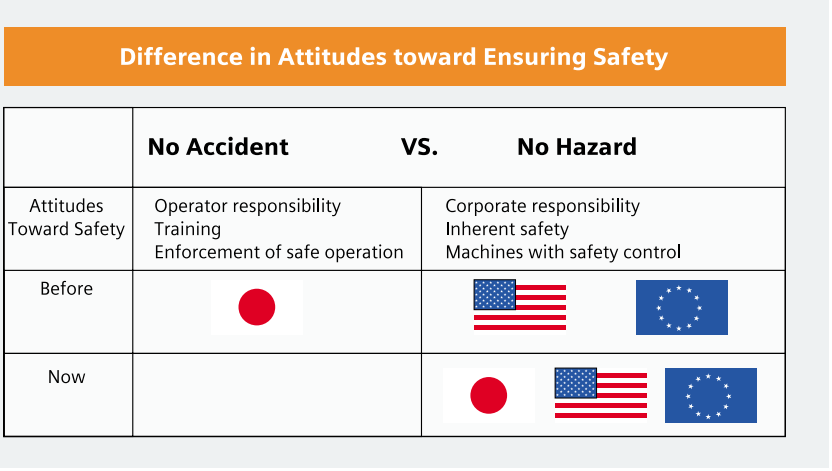


Fig. 1/15
Change in the concept of the responsibility for the safety of machinery in Japan (from: Toshihiro Fujita et.al.: "NECA Activities for Meeting Globalized Standards and Certification", Robot, Japan Robot Association, March 2004)

ISO/IEC number	JIS number	Note
ISO12100-1	JIS B 9700-1	earlier designation TR B 0008
ISO12100-2	JIS B 9700-2	earlier designation TR B 0009
ISO14121 (EN1050)	JIS B 9702	
ISO13849-1 (Ed. 1)	JIS B 9705-1	
ISO13849-2 (Ed. 2)	JIS B 9705-1	
IEC60204-1	JIS B 9960-1	without Annex F or Route Map of the European foreword
IEC1508-1 to 7	JIS C 0508	
IEC 62061		A JIS number has still not been allocated

For machinery OEMs and users operating worldwide

Japanese machinery construction OEMs that export their machines must be compliant with European and US legislation so that their products fulfill the requirements of the target markets. Companies with globally distributed production facilities also align themselves to the European and American requirements in order to have, as far as possible, standard safety concepts in all of their plants.

1.5 Important Addresses

Europe

1. CEN Members = sources for the domestic editions of EN + prEN

AENOR
Asociación Española de Normalización y Certificación (AENOR)
Génova, 6
E-28004 Madrid

Phone: + 34 91 432 60 00
Telefax: + 34 91 310 31 72
E-mail: dzc@aenor.es

AFNOR

Association Française de Normalisation
11, Avenue Francis de PressenséF-93571 Saint-Denis La Plaine Cedex

Phone: + 33 1 41 62 80 00
Telefax: + 33 14 917 90 00

BSI

British Standards Institution
389 Chiswick High Road
GB-London W4 4AL

Phone: + 44 208 996 90 00
Telefax: + 44 208 996 74 00

E-mail: first name_surname@bsi-global.com
E-mail: info@bsi-global.com

COSMIT

Czech Standards Institute
Biskupsky dvùr 5
CZ-110 02 Praha 1

Phone: +420 2 218 02 111
Telefax: +420 2 218 02 301
E-mail : info@csni.cz

DIN

Deutsches Institut für Normung e.V.
Burggrafenstr. 6
D-10787 Berlin

Phone: + 49 30 26 01 0
Telefax: + 49 30 26 01 12 31
E-mail: postmaster@din.de

DS

Dansk Standard
Kollegievej 6
DK-2920 Charlottenlund

Phone: + 45 39 96 61 01
Telefax: + 45 39 96 61 02
E-mail: dansk.standard@ds.dk

ELOT

Hellenic Organization
for Standardization
313, Acharnon Street
GR-11145 Athens

Phone: + 30 1 212 01 00
TX: (0601) 219670 elot gr
Telefax: + 30 1 228 62 19
E-mail: info@elot.gr

IBN/BIN

Institut Belge de Normalisation/
Belgisch Instituut voor Normalisatie
Avenue de la Brabançonne 29/
Brabançonnelaan 29
B-1000 Bruxelles/Brussel

Phone: + 32 2 738 01 11
Telefax: + 32 2 733 42 64
E-mail: info@ibn.be

IPQ

Instituto Português da Qualidade
Rua António Gião, 2
P-2829-513 Caparica

Phone: + 351 21 294 81 00
Telefax: + 351 21 294 81 01
E-mail: ipq@mail.ipq.pt

NEN

Nederlands Normalisatie-Instituut
Kalfjeslaan
Postbus 5059
NL-2600 GB Delft

Phone: + 3115690390
Telefax: + 3115690190
E-mail: info@nen.nl

NSAI

National Standards Authority of Ireland
Glasnevin
IRL-Dublin 9

Phone: + 353 1 807 38 00
Telefax: + 353 1 807 38 38
E-mail: nsai@nsai.ie

NSF

Norges Standardiseringsforbund
PO Box 353 Skøyen
N-0213 Oslo

Phone: + 47 22 04 92 00
Telefax: + 47 22 04 92 11
E-mail: info@standard.no

ON

Österreichisches Normungsinstitut
Postfach 130
Heinestraße 38
A-1020 Wien

Phone: + 43 1 213 00
Telefax: + 43 1 213 00 818
E-mail : office@on-norm.at

SEE

Service de L'Energie de l'Etat
Organisme Luxembourgeois
de Normalisation
B.P. 10
L-2010 Luxembourg

Phone: + 352 46 97 46 1
Telefax:+ 352 22 25 24
E-mail: see.normalisation@eg.etat.lu

SFS

Suomen Standardisoimisliitto r.y.
PO Box 116
FIN-00240 Helsinki
Finland

Phone: + 358 9 149 93 31
Telefax: + 358 9 146 49 25
E-mail: sfs@sfs.fi

SIS

Standardiseringen i Sverige
Box 6455
S-113 81 Stockholm

Phone: + 46 8 610 30 00
Telefax: + 46 8 30 77 57
E-mail: info@sis.se

SNV

Schweizerische Normen-Vereinigung
Bürglistraße 29
CH-8400 Winterthur

Phone: + 41 52 224 54 54
TX: (045) 755931 snv ch
Telefax: + 41 52 224 54 74
E-mail: info@snv.ch

STRI

Icelandic Council for Standardization
Laugavegur 178
IS-105 Reykjavik

Phone: + 354 520 71 50
Telefax: + 354 520 71 71
E-mail: stri@stri.is

UNI

Ente Nazionale Italiano di Unificazione
Via Battistotti Sassi, 11b
I-20133 Milano MI

Phone: + 39 02 70 02 41
Telefax: + 39 02 70 10 61 06
E-mail: uni@uni.com

CEN

European Comittee for
StandardizationRue de Stassrt 36
B-1050 Bruxelles

Phone: + 3225500811
Telefax: + 3225500819
E-mail: infodesk@cenorm.be

CENELEC

European Comittee for
Electrotechnical Standardization
Rue de Stassrt 35
B-1050 Bruxelles

Phone: + 3225196871
Telefax: + 3225196919
E-mail: info@cenelec.org

2. DIN – Deutsches Institut für Normung e.V., important Standards committees with reference to machines

NAM

Normenausschuss Maschinenbau
(NAM)im DIN
Lyoner Str. 8
Postfach 710864
60498 Frankfurt/M.

Phone: 069/6603-1341
Telefax: 069/6603-1557

NWM

Normenausschuss Werkzeugmaschinen
Corneliusstraße 4
60325 Frankfurt

Phone: 069/75608123
Telefax: 069/75608111

AGSA, FNErg, FNFW, FNL, NAL, NALS, NAS, Nasg, NI, NKT, NMP, Textilnorm

DIN Deutsches Institut für Normung e.V.
10772 Berlin

Phone: 030/2601-0
Telefax: 030/2601-1260

FNCA, FNKä, FWS, Naa, NAD, NL, NÖG, NRK, NÜA

DIN Deutsches Institut für Normung e.V.
Zweigstelle Köln
Kamekestraße 8
50672 Köln

Phone: 0221/5713-0
Telefax: 0221/5713-414

NA EBM

Normenausschuss Eisen-, Blech- und Metallwaren
Kaiserwerther Str. 137
40474 Düsseldorf

Phone: 0211/4564274/276
Telefax: 0211/4564277

NA FuO

Normenausschuss Feinmechanik und Optik
Turnplatz 2
75172 Pforzheim

Phone: 07231/918822
Telefax: 07231/918833

FAKAU

Normenausschuss Kautschuktechnik
Zeppelinstr. 69
Postfach 900360
60487 Frankfurt/M.

Phone: 069/7936-0/117
Telefax: 069/7936165

DKE

Deutsche Kommission Elektrotechnik Elektronik
Informationstechnik im DIN und VDE
Stresemannallee 15
60596 Frankfurt/M.

Phone: 069/6308-0
Telefax: 069/9632925
E-mail: dke@vde.com

3. Sources for technical regulations in Germany

For EC Directives as well as legislation and regulations

Bundesanzeiger-Verlags GmbH
Amsterdamer Straße 192
50667 Köln

Phone: (0221) 97668-0
Telefax: (0221)

For DIN Standards and VDM Sheets

Beuth Verlag GmbH
Burggrafenstraße 6
10787 Berlin

Phone: (030) 2601-0
Telefax: (030) 2601-1260

For VDE Regulations as well as DKE and IEC Standards

VDE-Verlag GmbH
Bismarckstraße 33
10625 Berlin

Phone: (030) 348001-16
Telefax: (030) 3417093

For accident prevention regulations and ZH-1 documents from the Trade Associations

Carl Heymanns Verlag KG
Luxemburger Straße 449
50939 Köln

Phone: (0221) 94373-0
Telefax: (0221) 94373-901

Information about Standards, Regulations, Directives

Deutsches Informationszentrum für Technische Regeln (DITR) im DIN (Deutsches Institut für Normung)
Burggrafenstraße 6
10787 Berlin

Phone: (030) 2601-0
Telefax: (030) 2628125

America

Additional information about machine safety

ANSI
(American National Standards Institute)
http://www.ansi.org

OSHA
(Occupational Safety and Health Administration)
http://www.osha.gov

NFPA
(National Fire Protection Association)
http://www.nfpa.org

TUV
Rheinland of N.A. Inc.
http://www.us.tuv.com

UL
(Underwriter Laboratories)
http://www.ul.com

CSA
(Canadian Standards Association)
http://www.csa.ca

CCOHS
(Canadian Center for Occupational - Health and Safety)
http://www.ccohs.ca

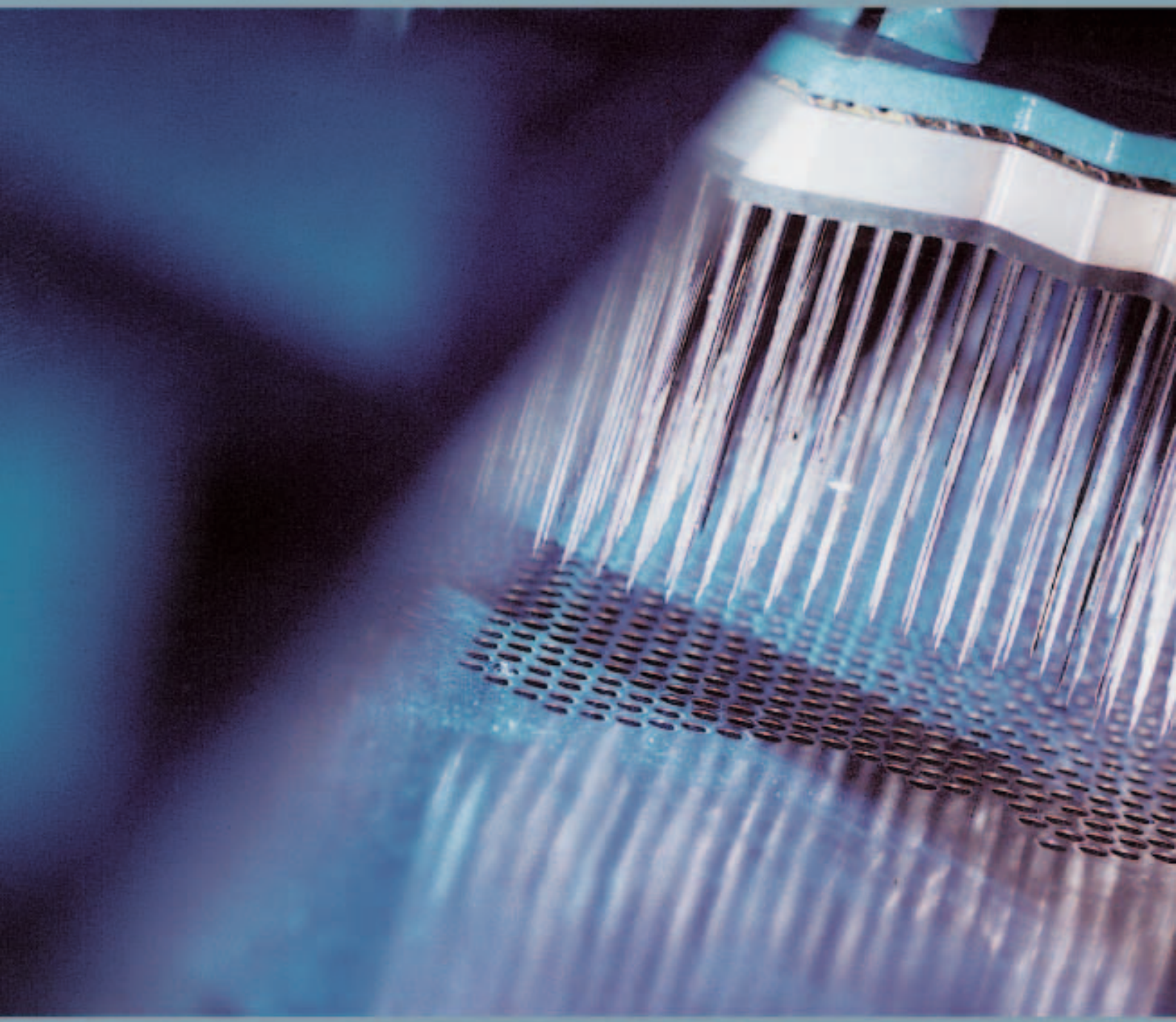
NIOSH
(National Institute of Occupational Health and Safety)
http://www.cdc.gov/niosh/homepage.html

NSC
(National Safety Council)
http://www.nsc.org

ASSE
(American Society of Safety Engineers)
http://www.asse.org

RIA
(Robotic Industries Association)
http://www.robotics.org

Global Engineering Documents
http://www.global.his.com



2

Specification and design of safety-relevant controls for machines

2 Specification and design of safety-relevant controls for machines

2.1 Overview

The structure of the following description is based on the lifecycle model, i.e. the sequence of the individual sections is oriented to the sequence in which the individual machine and plant engineering phases are normally carried-out.

Safety requires protection against a wide variety of hazards and dangers. The functional safety is discussed in the following. This is part of the safety of a machine or plant that depends on the correct function of its control or protective devices. Questions regarding hazards as a result of other risks, e.g. electricity, heat, radiation etc. are not discussed. This also applies to the economic aspects.

This description is based on the presently valid safety requirements in Europe. However, if they have already been identified, changes and revisions to be expected have been taken into account. Where relevant, deviating requirements for applications outside Europe are also addressed.

As a result of the different regulations and standards, machines and process equipment are considered separately - even if the basic principles, with which safety is to be achieved, are the same.

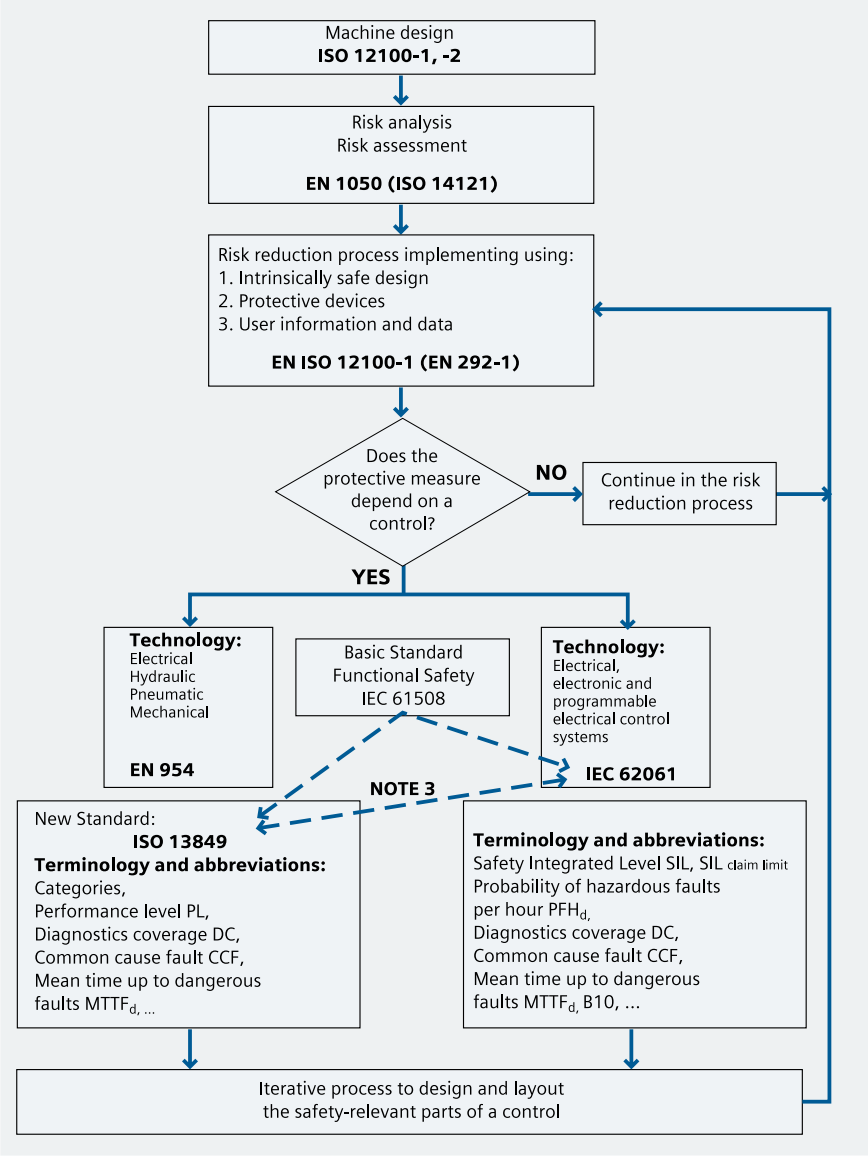


Fig. 2/1
Design process of a machine Note 3: For non-electrical systems: Use the parts that correspond to EN ISO 13849-1 (rev) as subsystems

[1] The term "Machine" includes, in the following, also combinations of machines, i.e. "integrated production systems".

2.2 Design and implementation process of the machine, risk assessment, process to reduce risks

The lifecycle of a machine is roughly subdivided into the sections shown in 2/1. The individual phases encompass clearly defined tasks so that specific steps can be executed by different persons or organizations.

One strategy to reduce the risk of a machine is described in ISO 12100-1 Chapter 5. This clearly states the priority that must be allocated to the various aspects of the machine design.

When carrying-out this process, it is necessary to take into account the following sequence:

- Safety of the machine over its complete lifecycle
- The ability of a machine to execute its functions
- User-friendliness of the machine
- Manufacturing, operating and disassembly costs of the machine

The process of reducing risks of a particular machine is realized in an iterative process. The individual steps are described in EN 1050 (also refer to Chapter 1 of this Manual). The process of reducing risks encompasses the risk assessment and, where necessary, determining the measures to reduce risks.

Basic technical principles are described in ISO 12100-2. These help mechanical engineers when designing machinery to construct a safe machine. The first and foremost objective is to achieve inherent safety of the machine. Only then should appropriate measures (e.g. guards) be provided to address remaining hazards and dangers (refer to ISO 12100-2 Chapter 4). The suitable implementation of safety-related control functions is an essential element in achieving inherent safety (refer to ISO 12100-2 Section 4.11). Reference is made to IEC 61508 for controls that contain programmable electronic components.

There are C Standards for many machine types. These already define the necessary measures to reduce the level of risk. They define the protective measures required with the associated Safety Performance - i.e. the required

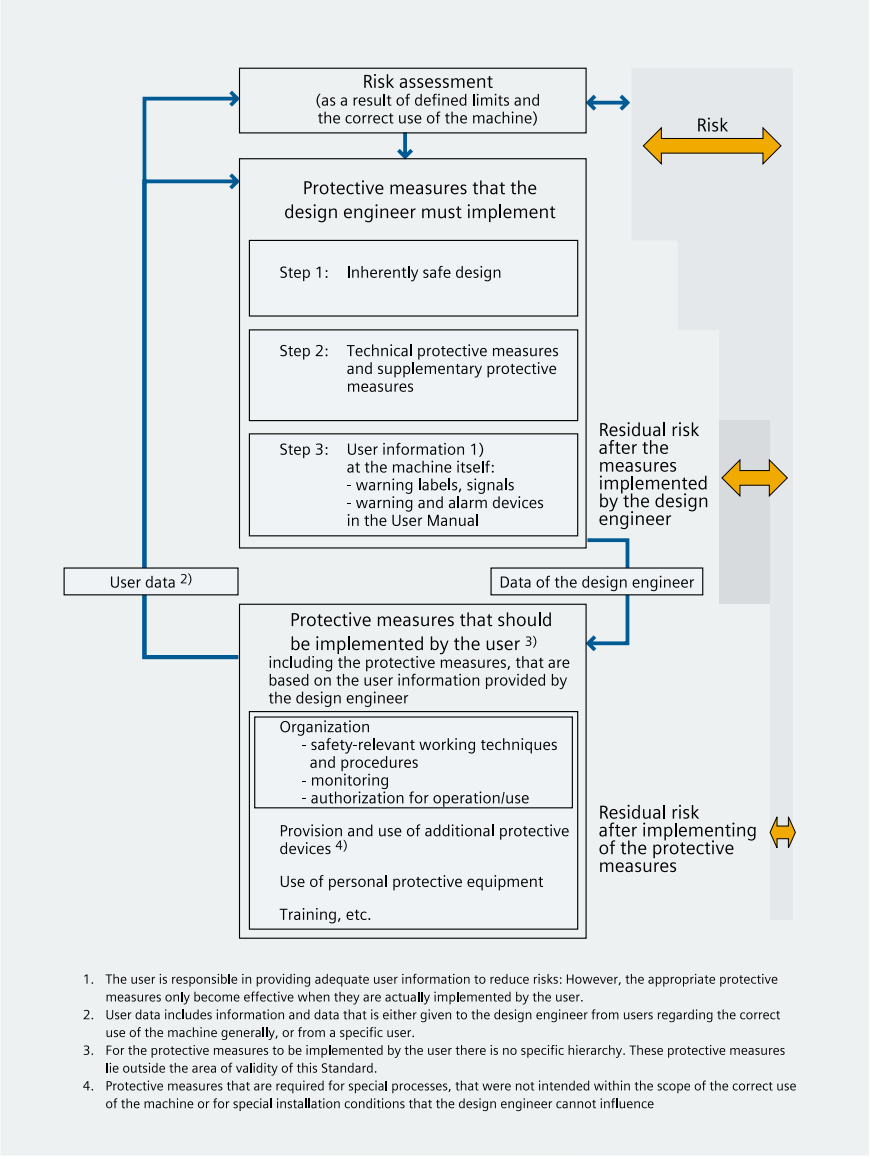


Fig. 2/2
Process to reduce risk

categories for the safety-related parts of controls.

In order to take into account technical development, or if there is no applicable C Standard, in many cases, when mechanically designing a machine, this process must be repeated. The risk reducing measures to be implemented should then be defined taking into account current state-of-the-art technology.

By specifying the safety requirements, the machine design engineer defines the requirements placed on the control and the protective equipment and devices. This specification includes a precise description of the individual safety functions and their required Safety Performance.

Defining measures necessary to reduce risk

For many machine times, there are specific C standards in which the necessary protective measures are already defined. The machinery manufacturer can apply these Standards if they apply for the machine being considered and he can then assume (refer to Chapter 1 “Presumption of conformance”) that the safety goals of the EU Machinery Directive are fulfilled.
In this case, the necessary Categories according to EN 954 should be specified for the safety-related control functions.

If the intended technical implementation of the machine considered corresponds to the information in the C Standard, then the risk analysis steps, described in the following, do not have to be repeated. The safety functions and their Safety Performance, i.e. the required Category, are specified by the C Standard.
If complex electronic equipment - e.g. safety PLC controllers - are used to implement safety functions, then the specified category cannot be directly applied.
The requirements associated with the Categories of EN 954 are, alone, not sufficient. Programmable controls for safety tasks must be in compliance with IEC 61508. In order to fulfill protective goals associated with a specific category, the programmable control must achieve the assigned SIL according to Fig. 2/3.

If the machine design deviates from the specifications listed in the C Standard, for example, in order to utilize new functionality of electronic safety controls or safety-related drive functions, a risk analysis must be carried-out, and the appropriate Safety Performance (footnote 2) must be determined for the new technology.

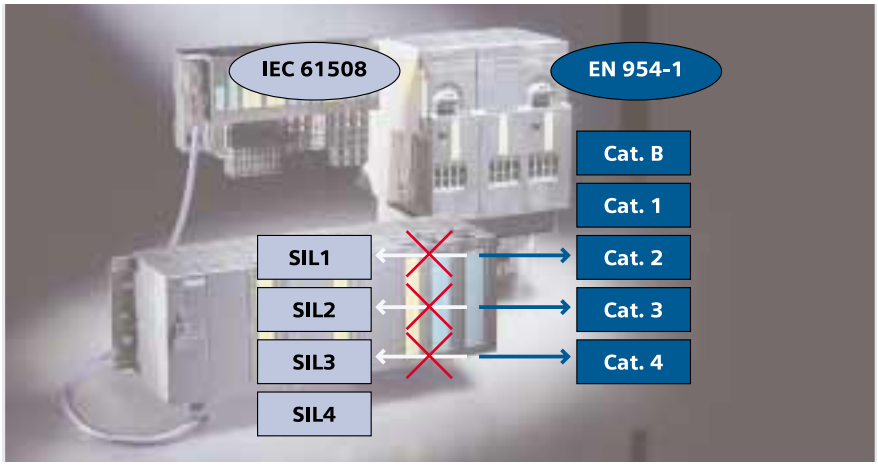


Fig. 2/3
SIL necessary to fulfill specific categories

Defining the limits of a machine

The machine design starts with the definition of its limits. These include:

- Limits of use:
  This is the definition of correct use including the various operating types, phases of use and different intervention-possibilities for the user, as well as sensible, predictable incorrect use.

- Spatial limits:
  (e.g., space for motion, space requirement for installation and maintenance, "operator/machine" and "machine/power feed" interfaces)

- Ambient/environmental limits:
  Limit values for ambient conditions, e.g. temperature, humidity

- Time limits:
  Defining the predictable "lifetime limit" of the machine, taking into account its - correct use and/or several of its parts (e.g.tool, parts subject to wear, electronic components).

Identification of possible hazards

After the limits of the machine being considered have been defined, all of the possible hazards that can arise from this machine are identified. (Chapter 4 of ISO 12100-1 includes a list of possible hazards to be considered.)

When identifying possible hazards, it should also be investigated as to whether functional faults or failures relating to the control, control devices or existing protective equipment, can result in hazards. Possible incorrect behavior (e.g. the control generates an on signal although an off signal is output and should be kept) should be analyzed regarding its effect on the machine and its protective devices and equipment. In this case, it does not have to be investigated as to which "internal causes" in the equipment being considered, can result in an incorrect function.

For every possible functional fault it should be investigated as to which hazards could possibly be generated. For instance, it should be checked,

- Whether any fault or a combination of faults in the control can result in a dangerous (incorrect) function of the machine (e.g. accidental starting)

- Whether, when using variable-speed drives, if the actual speed deviates from the setpoint speed, a hazard is generated.

- Whether the failure of an operator-command (e.g. stop command can result in a hazard

To start, for the risk analysis, the "worst case" investigation is used as basis. This means that it must be assumed that functional faults can occur. If this analysis indicates that a functional fault can cause a hazard, then this function is safety-related and a risk assessment must be made. Depending on the result of this risk assessment, measures to reduce the risk are required.

[2] The term "Safety Performance" is used here as a higher-level term for safety-relevant performance of the control. It encompasses the "Category", "Safety Integrity" and "Performance Level" terms used in the various Standards.

Fig. 2/4
Elements of risk evaluation

Risk assessment and risk evaluation

Also refer to EN 1050 Chapters 7 and 8.

For all of the previously identified hazards, the associated risks must be evaluated. If the risk of a specific hazard exceeds a tolerable level, then measures must be applied to reduce this risk.

Note: The result of the evaluation should be documented for each individual hazard.

A risk is created by the interaction of various causes (refer to Fig. 2/4).

- Severity of the possible damage
- Frequency with which somebody stays in the hazardous area
- Probability that the dangerous event actually occurs
- Possibility of avoiding or reducing the damage

Its magnitude can be estimated by evaluating these elements.

Risk reduction

If the estimated risk appears too high, then it must be reduced. To start, an attempt must be made to achieve this by modifying the mechanical design of the machine to make it safe (refer to the Machinery Directive, Appendix I (1) 1.1.2 and ISO 12100-1 Chapter 5.4). If this is not possible, then the risk must be minimized by using suitable protective measures.

- The severity of possible damage can, for example, be reduced by reducing the speed of motion or forces of machine-parts while personnel are present.

- Using guards and similar devices, it is possible to reduce the frequency with which personnel are in the hazardous zone.

- There is always a certain probability that a machine does not behave as it should (i.e. for which it was originally designed) or protective devices fail. This can be caused by faults in any parts of the machine. This risk factor can be reduced by suitably designing and implementing the safety-related parts and components.
  The control of the machine also belongs to the safety-relevant parts if, due to its failure, a hazard can occur. The risk that is caused by a control fault can be reduced by implementing the control acc. to IEC 62061.

- The possibility that damage can be avoided, can be increased, among other things, if the-hazardous states are identified early on, e.g. using signal lamps.

The probability of the occurrence of an undesirable event is a common parameter of all of these elements. The risk can be reduced by reducing this probability (refer to Fig. 2/5).

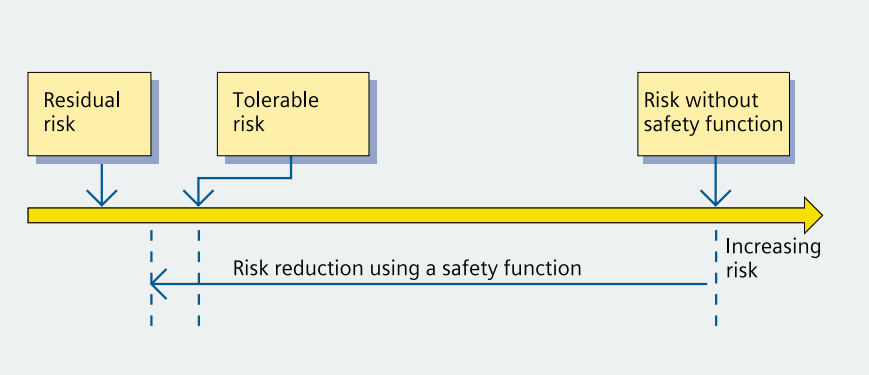


Fig. 2/5
Reducing risks

Measures regarding risk reduction

The risk assessment concept is oriented to the possible hazards. It specifies that for each identified hazard, suitable measures must be applied to remove it. Or, if this is not possible, then the probability that it occurs, must be adequately reduced.

Safety-related control functions

If the risk assessment indicated that a hazard is generated by a possible functional fault of the control, this risk can be reduced by appropriately reducing the probability of dangerous control faults.

Situations such as this are, for example, present if a machine is stopped so that service or setting-up work can be carried-out or the speed of the machine is reduce so that personnel can safety work at the machine. In this case, a hazard can occur if the machine was to unexpectedly start or suddenly accelerate - e.g. due to a control fault.

If the range of motion is limited for specific activities to protect the operator, then if this limit fails, it can result in a hazard.

The probability of failure of this function must therefore be sufficiently low in order to limit the risk to a tolerable level.

Example (1) safety-related control function

Machine with several moving parts (axes). There is a danger of injury due to the movement of each of these parts. The operator must enter the hazardous zone in order to carry-out repair and service work, but the machine should not be completely shut down as otherwise the product is (could be) damaged.

During repair, in order to protect the operator and the product, the speed of motion is limited to a non-dangerous level or specific parts of the machines are kept in a defined position. When velocity limits and positions are to be maintained, then this represents a safety-related function. If the associated control function would fail, this would result in a potential hazard for the operator (e.g. as a result of unexpected acceleration, crushing etc. when leaving the position).

In this particular case, the safety function is: “Limiting the speed of specific machine parts and maintaining the selected position of certain machine parts. If a limit value is exceeded, e.g., due to a fault, then the drive involved should be shut down and a mechanical brake applied.”

A risk evaluation must be carried-out for this situation in order to determine the necessary Safety Performance of the safety function.

Guards

If the risk assessment has indicated that guards are required then these must be implemented so that it is adequately improbable that they fail. Such protective devices (e.g. guards) must be monitored at all access positions so that when the machine is powered-up, personnel cannot access the hazardous zone. In addition to this measure, which restricts the access of personnel, it may also be necessary to limit the range of motion of machines or emissions (e.g. metal chips). The zone in which personnel can be present (refer to Fig. 2/6) must be protected, for example, by preventing that parts of the machine can extend or move into this particular zone.

Example (2) safety-related protective locking-out

In the productive phase, it is not permissible that personnel can be in the machine operating zone (production cell). This is because there is a high danger of injury due to the fast and in some cases unexpected motion of the machine. This is the reason that the machine may only run in productive operation if it is ensured that nobody can enter into the hazardous range by locking-out and interlocking all of the access possibilities.

In this case, the safety function is as follows: "During productive operation, all access points to the machine working area (production cell) are interlocked. If a fault is detected, e.g. in an interlocking function, where inadmissible access to the machine can no longer be completely excluded, then the machine must be stopped."

A risk assessment must be made for this situation in order to determine the necessary Safety Performance of the safety function.

Safety-related control functions are defined to remove or reduce the risk of each identified hazard. In order that these functions achieve the required level of risk reduction, they must have an appropriate Safety Performance. The necessary Safety Performance of each and every function must be determined for the hazard to be removed.

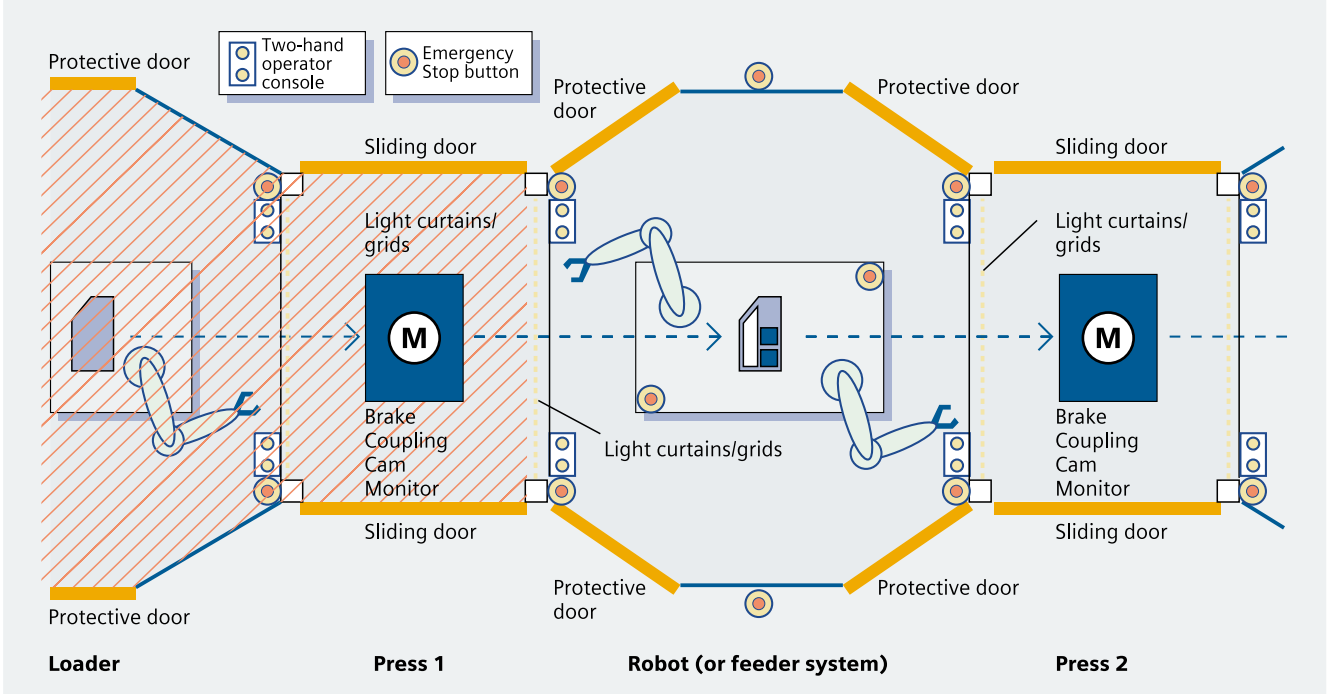


Fig. 2/6
Hazardous zones of an integrated machine

2.3 Does the protective measure depend on the control?

Risk elements according to EN 1050 (ISO 14121)

The assessment according to EN 1050 allows the risk to be assessed using four risk elements:

- Severity of the possible damage
- Frequency with which personnel stay in the hazardous zone
- Probability that a dangerous event occurs
- Possibility of avoiding or reducing damage

In turn, these risk elements form the input parameters to implement a safety-related control function: They permit a risk to be allocated to the requirements of the safety-related control.

This is the reason that EN 954-1 - i.e. also IEC 62061 - offer a technique to evaluate the risk elements and to classify the Safety Performance.

Determining the necessary Safety Performance (Safety Integrity)

If, when assessing and investigating the risk, it was defined that functional faults of the control or the failure of protective devices could result in a high risk, then their probability must be reduced until the remaining risk can be tolerated. This means that the control must achieve adequate "Safety Performance ".

In order to answer the question as to what can be adequately assumed to be safe, up until now, the technique (risk diagram) shown in Appendix B of EN 954-1 / ISO 13849-1 was used. This then allowed "specific categories" to be determined for the safety-related control functions.

Now, in the form of IEC 62061, in addition to EN 954, there is a new Standard for safety-related machine controls. A technique is described in this Standard that uses a quantified - and therefore hierarchic graduation - of the Safety Performance orientated to the probability. The result of the risk analysis is then the Safety Integrity Level (SIL) for the safety functions involved.

A similar, quantified and therefore hierarchic graduation of the Safety Performance will be introduced with the new Edition of ISO 13849-1. The level, designated there as Performance Level (PL) correlates with the SILs of IEC 62061 through the assigned probability of failure.

The techniques described in both of these standards are based on the same principles. This is the reason that the user can select which standard he wishes to apply. The responsible technical committees of IEC and ISO recommend the selection specified in the following table (Fig. 2/11).

Note: If a C standard exists for the machine type being considered, then the protective measures described there have priority and should be predominantly implemented with the specified Categories. However, the specifications should be checked to see whether they correspond to the latest technical developments.

Safety performance to implement the control according to EN 954

A technique to determine the necessary category for a specific risk is described in EN 954-1. However, the categories are not hierarchically structured. This is the reason that the risk diagram, shown in Fig. 2/7, is only a recommendation. Further, this technique means that different categories can be selected for a specific risk. The result is not clear and can also be influenced by the technology of the solution being used.

[3] The measure for "Safety Performance" is defined differently in the various standards: Categories in EN 954, Safety Integrity Level (SIL) in IEC/EN 61508 and IEC 62061 and Performance Level (PL) in draft ISO 13849-1(rev).

[4] The term "Safety Performance" is used here as higher-level term for the safety-related performance of the control system. It encompasses the "Category", "Safety Integrity" and "Performance Level" terms used in the various Standards".

Technique to evaluate the risk elements and categorize the Safety Performance.

Risk diagram according to EN 954

The objective is to determine a required category using the risk elements.

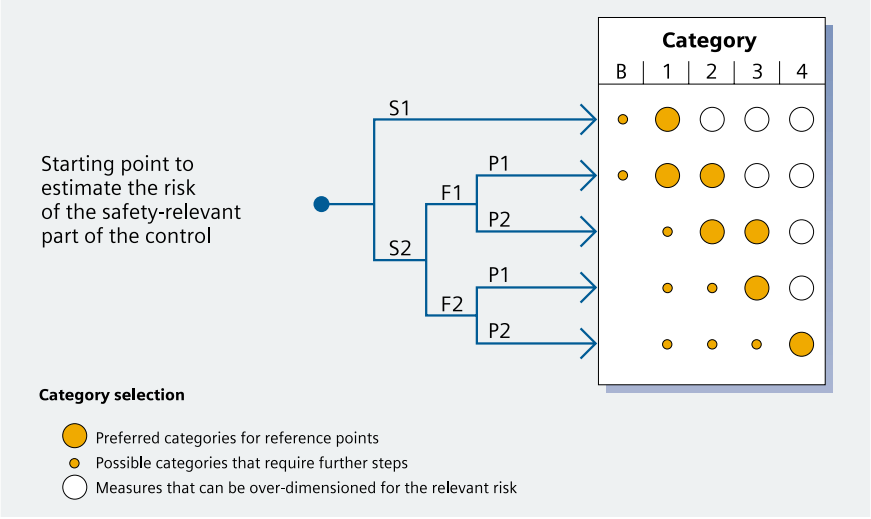


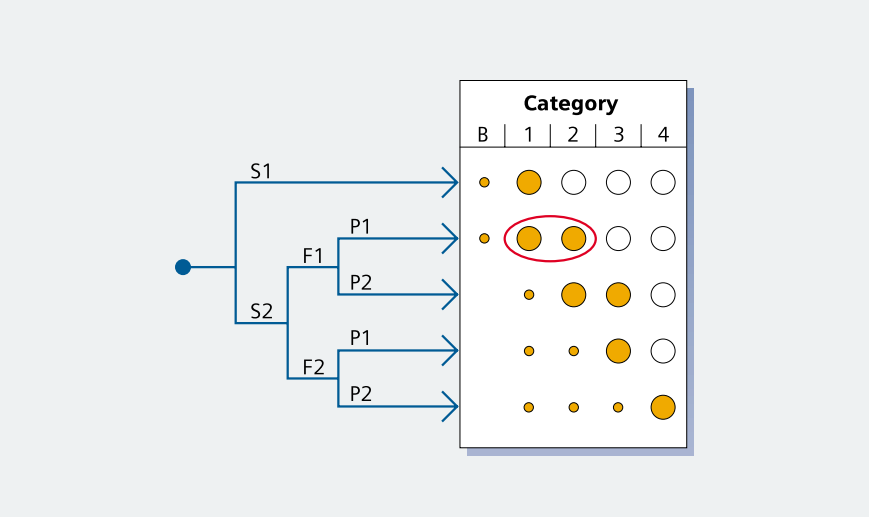
Fig. 2/7
Risk diagram to determine the required Categories from EN 954-1

Information to interpret the risk diagram according to EN 954

Example 1:

The risk assessment goes through S2 (severe, irreversible injury of one or several persons or death of one person), F1 (seldom to more often) and P1 (possible under certain conditions) to a required Category 1 or 2.

In so doing, Category 2 does not represent a better "resistance" to a fault (one fault results in the loss of the safety function), however, the fault detection is improved when compared to Category 1.

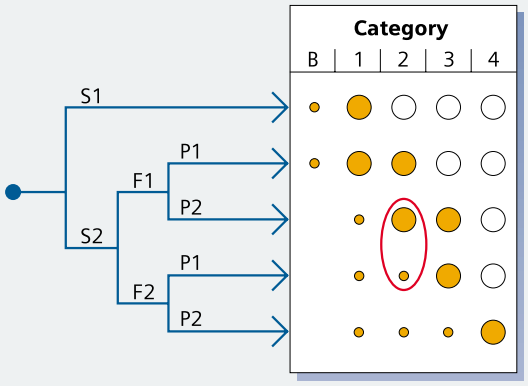


[5] EN 954 is called ISO 13849 internationally.

Example 2:

The immunity with respect to faults can be increased by additional measures, but the category remains the same.

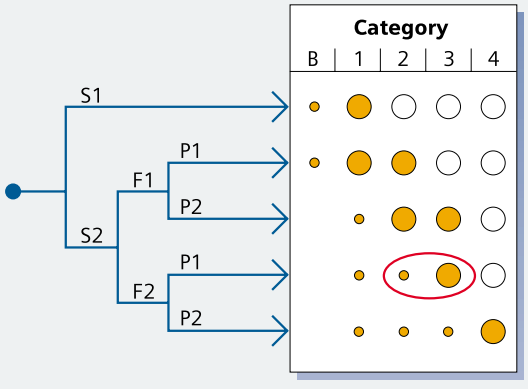
In this example, the category reached is just as before, Category 2.



Example 3:

The required Category 3 cannot be reached using supplementary measures with another category (in this case with Category 2).
In this example, although the same risk is covered (the same "Safety Performance" reached), however, the risk assessment demands, just as before, a Category 3 to reduce risk.

A hierarchically graduated, quantified level for the Safety Performance - designated as Performance Level (PL) - is introduced with the scheduled new Edition of EN 954-1 as ISO 13849-1(rev) (refer to Fig. 2/8). This therefore avoids any ambiguity when selecting the appropriate category.



Risk diagram according to prEN ISO 13849-1

The objective is to determine a required Performance Level PL_r - i.e. the probability of dangerous failures in the system using the risk elements.

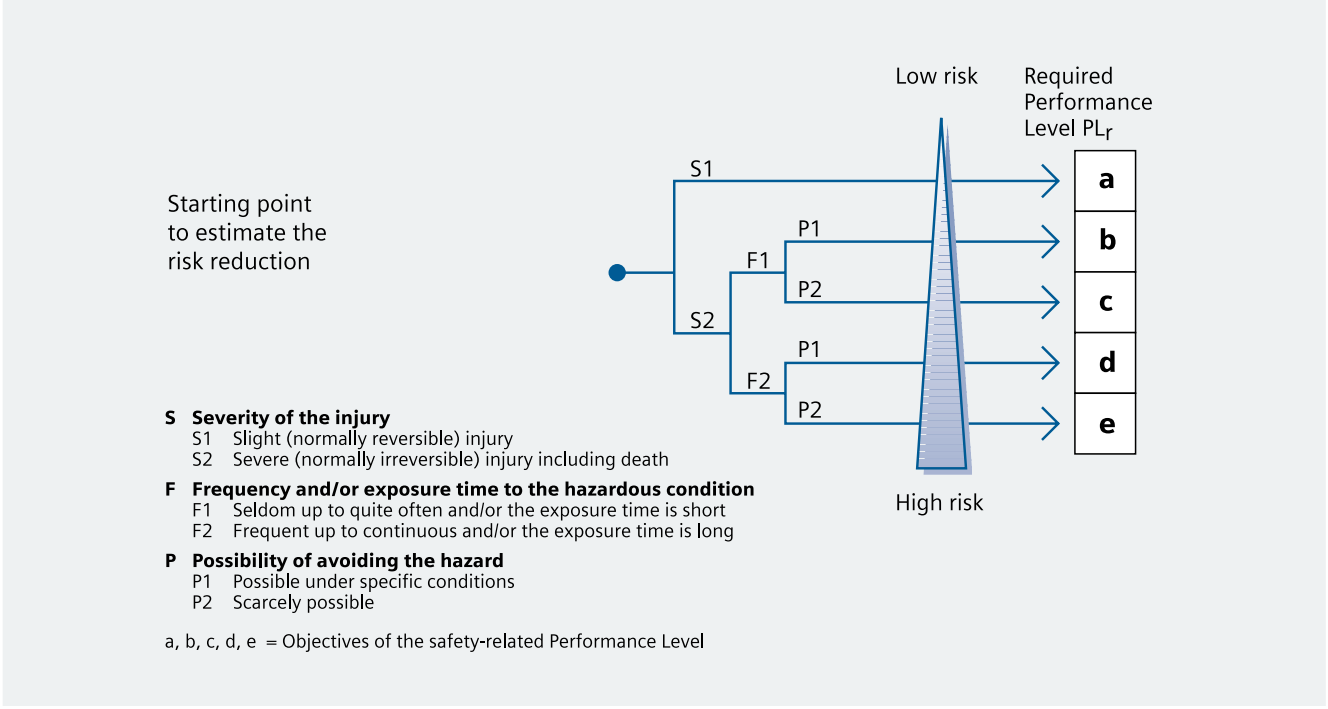


Fig. 2/8
Risk diagram (Draft) according to ISO 13849-1 (rev) to determine the required Performance Level

The Performance Level (PL) is a quantitative measure of the Safety Performance just like the Safety Integrity Level (SIL) in IEC 61508 and IEC 62061. Fig. 2/9 shows the inter-relationship between these two parameters.

Initially, this apparent variance appears confusing.
However, there are defined relationships between the various levels of the required Safety Performance.

The responsible bodies and associations have still not officially defined the allocation of the required categories to the required Performance Levels or Safety Integrity Levels. However, the following allocation can be made,

[6] The risk diagram shown is a draft that still has to be discussed in the responsible associations and committees.

Performance level PL	Average probability of dangerous failures within one hour	SIL EN 61508-1 (IEC 61508-1) for information
a	≥ 10-5 to < 10-4	no special safety requirements
b	≥ 3x 10-6 to < 10-5	1
c	≥ 10-6 to < 3x10-6	1
d	≥ 10-7 to < 10-6	2
e	≥ 10-8 to < 10-7	3
Comment 1: The representation of each hazardous situation is subdivided into 5 stages from a to e. In this case, the risk reduction for a is the lowest, for e, the highest. Comment 2: Performance Levels b and c together cover one order on the magnitude scale of the average probability of dangerous failures per hour (also on the SIL scale).		

Fig. 2/9
Performance Level

based on the same risk parameters, from the risk diagrams in Figs. 2/7 and 2/8:

Category 1 → PL_r b → SIL 1
Category 2 → PL_r c → SIL 1
Category 3 → PL_r d → SIL 2
Category 4 → PL_r e → SIL 3

This allocation of a required Category to the required PL_r or SIL should be considered to be a simplification. On a case-for-case basis, as a result of the multiple interpretation for the categories, the special issues associated with the particular application should be taken into consideration.

Safety Performance for implementing a control in compliance with IEC 62061

The technique described in Appendix A in IEC 62061 is also based on the risk parameters defined in EN 1050; however, contrary to ISO 13849-1 it uses a tabular technique that can be directly used to document the risk evaluation carried-out and allocation to a particular SIL.

The associated weighting should be selected for the individual risk parameters using the values specified in the header of the table. The sum of the weighting of all parameters provides the probability class of the damage.

Cl = Fr + Pr + Av

Refer to the explanation on Fig. 2/10.

Using this probability class and the possible severity of damage of the hazard being considered, the necessary SIL for the associated safety function can be read from the table.

Table to determine the Safety Integrity Level according to IEC 62061 (SIL assignment)

The objective is to determine the required Safety Integrity Level SIL - i.e. the probability of dangerous systems failures - using the risk elements.

Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl					Frequency and duration, Fr		Probability of hzd event, Pr		Avoidance Av	
		3 - 4	5 - 7	8 - 10	11 - 13	14 - 15						
Death, loosing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Common	5		
Permanent, loosing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Possible	3
							> 1 yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Comments

	Extent of the damage CL
	Damage magnitude Se
	Time in the hazardous area Fr
	Probability of occurrence Pr

Fig. 2/10
Example of the form for SIL measures

2.4 Specification of the safety requirements

If control functions were identified as safety-related or if protective measures should be implemented using the control, then the precise requirements for these “safety-related functions” (“safety-related control functions”) should be defined in the specification of the safety requirements. This specification describes, for each safety-related function, among other things, the following:

- Its functionality, i.e. all of the necessary input information, its interlocking and the associated output states or actions as well as the frequency of use
- The necessary response times
- The demanded Safety Performance

The specification of the safety requirements includes all of the information that is required to design and implement the control.
It is the interface between the machine construction company and manufacturer/integrator of the control and can be used to clearly demarcate and assign levels of responsibility.

Design and implementation of safety-related controls

Which standard is to be applied - ISO 13849 or IEC 62061?

A safety-related control for machines can be implemented, both according to IEC 62061 as well as also according to ISO 13849. The safety objectives of the Machinery Directive regarding functional safety are fulfilled with the requirements of each of the two standards. The following table provides help when deciding which of the standards to select - that is provided as recommendation in the foreword of both of these standards.

	Technology to implement safety-related control functions	EN ISO 13849-1(rev.)	IEC 62061
A	Non-electrical, e.g. hydraulic	X	Not covered
B	Electromechanical, e.g. relays and/ or simple electronics	Limited to designated architectures (refer to Comment 1) and max. up to PL = e	All architectures and max. up to SIL 3
C	Complex electronics, e.g. programmable electronics	Limited to designated architectures (refer to Comment 1) and max. up to PL = d	All architectures and max. up to SIL 3
D	A combined with B	Limited to designated architectures (refer to Comment 1) and max. up to PL=e	X refer to Comment 3
E	C combined with B	Limited to designated architectures (refer to Comment 1) and max. up to PL = d	All architectures and max. up to SIL 3
F	C combined with A, or C combined with A and B	X refer to Comment 2	X refer to Comment 3

"X" indicates that the point is covered by this standard.

Comments

1 Designated architectures are described in Appendix B of EN ISO 13849-1 and provide a simplified basis for quantification.

2 For complex electronics: Using designated architectures in compliance with EN ISO 13849-1 up to PL = d or every architecture in compliance with IEC 62061.

3 For non-electrical systems: Use the parts that correspond to EN ISO 13849-1 (rev) as subsystems.

Fig. 2/11
Recommended use of IEC 62061 & ISO 13849-1 (rev.)

Note:

In January 2005, IEC 62061 was published as IS and is ratified as EN 62061. In 2004, ISO 13849-1 (rev) published the Draft prEN ISO 13849-1 (and DIS ISO 13849-1) for comments. As a result of the comments that were received, changes can still be expected before ISO 13849-1 can be published for final voting. A final edition can be expected, at the earliest, at the end of 2005.

Formally, presently only EN 954-1 is harmonized under the Machinery Directive (beginning of 2005). This makes it the binding Standard to fulfill the EU Machinery Directive. However, when applying IEC 62061, the requirements of EN 954-1 are fulfilled and beyond this, also the current state-of-the-art technology for programmable electronic systems, including bus communication.

The draft of ISO 13849-1 addresses, just the same as EN 954-1, various technologies. For instance, electrical, hydraulic, pneumatic and mechanical.

The objective is to be able to implement a safety-related control function based on the “intended architectures” and an appropriate category: This reflects today's implementation strategies that are practiced.

No statements were made regarding safety-related software. In fact, quite the contrary, reference was explicitly made to other Standards (for example, the subject of software is described in detail in the IEC 62061).

2.5 Design and implementation of (safety-related) controls according to IEC 62061

Goal: A safety-related (control) system must correctly execute a safety function. Even when a fault develops, it must behave so that the machine or plant either remains in a safe condition or is brought into a safe position.

Determining the necessary Safety Performance (Safety Integrity)

Also refer to Chapter 2.3 "Does the protective measure depend on a control?"

Philosophy/theory

Principle structure for a safety-related control system

The essential prerequisite that a control correctly functions as it was originally intended is its correct construction. In order to achieve this objective, IEC 62061 has defined a systematic top down design process:

A safety-related electrical control system (SRECS) includes all components - from information detection through arithmetic and logical operations up to and including the execution of actions. In order to permit a straightforward, systematic procedure to create the design that should fulfill the safety-related evaluation and the implementation of an SRECS, which fulfills the requirements of IEC 61508, IEC 62061 uses a structure that is based on the following architectural elements (refer to Fig. 2/12) (this structure can also be used if the safety-related parts of the control are to be implemented acc. to EN 954).

To start, a differentiation is made between a "virtual (i.e. functional) perspective" and the "real (i.e. system) perspective". The functional perspective only considers the functional aspects, independent of the implementation using hardware and software. For instance, in the virtual perspective, consideration is only given to which information is to be detected, how this is to be processed and which action can result from it. However, no statement is made whether, e.g. redundant sensors are required in order to detect information - or how the actuators are to be implemented. The implementation using a SRECS is only considered with the "real perspective". In this case, it must be decided, for example, whether one or two sensors are required to detect certain information in order to achieve the required Safety Performance level. The following terminology was defined.

Terminology **to structure the functions** (functional perspective):

Safety-related control function
Control function with a defined level of integrity that is executed by an SRECS with the goal of maintaining the safe condition of the machine or preventing hazardous situations at the machine.

Function block
Smallest unit of a safety-related control function (SRCF), whose failure results in the failure of the safety-related control function.

Comment: In IEC 62061, an SRCF (F) is considered as logically ANDing the function blocks (FB), e.g. F = FB1 & FB2 & ... & FBn.

The definition of a function block differs from that used in IEC 61131 and other Standards.

Function block element
Part of a function block.

Terminology used **when structuring a real system** (system perspective):

Safety-related electrical control system
Electrical control system of a machine whose failure can result in the immediate increase of the risk.

Comment: An SRECS encompasses all parts of an electrical control system whose failure can result in the reduction of the functional safety or in the loss of the functional safety. This can include both - power and control circuits.

Subsystem
Element of the architectural design of the SRECS at the topmost level. Whereby, if any subsystem fails, this results in failure of the safety-related control function.

Comment: Contrary to the general use of terminology, where "subsystem" can mean any unit that has been created by splitting-up the total entity, "subsystem" in IEC 62061 is used in a strictly defined hierarchy of the terminology. "Subsystem" means the subdivision at the topmost level. The parts that are created from additional subdivision of a subsystem are known as "subsystem elements".

Subsystem element
Part of a subsystem that includes the individual components or a group of components.

Using these structural elements, control functions can be structured according to a clearly defined technique so that defined parts of the function (function blocks) can be assigned specific hardware components - the subsystems. This means that clearly defined requirements are obtained for the individual subsystems so they can be designed and implemented independently of one another.

The architecture to implement the complete control system is obtained by arranging the subsystems with respect to one another just the same as the function blocks are arranged within the function (logically).

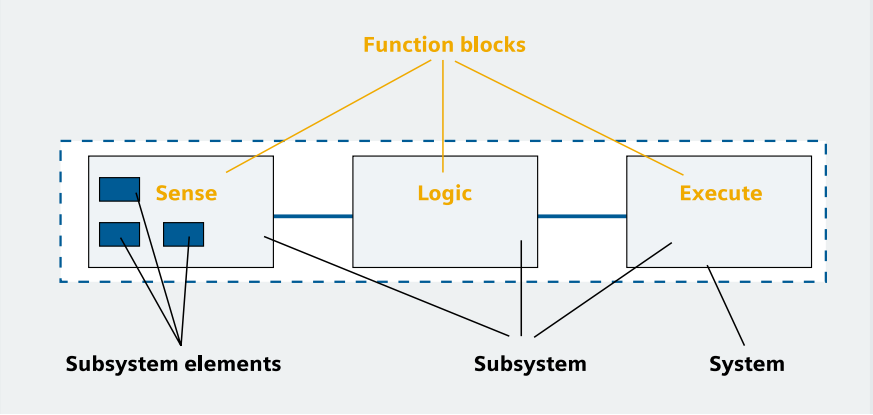


Fig. 2/12
Structural elements of the system architecture

Process to design a safety-related control system SRECS

If the safety requirement specifications are available, the intended control system can be designed and implemented. A control system that fulfills the specific requirements of a particular application can generally not be purchased pre-configured, but instead must be designed and constructed individually for the particular machine from the devices that are available.

In the design process (refer to Fig. 2/13), initially, a suitable control system architecture is designed for each safety function. The architectures of all safety functions of the particular machine can then be integrated to form a control system.

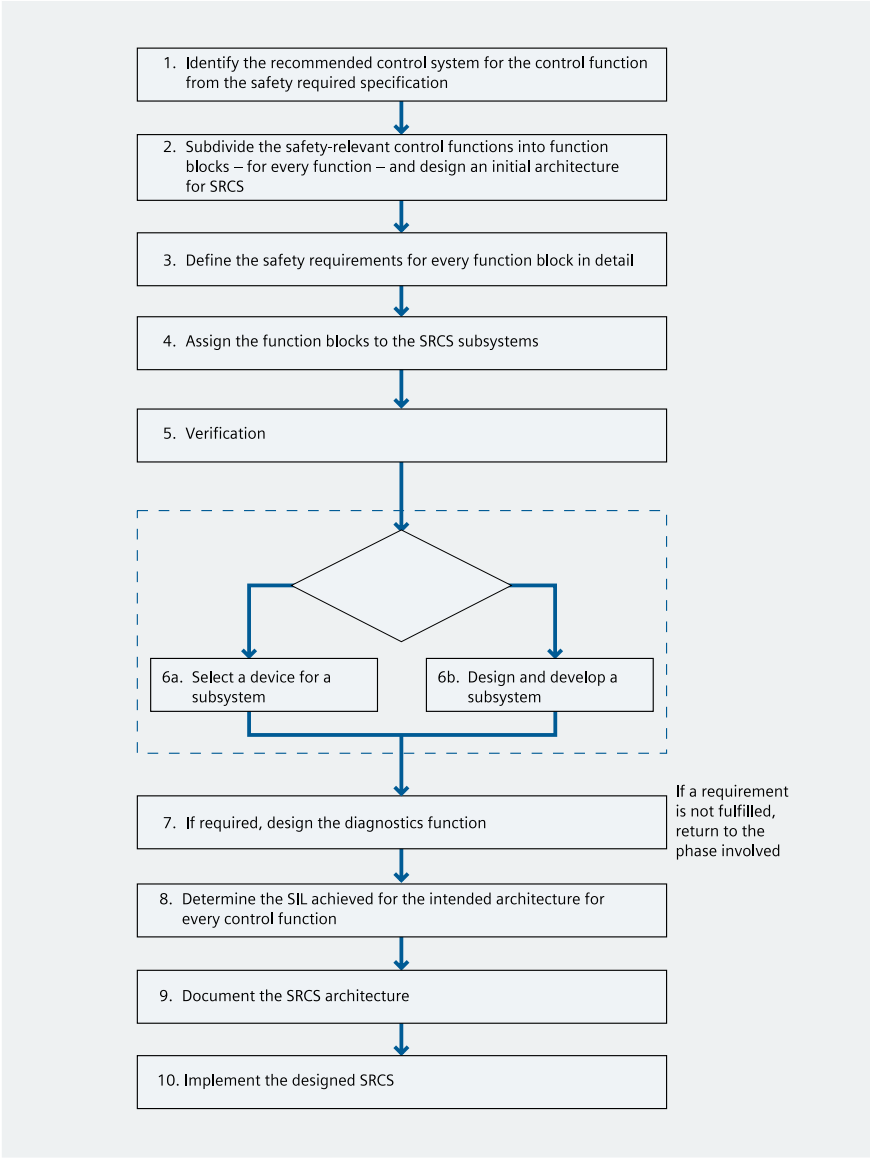


Fig. 2/13
Process to design a safety-related control system

Structuring the safety function

The basic principle of the structured design is that each control function is subdivided into (intended) function blocks so that these can be assigned to specific subsystems (Fig. 2/14). The demarcation of the individual function blocks is selected so that they can be completely executed by certain subsystems. In so doing it is important that every function block represents a logical unit that must be correctly executed so that the complete safety function is correctly executed.

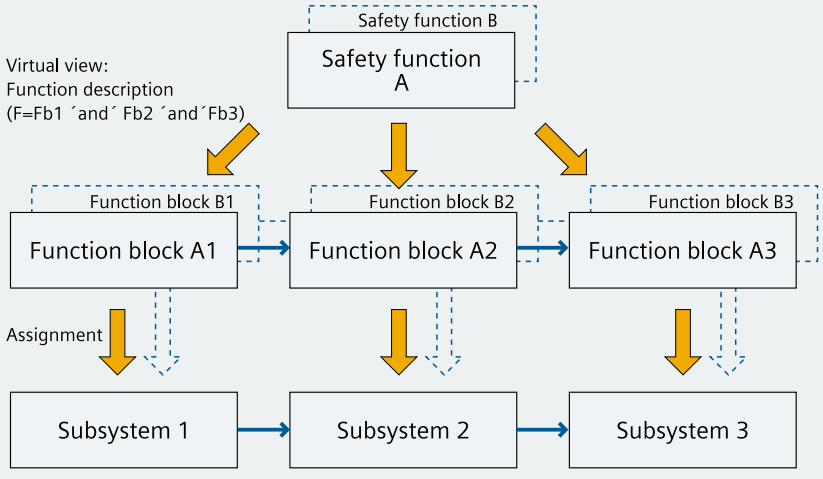


Fig. 2/14
Subdivision of a safety function into function blocks and assignment to subsystems

Generally, a control function comprises basic elements (Fig. 2/15).

- Detecting (e.g. machine states/conditions, operator commands, states of the protective devices and equipment)
- Interlocking (i.e. interlocking the status/condition information, operator commands, etc. and if required, deriving an action)
- Executing (... the action initiated from the interlocking - logical operation)

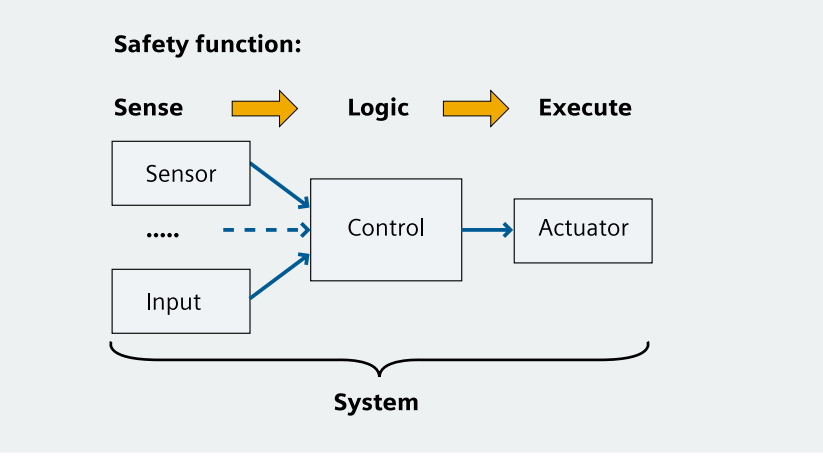


Fig. 2/15
Basic elements of a control function

In the sense of the specification of a safety function, every piece of information and data to be detected is assigned a dedicated "function block". In the same way, every action to be executed is assigned a dedicated "function block". The interlocking and logical operations applied to the information and data that has been detected - this is the safety function logic - is also considered as a dedicated subfunction. This means that it is also assigned to a "function block". This "logic" function block initiates, dependent on the information and data detected, the actions to be executed. This means that several function blocks can belong to a safety-related function - both for detecting as well as for executing.

Subdivision of a safety function into function blocks for example (2)
simple safety function F described for the measures to reduce risks, that prevents access to the hazardous zone while the machine is running:

F = During productive operation, all access entry points to the working zone of the machine (production cell) are interlocked.

The subdivision results in the function blocks:
F1 = Detecting the selected status
F2 = Logic: Dependent on the selected operating mode, initiate interlocking of doors A and B,
F3 = Interlock door A
F4 = Interlock door B
The individual function blocks have defined limits so that to correctly implement and execute safety function F, all of its function blocks must be correctly executed. Therefore the following logical operation applies

F = F1 `and´ F2 `and´ F3 `and´ F4;

Behavior when a fault develops:
If a fault, e.g. is detected in an interlocking function, so that unauthorized access to the machine can no longer be excluded, then the machine must be stopped.

As a result of these inter-relationships, the Safety Performance required for the complete safety function can be transferred as follows to the function blocks and the subsystems assigned to them. (EN 954 and IEC 62061 are considered separately in the following due to their different concepts.)

Note:

In this first step, only the demarcation of the function blocks and the subdivision of the system into subsystems (as defined above!) is made. If it is necessary to consider the subsystems, then this is only done in a next step that is described below.

Required Safety Performance of the subsystems

The Safety Performance of a safety-related control system always refers to the complete safety-related function - as defined in the safety requirements specification for the system. Using the general structure described above, the required Safety Performance can be derived for the individual subsystems.

There are differences in the systemology of the requirements of IEC 61508 and IEC 62061 on one hand and EN 954 (or ISO 13849) on the other hand. This results in differences when determining the details of the required Safety Performance of a subsystem.

Safety Performance of a subsystem acc. to IEC 61508 and IEC 62061

"Safety Integrity" acc. to IEC 61508 *and therefore also IEC 62061) specify that three basic requirements must be complied with:
(1) systematic integrity),
(2) structural restrictions,
i.e. the fault tolerance and
(3) limited probability dangerous,
random (hardware) failures (PFH_D).
that are graduated according to the SIL.

The systematic integrity (1) of the system, specified and required for the complete function as well as the structural restrictions (2) apply to the individual subsystems, just the same as for the system. This means that if each individual subsystem fulfills the required systematic integrity and the structural restrictions of a specific SIL, then the system also fulfills it. However, if a subsystem only fulfills the lower requirements of a lower SIL, then this limits the SIL that the system can achieve. This is the reason that a "SIL claim limit" (SIL CL) is defined for a subsystem.

- Systematic integrity:
  SIL SYS <= SIL CL_{lowest}
- Structural restrictions:
  SIL SYS <= SIL CL_{lowest}

In order to interconnect the subsystems, the same requirements must be fulfilled. This is the reason that individual wiring connections are considered as a component of one or both connected subsystems. For bus connections, the send (transmit) and receive hardware and software are parts of subsystems.

Limiting the probability of dangerous, random faults (3) applies to the complete function, i.e. it may not be exceeded by all of the subsystems together. Therefore, the following applies:

$$PFH_D = PFH_{D1} + ... + PFH_{Dn}$$

For bus connections, it is also necessary to add the probability of possible data transmission errors (P_{TE}).

The SIL CL, PFH_{Dn} and P_{TE} parameters discussed here, can be specified by manufacturers of subsystems in the associated data sheets.

Safety-related parameters of subsystems

The description of a subsystem includes, in addition to the precise specification of its functionality and application conditions, also the safety parameters to specify its Safety Performance.

For designs acc. to IEC 62061

- The maximum SIL, for which it is suitable, SIL CL
- The probability of (dangerous), random faults, PFH_D
- And for bus connections, the probability of undetected data transmission errors, P_{TE}

System design for a safety function

Draft architecture

The architecture of a control system for a specific safety function corresponds, as far as its logical structure is concerned, to the previously determined structure of the safety function. In order to define the real system structure, the function blocks of the safety function are assigned to specific subsystems. The subsystems are then interconnected with one another, so that the connections, specified by the function structure, are established. The physical interconnections are made corresponding to the features of the interconnection system used - e.g. using individual wiring (point-to-point) or using buses.

The same procedure is applied to additional safety-related functions of the machine or plant. In this case, function blocks that correspond to this or other safety functions can be assigned the same subsystems. This means that the same sensors can be used, e.g. if the same information must be sensed for two different functions (e.g. the position of the same protective door).

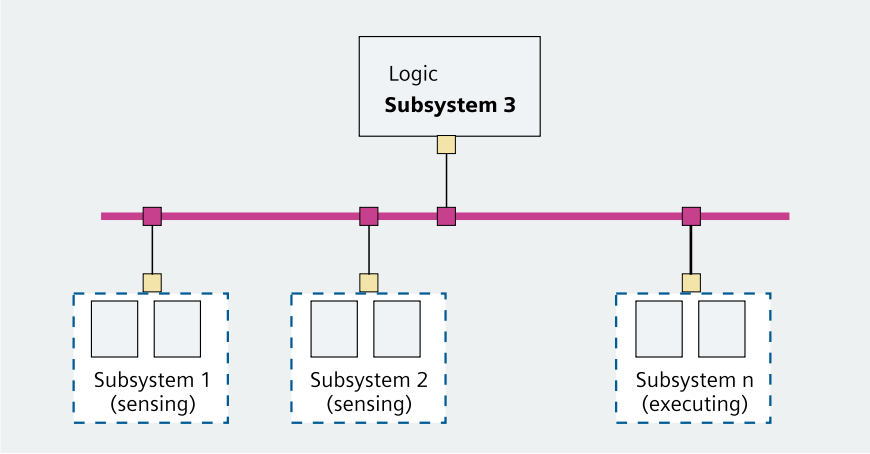


Fig. 2/16
Example of the system architecture for a safety function

Selecting suitable devices and equipment (subsystems)

A subsystem that is to be used to implement a safety function, must have the required level of functionality and fulfill the appropriate requirements of IEC 62061. Microprocessor-based subsystems must fulfill IEC 61508 for the appropriate SIL.
Devices and equipment that fulfill a specific Category according to EN 954 can be used as subsystems. The requirements necessary to integrate these devices into the design concept of IEC 62061 are described in Section "Implementing subsystems".

For designs according to IEC 62061

The individual subsystems must fulfill the specified safety-related parameters (SIL CL and PFH_D).

Subsystems can also be used that fulfill specific Categories. The appropriate safety-related parameters - "SIL CL" and "PFH_D" - can be determined based on the specified Category (refer to IEC 62061, Sections 6.7.6 and 6.7.8).

In many cases, devices require additional fault detection measures (diagnostics) in order that they can actually achieve the specified Safety Performance for use as subsystem. This fault detection functionality can be realized using, e.g. supplementary devices (for instance 3TK28) or the appropriate software diagnostic blocks in the logic processing (refer to "Subsystem design"). In this case, the description of the device must include the appropriate information.

If a suitable device is not available that fulfills the requirements of such a specified subsystem, then it must be created using devices that are available. This requires the next step of the design. Also refer to the Section "Subsystem design".

Implementing the safety-related control system

A safety-related control system must be implemented so that it fulfills all of the requirements corresponding to the demanded SIL. The goal is to reduce the probability of systematic as well as random faults, which could result in the dangerous failure of safety functions, to a sufficiently low level. The following aspects should be taken into account

- Hardware integrity, i.e. restrictions regarding the architecture, (fault tolerance) and limited probability of failure
- Systematic integrity, i.e. requirements regarding avoiding and controlling faults,
- Behavior when detecting a fault and software design/ development

Hardware integrity

Every subsystem must have sufficient fault tolerance corresponding to the SIL of the system. This depends on what proportion of the faults go in the safe direction, referred to the probability of all possible faults of the subsystem. Potentially dangerous faults of a subsystem that can be detected in plenty of time as a result of the appropriate diagnostic functions, belong to those faults that go in a safe direction.

The permitted probability of failure of a safety function is limited by the SIL defined in the specifications (refer to Fig. 2/17).

Systematic integrity

Measures, both to avoid systematic faults and errors as well as to control faults remaining in the system, must be applied:

Avoiding systematic faults

- The system must be installed according to the safety schedule
- The manufacturer's data of the devices used must be carefully adhered to
- The electrical installation must be in compliance with IEC 60204-1 (7.2, 9.1.1 and 9.4.3)
- The design must be carefully checked to ensure its suitability and correctness
- A computer-supported tool must be used that uses pre-configured and tested elements.

Controlling systematic faults

- By disconnecting the energy feed
- Measures to control temporary subsystem failures or faults, e.g. due to power interruptions
- When connecting-up subsystems through a bus, the requirements of IEC 61508-2 regarding data communications must be fulfilled (e.g. PROFIsafe and ASIsafe)
- Faults in the connection (wiring) and the subsystem interfaces must be detected and suitable responses initiated. For systematic handling, the interfaces and the wiring are considered as a components of the associated system.

Details, also refer to IEC 62061 6.4

Behavior when detecting a fault

If subsystem faults can result in hazardous failure of a safety-related function, then these must be detected in plenty of time and an appropriate response initiated in order to avoid a hazard. The failure rates of the devices used and the SIL of the system to be achieved (or the required PFH of the subsystem) define to which level automatic fault detection (diagnostics) is necessary.

How the system or the subsystem must behave when a fault is detected, depends on the fault tolerance of the associated subsystem. If the detected fault does not directly result in a failure of the safety-related function, i.e. fault tolerance > 0, then a fault response is not immediately necessary, in fact only if the probability that a second fault occurs becomes too high (generally, this involves hours or even days). If the fault that is detected directly results in the safety-related function failing - i.e. a fault tolerance = 0 - then a fault response is immediately required, i.e. before a hazard actually occurs.

Safety Performance level reached

For every safety-related function it is specified which Safety Performance it requires. This must be fulfilled by the safety-related control system.

For each safety-related function, it must be determined as to which Safety Performance a system reaches. This is realized using the architecture of the system and the safety-related parameters of the subsystems that are involved in executing the safety-related function being considered.

Design acc. to IEC 62061

The SIL that is achieved is limited by the "SIL claim limit" of its subsystems. The lowest value of the subsystems used limits the SIL of the system to this value (the weakest link defines the strength of the chain).

Systematic integrity:
SIL SYS <= SIL CL_{lowest}

Structural restrictions:
SIL SYS <= SIL CL_{lowest}

The safety requirements must be fulfilled when connecting the subsystems with one another. In this case, individual wiring connections are considered as part of one or the two connected subsystems. For bus connections, the send and receive hardware and software are part of the subsystems.

In addition to this principle suitability (claim limit), the probability of a dangerous failure of every safety-related function must be considered. This value is obtained by simply adding the probabilities of failure of the subsystems involved in the function:

$PFH_D = PFH_{D1} + ... + PFH_{Dn}$

For bus connections, in addition, the probability of possible data transmission errors (PTE) must be added.

The value determined for a certain safety function must be less (or the same) as the value defined by the associated SIL.

Design according to EN 954

The category of the system reached corresponds to the category of its subsystems.

If computer-based subsystems and bus communications are used, then these must fulfill certain SIL acc. to 61508. The following assignment applies: A subsystem suitable for SIL 1 can be used for Category 2 and, correspondingly, SIL 2 for Category 3 or SIL 3 for Category 4.

Probability of a dangerous fault per hour (PFH_D)

	SIL 1	SIL 2	SIL 3
PFH_D	$< 10^{-5}$	$< 10^{-6}$	$< 10^{-7}$

Fig. 2/17
Limit values of the probabilities of dangerous faults of a safety function

System integration for all safety-related functions

After the architectures for all of the safety related functions have been designed, then the next step is to integrate these function-specific architectures to create a full, safety-related control system.

There, where several safety-related functions have identical function blocks, common subsystems can be used to implement them. For instance, only one safety PLC is required to implement the logic of all of the safety functions. Or, in order to remove different hazards (i.e. different safety functions) the condition of the same protective door must be sensed, then the sensor required only has to be installed once at this door.

This has no influence on the Safety Integrity, that has already been defined for the individual functions. Only for electromechanical devices (i.e. devices that are subject to wear), does this have to be taken into account when determining their switching frequency.

Designing and implementing subsystems

As an alternative to selecting an existing subsystem, a subsystem can be made-up of devices that alone do not fulfill the safety requirements but so that the subsystem then achieves the necessary Safety Performance. This is - in reference to the systematic integrity and the architectural constraints - the SIL claim limit (SIL CL) specified by the required SIL of the safety-related function. When designing the system architecture, the maximum PFH values for the individual system systems was defined for the probability of the dangerous random faults (PFH_D).

> IEC 62061: The safety performance of a subsystem is characterized by the SILCL determined by its architectural constraints (6.7.6), its SILCL due to systematic integrity (6.7.9) and its probability of dangerous random hardware failure (6.7.8).

Generally, at least for SIL 2 and SIL 3, redundancy is required. Whether it be to achieve the necessary fault tolerance or to permit fault detection (diagnostics).
However, it may also be necessary to combine two devices to form a subsystem in order to reduce the probability of dangerous failure.

> If, for example, for the access interlocking of example (2) risk reducing measures SIL 2 or 3 (or Category 3 or 4) is required, then simple door interlocking functions or limit switches are not sufficient. For example, two tumbler mechanisms must be used to interlock every door and measures to detect faults must be implemented.

The precise requirements when designing and implementing subsystems are described in IEC 62061, Sections 6.7 and 6.8. The following description provides an overview.

Designing the subsystem architecture

A special subsystem architecture always has to be designed, if, with the devices intended for a specific task (subfunction "function block") the necessary Safety Integrity (Safety Performance) is not directly achieved. Generally, the safety-related features and characteristics

- Low probability of failure
- Fault tolerance, fault control
- Fault detection

can only be achieved using special architectures. To what extend certain measures are required, depends on the required Safety Performance (Safety Integrity).

The subsystem is assigned a (sub) function, the function block (e.g. keeping a door interlocked). Initially, this function block (from the philosophy) is subdivided into individual elements (function block elements), that can then be assigned specific devices - the subsystem elements (refer to Fig. 2/18). Generally, the same function can be assigned two function block elements (the function was practically doubled). If these function block elements are then implemented using specific devices, then the system has a simple fault tolerance (simple redundancy).

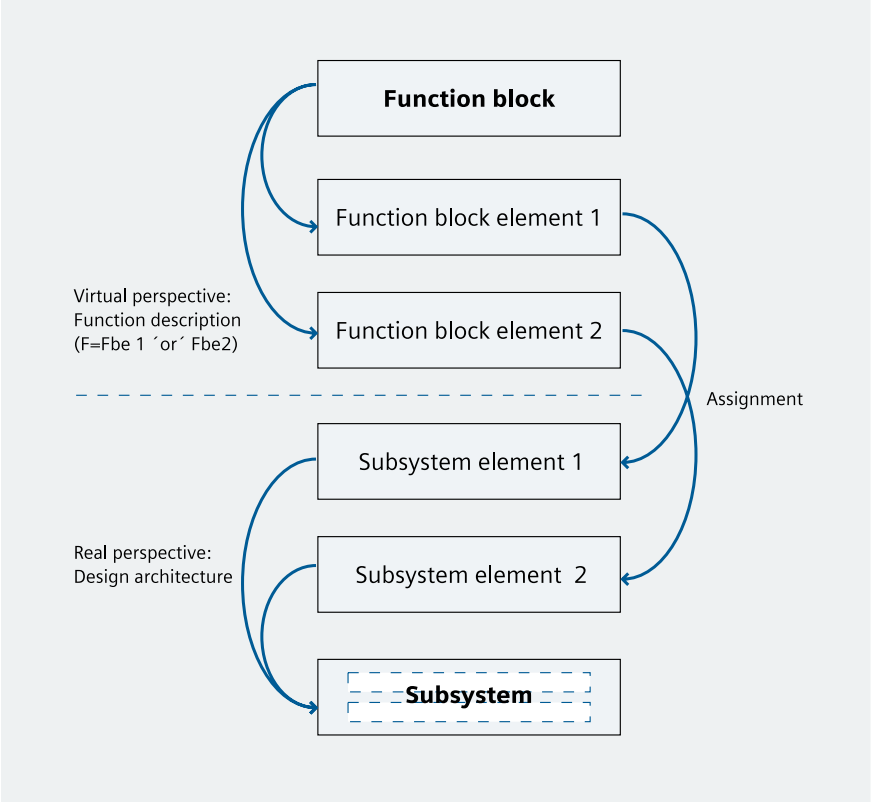


Fig. 2/18
Example for designing a subsystem architecture

If, in order to implement function block F3 "Interlock door A" of example (2) a simple tumbler mechanism is not sufficient in order to achieve the specified Safety Performance, then a subsystem with higher Safety Performance can be implemented with the two following basic solutions.

a) A second door tumbler mechanism is connected in parallel → simple redundancy.
b) The door tumbler mechanism is supplemented by a door position monitoring function → fault detection

In example a) for homogeneous redundancy, the function block "interlock door A" is subdivided into two identical function block elements where each element has this function. In order to detect possible faults, in spite of this redundant arrangement, additional measures are required.
In example b), the function block "interlock door A" is not subdivided any further. It is assigned one-to-one to a function block element.
The additional door position monitoring is used for fault detection. It does not improve the door tumbler mechanism itself. However, the monitoring function can detect if the door tumbler mechanism fails and it can then initiate an appropriate response.

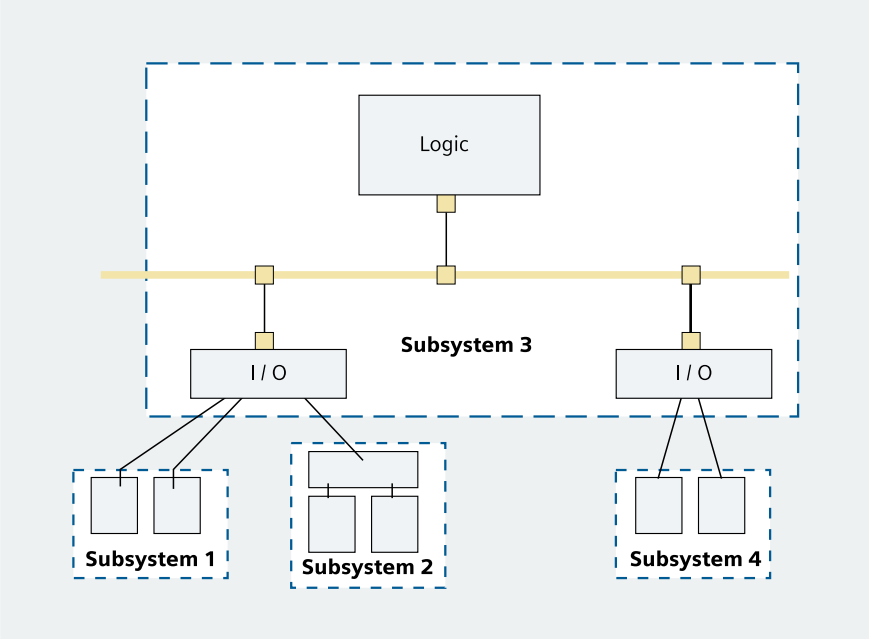


Fig. 2/19
Examples of subsystem architectures

Fault detection of a subsystem (diagnostics)

For a subsystem without fault tolerance, every fault results in the loss of the function. If the function fails, depending on the fault type, this can result in a hazardous or safe state of the machine. Faults, that result in a hazardous condition of the machine are critical. They are designated as "dangerous faults". In order to avoid that a dangerous fault actually results in a hazard, certain faults can be detected using diagnostic routines and the machine can be brought into a safe state before the machine goes into a dangerous state. A dangerous fault, detected with a diagnostics routine, can then be converted in this way into a "safe fault".

For a redundant subsystem, the first fault does not result in the failure of its function. Only an additional fault can result in the loss of the function. In order to avoid the subsystem failing, this means that the first fault must be detected before a second fault occurs. The fault detection must naturally be linked with a suitable system response. In the simplest case, for example, the machine is stopped in order to bring it into a safe condition that does not require the (faulted) safety-related function.

As a result of the fault detection (diagnostic routine) linked with a suitable fault response, in both cases, the probability of a dangerous failure of the safety-related function involved is reduced. To what extent the probability is actually reduced depends, among other things, how many of the possible dangerous faults are detected. The measure for this is the diagnostic coverage (DC).

In the subsystem involved, the fault of a subsystem can be detected by itself or by another device, e.g. the safety PLC. Examples for the different diagnostic arrangements are shown in Fig. 2/20.

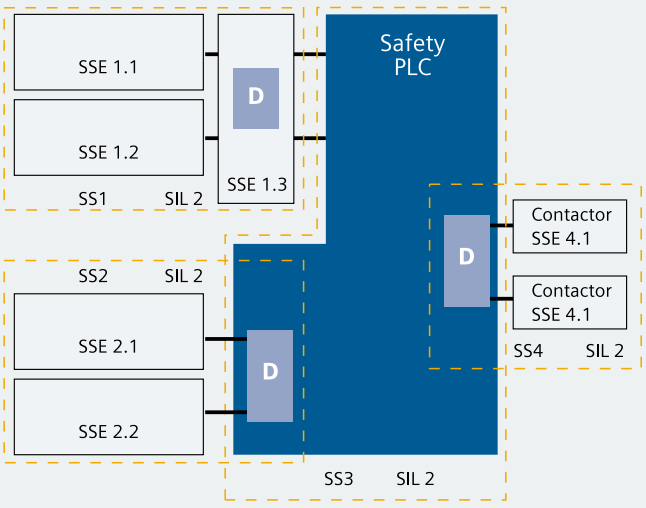


Fig. 2/20
Arrangement of diagnostic functions of subsystems

Systematic integrity of a subsystem

When designing and implementing a subsystem, measures must be made to both avoid as well as control systematic faults; for example:

- The devices used must be in compliance with International Standards.
- The application conditions specified by the manufacturer must be fully complied with.
- The design and the materials used must be able to stand-up to all of the ambient/environmental-conditions that can be expected.
- The behavior due to ambient/ environmental effects must be able to be produced so that a safe condition of the machine can be maintained.
- Online fault detection
- Positive actuation to initiate a protective measure.

The requirements described in IEC 62061 only involve the design of electrical systems having a low degree of complexity - i.e. no micro-processor based subsystems. The required measures apply the same for all SIL.

Probability of failure (PFH_D) of a subsystem

The possible failures are subdivided into "safe" or "hazardous" failures In this case, the hazardous failures of a subsystem are defined as follows.

Dangerous failure

Failure of an SRECS, a subsystem or subsystem element with the potential to cause a hazard or state that is not functional.
Comment: Whether such a condition occurs or not can depend on the system architecture; In systems with multiple channels to improve the safety, a dangerous hardware fault with low probability results in an overall dangerous condition or in the failure of a function.

This means, for example: For a redundant subsystem (i.e. fault tolerance 1), a fault in a channel is considered dangerous if it is potentially dangerous i.e. if there is no second channel then this could result in a dangerous machine state.

For safety-related requirements, only the probability of dangerous failures is decisive. The so-called "safe faults" have a negative impact on the system availability, but do not result in any hazard.

The probability of failure of a subsystem depends on the failure rates of the devices that comprise the system, the architecture and the diagnostic measures. Formulas are described in the following for the most usual architectures. They apply under certain prerequisites that are detailed in IEC 62061:

For sufficiently low (1>> λ .T) failure rates (λ) of the subsystem elements, the following equation can be used:

$\lambda = 1/MTTF$

For electro-mechanical devices, the failure rate (λ) should be defined where the B10 value of the device and the operating cycles rate C of the specified application are used in the following equation:

$\lambda = 0.1*C/B_{10}$

The following terms are used in the formulas:

$\lambda = \lambda_S + \lambda_D$;
whereby λ_S is the rate of non-hazardous failures and λ_D is the rate of hazardous failures.

$PFH_D = \lambda_D * 1h$;
Average probability of dangerous failures within one hour

T2 : Diagnostics test interval

T1:
Proof test interval or lifetime; the lower value is applied

Generally, only a specific percentage of the faults can be detected using diagnostic routines. The diagnostics coverage specifies this percentage.

The diagnostics coverage can be calculated using the following formula:

$DC = \Sigma \lambda_{DD} / \lambda_{Dtotal}$

whereby λ_{DD} is the rate of detected hazardous hardware faults and λ_{Dtotal} the rates of dangerous hardware failures.

In order to determine the diagnostic coverage, the individual faults (failure modes) are weighted corresponding to their relative frequency.
Typical ratio numbers for a series of devices are specified in Table D.1 from IEC 62061. When determining the fault coverage for a subsystem, all of its components (subsystem elements) must be considered. These also include, for example, the terminals and the wiring of the individual parts and components.

Structure without fault tolerance, with diagnostics

With this structure (Fig. 2/21), the subsystem fails if any of its associated elements fail; this means that a single fault results in failure of the actual safety-related function. However, this still does not necessarily mean a dangerous loss of the safety-related function. Depending on the fault type, the machine can go into either a safe or dangerous condition, i.e. the subsystem has a "safe" or "dangerous" fault. If the probability of dangerous faults (PFH_S) is greater than that specified, then these faults must be detected using diagnostic routines and a fault response initiated before a hazard can actually occur. This means that dangerous faults become safe faults and in turn, the probability of a dangerous failure of the subsystem is reduced. As a consequence - the specified failure probability may be able to be reached.

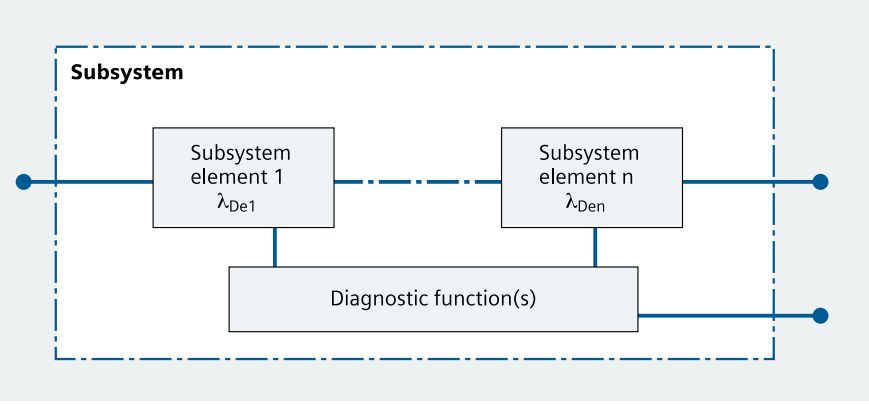


Fig. 2/21
Logical structure of a subsystem without fault tolerance and diagnostics

(Note: For the structure shown in Fig. 2/21, the subsystem has diagnostics with an independent shutdown path. Depending on the diagnostics coverage, using this particular structure, Category 2, 3 or 4 acc. to EN 954-1 can be fulfilled.)

IEC 62061 6.7.8.2.4

Every undetected dangerous fault of a subsystem element results in a potentially dangerous failure of the safety-related control function. If a subsystem element fault is detected, the diagnostics function initiates a fault response function. For this particular structure, the probability of dangerous faults of the subsystem is given by:

$\lambda_{DssC} = \lambda_{De1} (1 - DC1) + ...+ \lambda_{Den}(1 - DCn)$

$PFHDssC = \lambda_{DssC} * 1h$

Structure with simple fault tolerance and with diagnostics

For this structure (refer to Fig. 2/22), the first fault does still not result in failure of the function. However, the fault must be detected before the probability that a second fault occurs, i.e. the subsystem fails, exceeds the specified limit.

In addition to independent, random faults, for redundant subsystems, there is also the possibility of common cause failures that must be considered. Homogeneous redundancy does not help against such faults. This is reason that systematic measures must be applied in the design phase

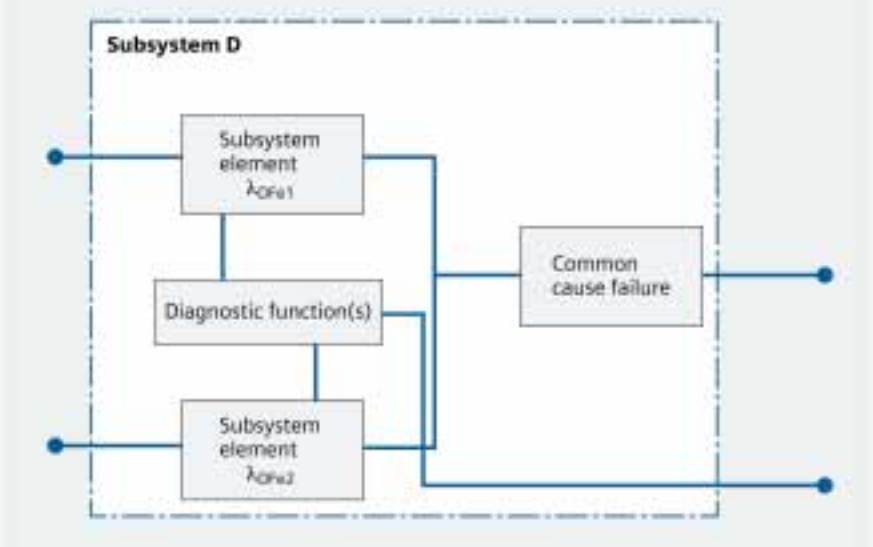


Fig. 2/22
Logical structure of a subsystem with simple fault tolerance with diagnostics

so that their probability is kept sufficiently low. Common cause failures can never be completely excluded. This means that when calculating the failure probability of the subsystem, they must be taken into account. This is done using the Common Cause Factor (β), which is used to evaluate the effectiveness of the measures applied. A table to determine the Common Cause Factor reached is provided in Annex F of IEC 62061.

For this structure, an individual fault of any subsystem element does not result in the failure of the safety-related control function. The following terms are used to calculate the failure probability of the subsystem:

T2: Diagnostics test interval;

t1: Proof test interval or lifetime, however, the lower of the two values;

β: β-Factor, i.e. Sensitivity to common cause faults;

$\lambda_D = \lambda_{DD} + \lambda_{DU}$; whereby λ_{DD} is the rate of detected and λ_{DU} rate of the undetected dangerous faults.

$\lambda_{DD} = \lambda_D * DC$
$\lambda_{DU} = \lambda_D * (1-DC)$

A differentiation is made between two versions when making the calculation.

The subsystem elements of both channels are different:

λ_{De1}: Rate of dangerous faults from subsystem element 1
DC1: Diagnostics coverage for subsystem element 1

λ_{De2}: Rate of dangerous faults from subsystem element 2
DC2: Diagnostics coverage for subsystem element 2

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De1} * \lambda_{De2} * (DC1 + DC2)] * T2/2 + [\lambda_{De1} * \lambda_{De2} * (2 - DC1 - DC2)] * T1/2 \} + \beta * (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} * 1h$

The subsystem elements of both channels are the same:

λ_{De}: Rate of dangerous faults from subsystem element 1 or 2
DC: Diagnostics coverage for subsystem element 1 or 2

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De}^2 * 2 * DC] * T2/2 + [\lambda_{De}^2 * (1 - DC)] * T1\} + \beta * \lambda_{De}$

$PFH_{DssD} = \lambda_{DssD} * 1h$

Structural restrictions of a subsystem

The structural restrictions demand a minimum of fault tolerance depending on the type of possible subsystem fault. The greater the percentage of "safe faults", then the lower the required fault tolerance for a specific SIL.

The appropriate limits are shown in Fig. 2/23. "Safe faults" in conjunction with this, are also dangerous faults that are detected using diagnostic routines.

Percentage of safe faults	Hardware fault tolerance	
	0	1
< 60 %	Not permitted	SIL1
60 % - < 90 %	SIL1	SIL2
90 % - < 99 %	SIL2	SIL3
Comment: A hardware fault tolerance of N means that N+1 faults can result in loss of the function.		

Fig. 2/23
Structural restrictions of a subsystem (excerpt from IEC 62061)

For instance, for a subsystem that is to be used for SIL 2, fault tolerance is not required (FT = 0), if the percentage (%) of its faults, that go in a safe direction, are more than 90%. Most devices do not achieve this value themselves. However, it is possible reduce the percentage of dangerous faults by detecting faults using diagnostic routines and initiating a suitable response in the plenty of time.

The safe failure fraction of a subsystem is the percentage of faults that result in a safe machine condition weighted for all subsystem faults according to their probability of occurrence

Definitions in IEC 62061

Percentage of safe faults (SFF)
Percentage of the complete rate of a subsystem that does not result in a dangerous failure.
The safe failure fraction (SFF) can be calculated using the following formula:

$(\Sigma\lambda_S + \Sigma\lambda_{DD}) \ / \ (\Sigma\lambda_S + \Sigma\lambda_D)$

Whereby

λ_S is the rate of safe failures,

$\Sigma\lambda_S + \Sigma\lambda_D$ is the overall failure rate,

λ_D is the rated of dangerous failures and

λ_{DD} is the rated of dangerous failures that are detected using diagnostics.

If, for a device, only its overall failure rate is specified, but the individual fault modes are not listed, then Appendix D of IEC 62061 provides some helpful information. Typical values for percentages of fault modes for the most usual device types are specified in the table. Which fault mode can result in a safe or dangerous failure of the safety-related function depends on the particular application.

Selecting the devices

In order to use devices in safety-related subsystems, their features, characteristics and the application conditions must be clearly defined.

In order to described the safety-specific features and characteristics, the following data is also required:

- The failure rate and the possible fault modes.
  Note: For electro-mechanical devices, the failure rate is specified as B10 value. (The B10 value is the number of operating cycles after which 10% of the devices have failed. Also refer to IEC 6810-2). Due to the frequency of individual fault modes also refer to IEC 62061 Appendix D.

- Features and characteristics that can be used for diagnostics (e.g. positively-driven auxiliary contacts).

Implementing subsystems

Every subsystem must be implemented as was defined in the design phase for its specified features and ambient conditions. If the subsystem is also implemented corresponding to the requirements in IEC 62061 to avoid and control systematic faults, then regarding its “systematic integrity” it is suitable for applications in safety functions up to SIL 3. It fulfills a SIL claim limit SILCL = 3.

2.6 Designing and implementing safety-related parts of a control according to EN 954-1 (ISO 13849-1 (rev))

Objective: A safety-related (control) system must correctly execute a safety-related function. When a fault develops, it must respond so that the machine or plant either remains in a safe condition or is brought into a safe condition.

Determining the necessary Safety Performance (Safety Integrity)

The requirements placed on the safety-related functions are determined using the risk assessment process (refer to Chapter 2.3 “Does the protective measure depend on a control?”).
EN 954-1 defines a Category for the Draft and the follow-on (subsequent) Standard ISO 13849-1 (rev) specifies a required Performance Level PL_r. Also refer to Chapter 2.3 “Does the protective measure depend on a control?”.

Process to design the safety-related parts of a control

The categories according to EN 954-1 refer, to the same degree, to the system (safety-related function) and its subsystems (safety-related parts of a control). When implementing the control according to EN 954, the same principle of structuring the safety-related system can be applied as described in IEC 62061.

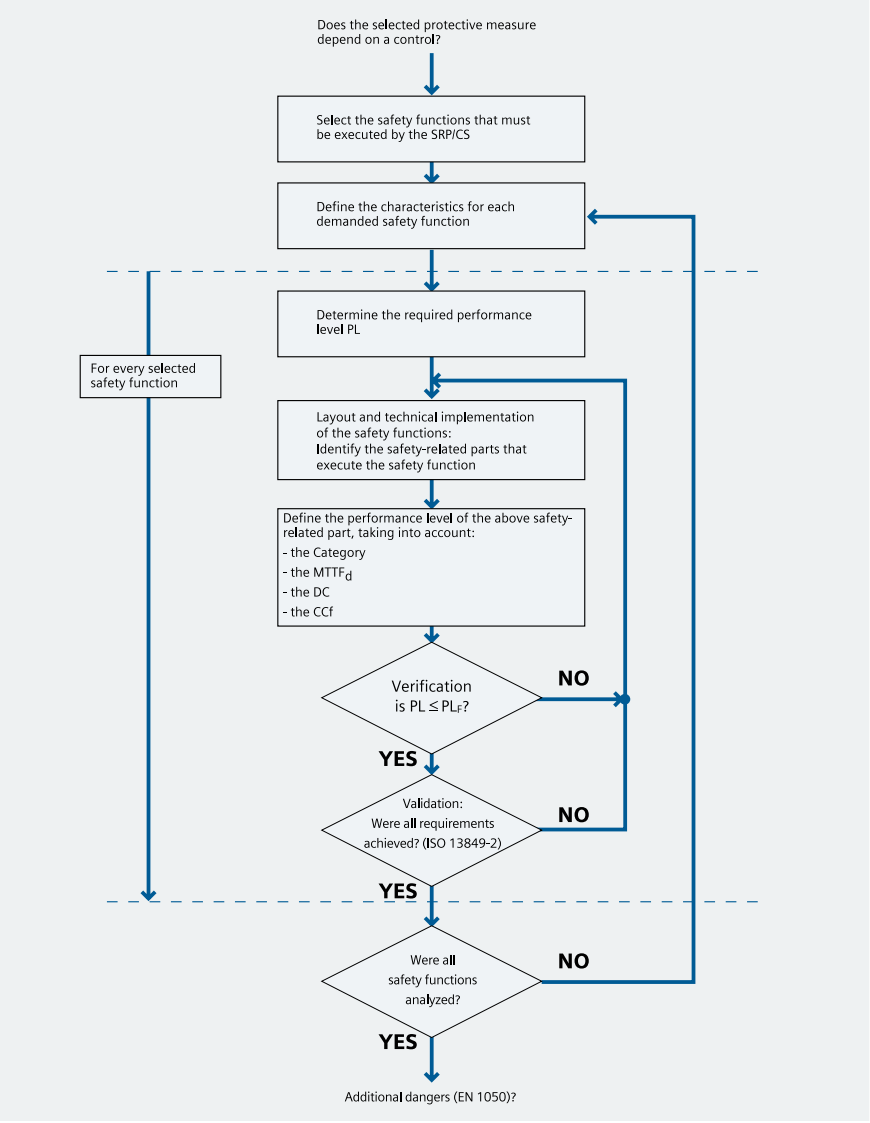


Fig. 2/24
Iterative process to design the safety-related parts of controls (SRP/CS)

Such a subsystem that is demarcated in such a way must then fulfill the Category that is specified for the protective function. The requirements of the associated category also apply for the wiring between these subsystems.

When compared with IEC 62061, for the Draft according to EN 954, a category is specified instead of SIL CL (SIL claim limit). The quantitative analysis of the probability of dangerous failures is eliminated.

On the other hand, in ISO 13849-1(rev), for the draft, in addition to the categories, the Performance Level PL_r is introduced as the quantitative level for the probability of failure.

The iterative process to design the safety-related parts of controls (SRP/CS) is shown in Fig. 2/24:

Implementing a safety-related function

The architecture depends on the Category required or the required Performance Level PL_r.

Draft according to EN 954

The Category of the system reached corresponds to the Category of the subsystems used.

The decisive basis in EN 954-1 is the fault detection and the fault control that can be implemented with one Category.
This is because only if a fault is detected, can a response be explicitly initiated: The quality of the fault detection defines the measure of the fault control and therefore implicitly defines the fault control measures (architectural draft).

Comment: If computer-based subsystems and bus communications are used, then these must fulfill a specific SIL acc. to 61508. In this case, the following assignment applies: A subsystem, suitable for SIL 1, can be used for Category 2 and appropriately, SIL 2 for Category 3 or SIL 3 for Category 4.

Draft according to ISO 13849-1 (rev)

The draft concept of ISO 13849-1 (rev) is based on special predefined architectures of the safety-related parts of the control.

A safety function can comprise one or several safety-related parts of a control (SRP/CS).

A safety-related function can also be an operating function, e.g. a two-hand circuit to initiate a process.

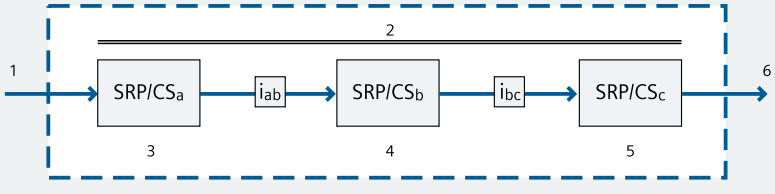
A typical safety-related function comprises the following safety-related parts of a control:

- Input (SRP/CS_a)
- Logic / processing (SRP/CS_b)
- Output / power transmission element (SRP/CS_c)
- Connections (i_{ab}, i_{ac}) (e.g. electrical, optical)

Comment: Safety-related components comprise one or several component(s); Components can comprise one or several element(s).

All connection elements are contained in safety-related parts.

If the safety functions of the control have been defined, the safety-related parts of the control must be identified. It is also important to assess their role in the process regarding reducing risk (ISO 12100).



1 Resource to initiate, e.g. manual input
2 Typical safety function (input, logic, output)
3 Input
4 Logic (processing)
5 Output
6 Machine actuator, shutdown device, brake(s)

Fig. 2/25
Arrangement of a typical safety-related function

Drafting and implementing categories

The requirements placed on the categories are shown simplified in ISO 13849-1(rev):

Category	Summary of requirements	System behaviour	Principles to achieve safety	$MTTF_d$ of each channel	DC_{avg}	CCF
B (see 6.2.1)	SRP/CSs and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterised by selection of components	low to medium	none	not relevant
1 (see 6.2.2)	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B.	Mainly characterised by selection of components	high	none	not relevant
2 (see 6.2.3)	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.	Mainly characterised by structure	low to high	low to medium	see Annex F
3 (see 6.2.4)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that: – a single fault in any of these parts does not lead to the loss of the safety function, and – whenever reasonably practicable the single fault is detected.	When a single fault occurs the safety function is always performed. Some but not all faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterised by structure	low to high	low to medium	see Annex F
4 (see 6.2.5)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that: – a single fault in any of these parts does not lead to a loss of the safety function, and – the single fault is detected at or before the next demand upon the safety function. If this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterised by structure	high	high including the accumulation of faults	see Annex F

NOTE For full requirements see Clause 6.

Category 3 in Appendix B of ISO 13849-1(rev) is listed here as example of a designated architecture:

- I1 and I2: Sensors 1 and 2 (e.g. two position switches with positively opening contacts)
- L1 and L2: Logic units 1 and 2 (one safety relay e.g. already includes these two units)
- O1 and O2: Actuator 1 and 2 (e.g. two contactors)

The structural features include:

- A redundant structure
- Monitoring sensors (discrepancy monitoring)
- Monitoring enable circuits (monitoring, comparable with the feedback circuits today)

Today, this architecture is already implemented in practice when applying EN 954-1.

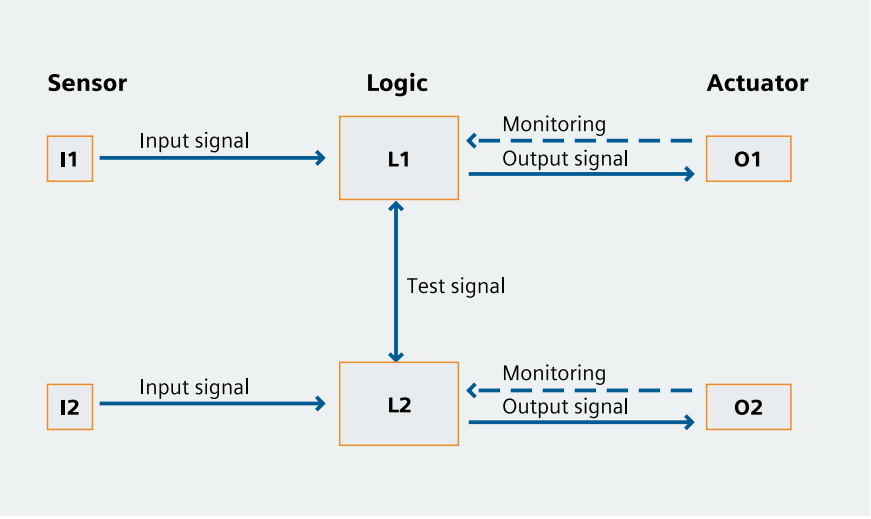
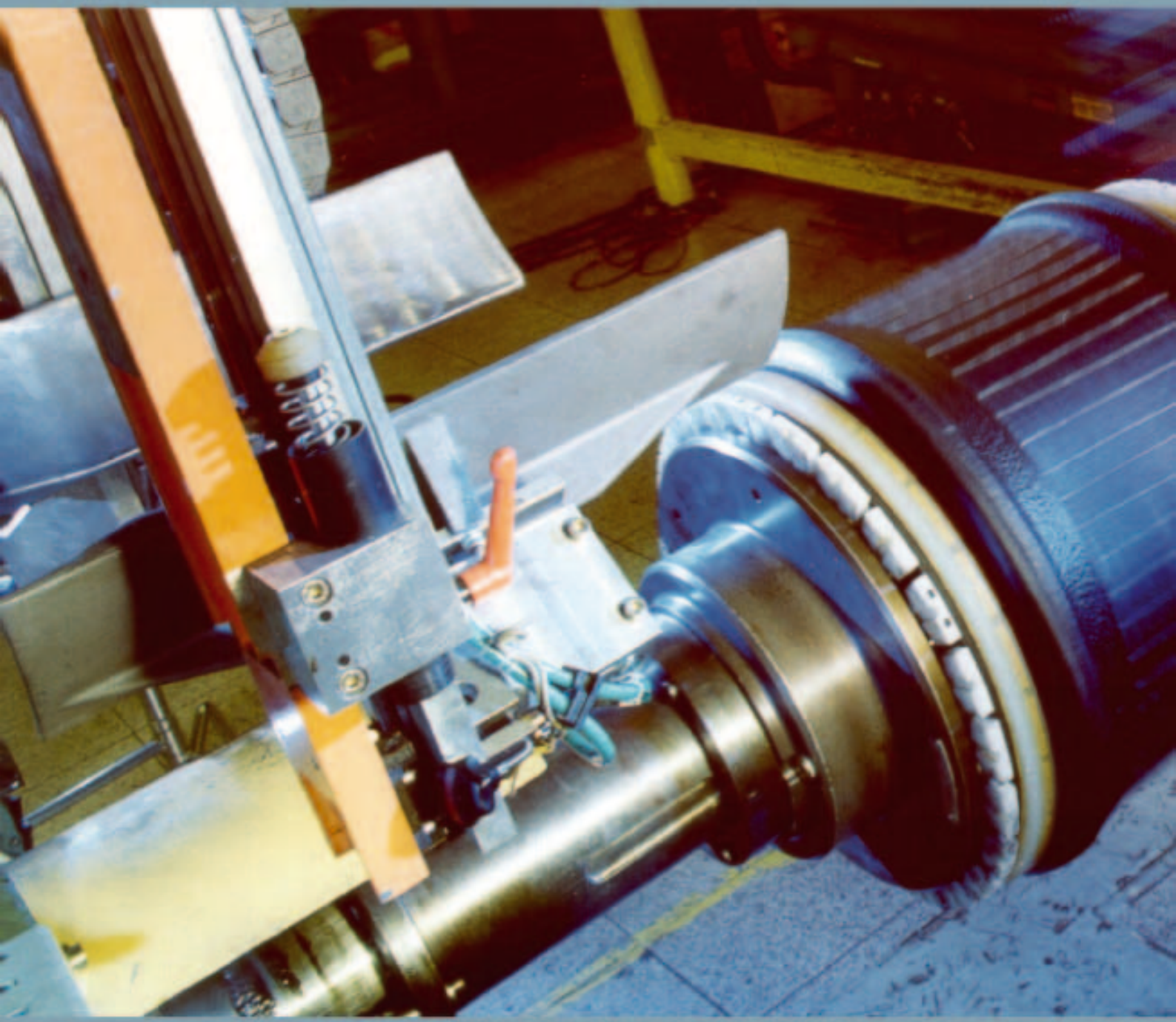


Fig. 2/26
Architecture for Category 3 acc. to ISO 13849-1(rev)

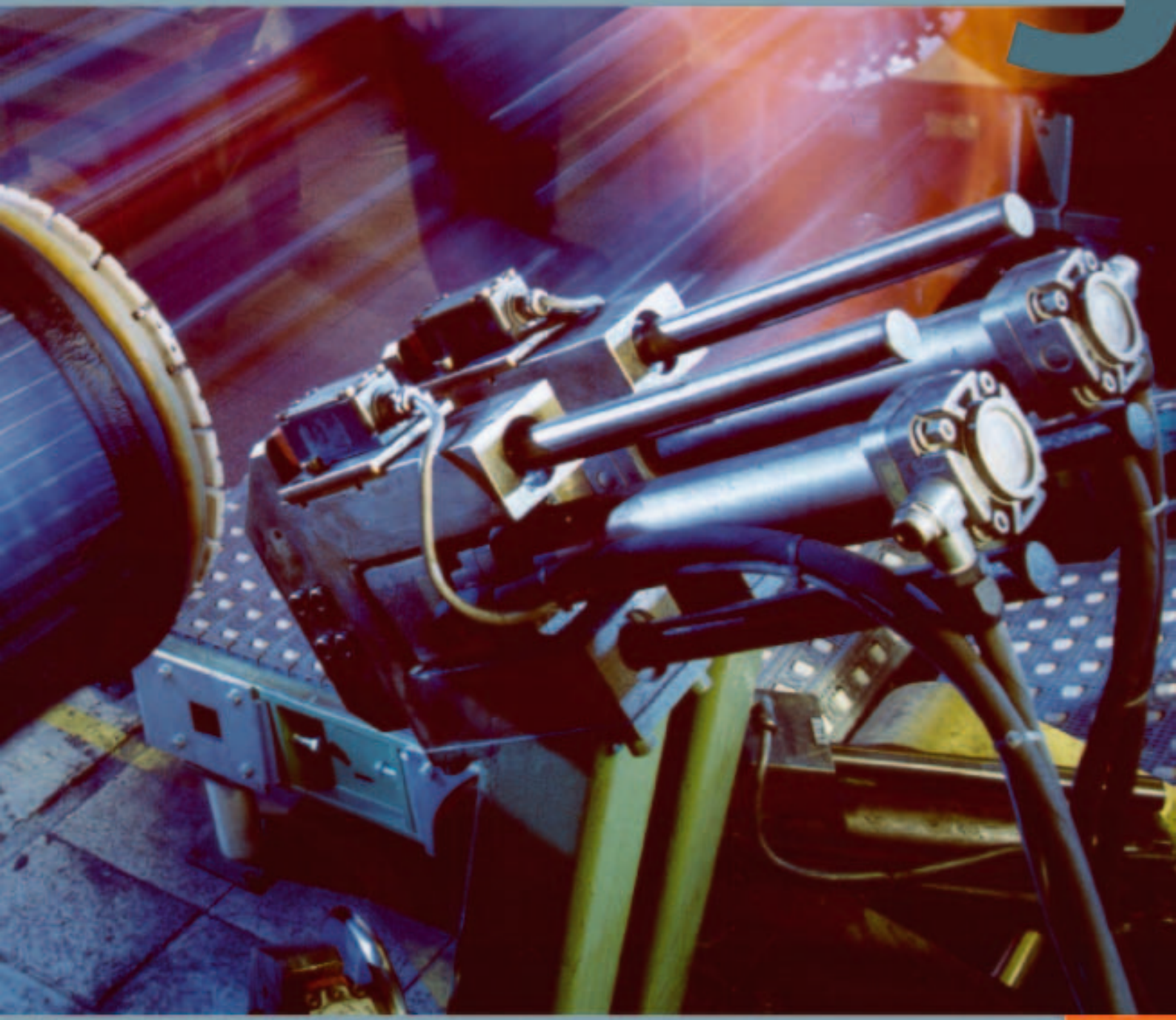
2.7 Specification and design of safety-relevant controls for machines in the United States.

Regulations and guidelines are covered in RIA 15.06:1999, ANSI B11.19, B11.TR-3 and B11.TR-4 for example. You will find informational only references to the IEC, ISO, and EN standards in the appendix section of these regulations.



Connecting sensors/actuators

3



3 Connecting sensors/actuators

3.1 Overview

This chapter on connecting sensors and actuators shows how the individual components are combined to form a complete system.

This is based on the three areas:

Detecting, evaluating and responding

Detecting means to input safety-related signals from e.g. Emergency Stop command devices or light curtains in a safety-related evaluation unit.

The safety evaluation unit - e.g. S7 F-CPU, SINUMERIK 840D Safety Integrated, ASIsafe safety monitor, Safety Unit or 3TK28 safety relays - process these signals, handle the necessary fault detection and output their signals corresponding to their shutdown logic to provide the appropriate response.

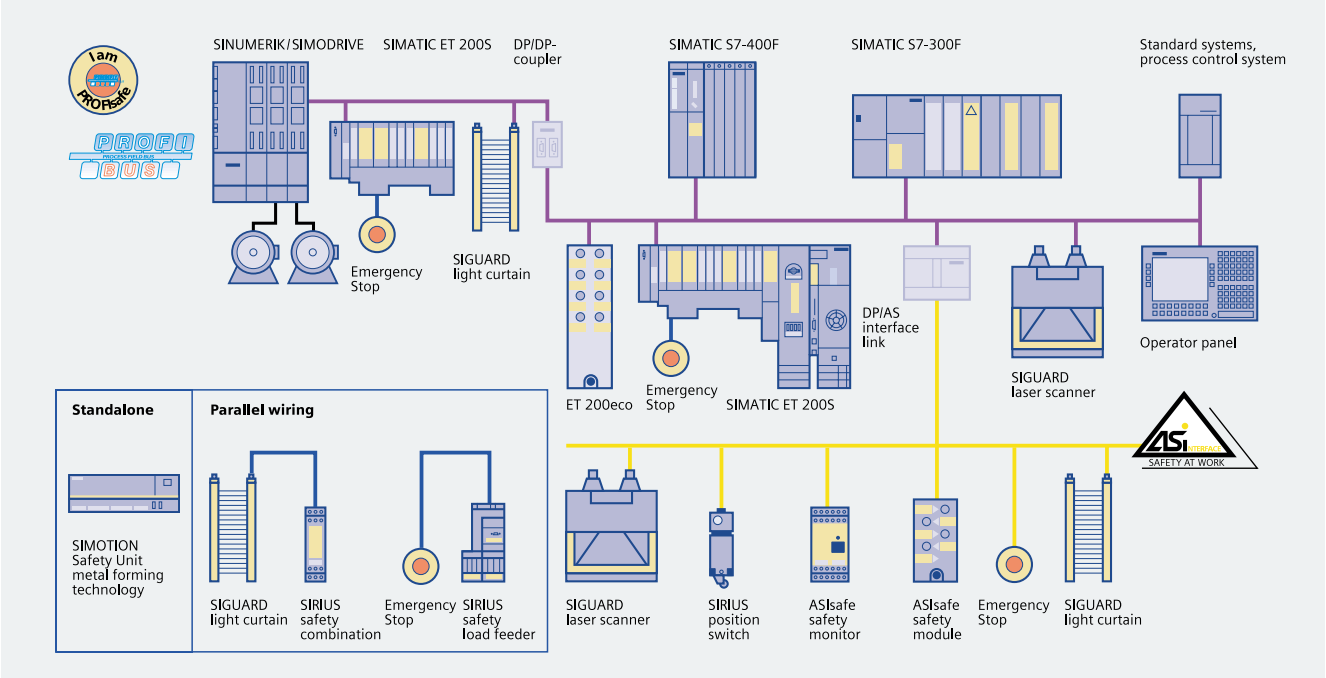
The response is realized using internal or external switching elements (actuators).

The examples shown here are of a general nature so that users can find a solution - independent of the selected evaluation unit - and then implement this in a way that suits them.

A selection of circuits that are usually used is shown in this Chapter.

In practice, other possibilities exist.

A selection of the most generally used circuit examples is shown.



3.2 Features

Sensors and actuators are connected to various evaluation units.

The following versions are possible when using Safety Integrated:

Conventional solution

- SIRIUS Safety Integrated
  - 3TK28.. safety relays
  - 3RA7.. safety load feeders
  - 3RG7848.. safety evaluation units for optical safety-related sensors

Bus-based solutions

ASIsafe

- SIRIUS Safety Integrated
  - 3RK11.. safety monitor
  - K45F and K60F compact modules (IP67)
  - Directly connecting electro-mechanical sensors (IP67)
  - Slimline modules S22.5F (IP20)
- Optical safety sensors are directly connected

PROFIsafe

- SIMATIC Safety Integrated
  - CPU S7-300 F
  - CPU S7-400 F
  - ET 200S, ET 200M and ET 200eco I/O
- SIRIUS Safety Integrated
  - ET 200S Motorstarter
- SINUMERIK
  - Via separate input/output hardware I/O from the PLC and NC or via PROFIsafe with the ET 200S and ET 200eco I/O modules together with the SINUMERIK 840D/ SIMODRIVE 611D control
- Optical safety sensors are directly connected

Possible sensor versions

1. NC/NC contacts (equivalent) → (positively-opening contacts)
This version is mainly used to shut down - e.g. for an Emergency Stop or protective door monitoring.

2. NO/NO contact (equivalent)
The version is predominantly used to power-up, e.g. for setting-up operation.

3. NC/NO contacts (non-equivalent)
The version is predominantly used to shut down and power-up, e.g. two-hand operator control

3.3 Standards - an overview

The information regarding standards, listed in this Chapter, is discussed in detail in Chapters 1 and 2.

EN 954-1

The necessary behavior of safety-related parts of a control regarding their resistance to potential dangers (fault detection, fault control) are described in Categories (B, 1 to 4).

ISO 13849-1 (rev.)

EN 954-1 is presently being revised in a Draft "ISO 13849-1 (rev.)" . The following new points in EN 954-1 "Safety of machinery - safety-related parts of controls": 1996 were recommended:

- The term "Performance Level" uses failure probabilities similar to SIL acc. to IEC 61508. This means that ISO 13849-1 also contains a quantified and hierarchic graduation of the Safety Performance: Instead of the deterministic approach of EN 954-1 - probabalistic methodology is now also introduced.
- Categories 1 to 4 will be supplemented by additional calculations to determine failure probabilities with a Performance Level (PL).

The design concept of ISO 13849-1 (rev.) based on special pre-defined architectures of "safety-related parts of the control" (in the informative Annex B as "designated architecture").

More detailed information of the concept according to ISO 13849-1 (rev.) will not discussed here as this is presently still being revised.

IEC 61508

IEC 61508 "Functional safety of safety-related electrical, electronic, programmable electronic systems" is the Standard on which IEC 62061 is based.

IEC 62061

IEC 62061 "Safety of machines - functional safety of electrical, electronic and programmable controls of machines" is considered as "state-of-the-art technology" and mainly concentrates on the requirements that the machinery construction OEM must fulfill when designing and implementing safety-related electrical controls.

It describes how a system is configured using existing subsystems and how the achieved Safety Performance can be determined: SIL, Safety Integrity Level, is used as a measure for the Safety Performance.

The SIL claim limit restricts itself to the achievable SIL of the system (safety-related function) although the "Random Integrity (safety integrity of poten-

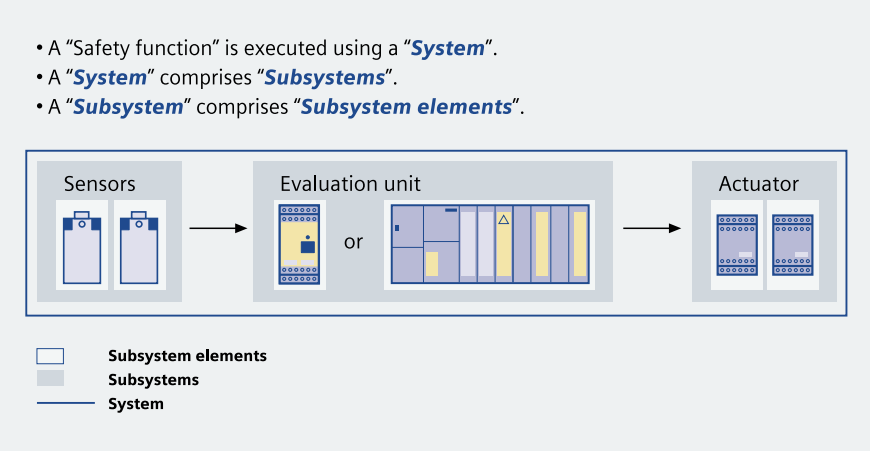


Fig. 3/1
System, subsystem, and subsystem elements according to IEC 62061

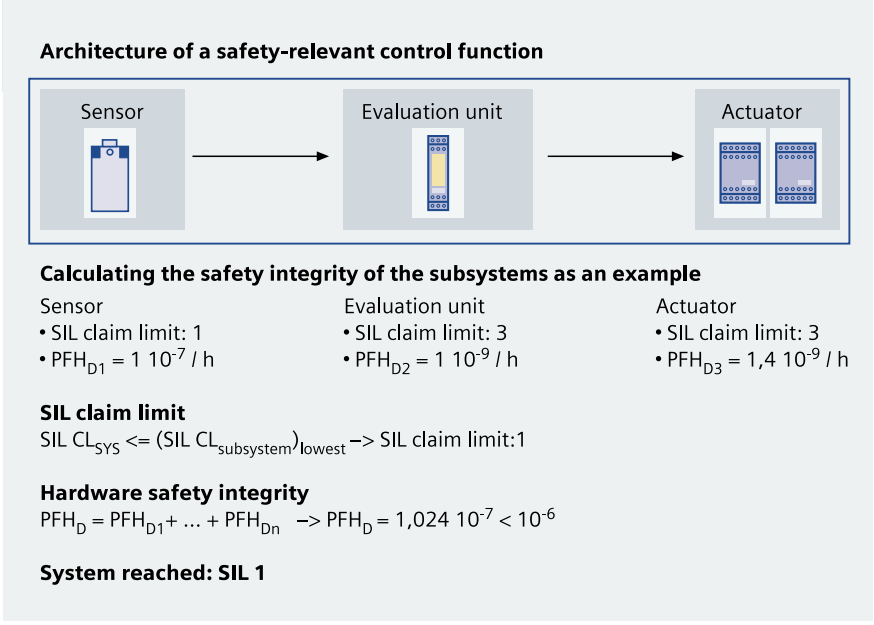


Fig. 3/2
Application example for an application according to IEC 62061

tially dangerous, random hardware failures)" achieves SIL 2.

The application in Fig. 3/2 comprises the following subsystems:

- Detecting (a position switch, 1-channel)
- Evaluating (3TK28.., with diagnostics)
- Responding (two contactors)

The PFH$_D$ values that are used in the calculation are only an example and do not represent actual values.

Principle approach when applying IEC 62061:

- The **1st requirement (SIL suitability claim limit of the subsystems)** limits the achievable Safety Performance of the system.

  SIL$_{SYSTEM}$ <= SIL$_{CLlowest}$

Every subsystem is only suitable up to a specific SIL as result of its systematic properties and features. This value limits the possible SIL of the system (weakest link in the chain).

- The **2nd requirement (hardware safety integrity)** is the limit of the probability of "dangerous faults" for the complete safety-related function; this means that the sum of all of the failure probabilities of all of the subsystems may not exceed the PFH$_D$ of the required SIL.

The failure probability of the contactors (the electro-mechanical subsystem "actuator") is defined using a simplified calculation with the B10 values according to IEC 62061.

The following equation applies for the system:

PFH$_{D(system)}$ = PFH$_{D(detecting)}$ + PFH$_{D(evaluating)}$ + PFH$_{D(responding)}$ + P$_{TE}$ <= required failure probability of the system

For safety-related communications, the probability of possible data transfer errors (P$_{TE}$) must be added.

- The **3rd request (selection and interconnection)** - when selecting and interconnecting the subsystems, the appropriate requirements of IEC 62061 6.4 must be fulfilled - "requirements relating to systematic safety integrity".

3.4 Connecting sensors/actuators

General information

Principle, Category B acc. to EN 954-1

The safety-related parts of machine controls and/or their protective devices and their components must be designed, constructed and selected in compliance with the applicable Standards so that they can withstand the ambient effects that are expected.

With the continually increasing intermeshing and globalization of the economy, a specific minimum standard is defined in the EU Economic Community with Category B.

Requirement

The control must be designed so that it can withstand the ambient effects that are to be expected.

System behavior

A fault that occurs can result in the loss of the safety-related function.

Principle

Achieving the level of safety is especially characterized by the selection of components, e.g. protected against spray water, protected against dust, protected against vibration etc.

Principle, Category 1 acc. to EN 954-1

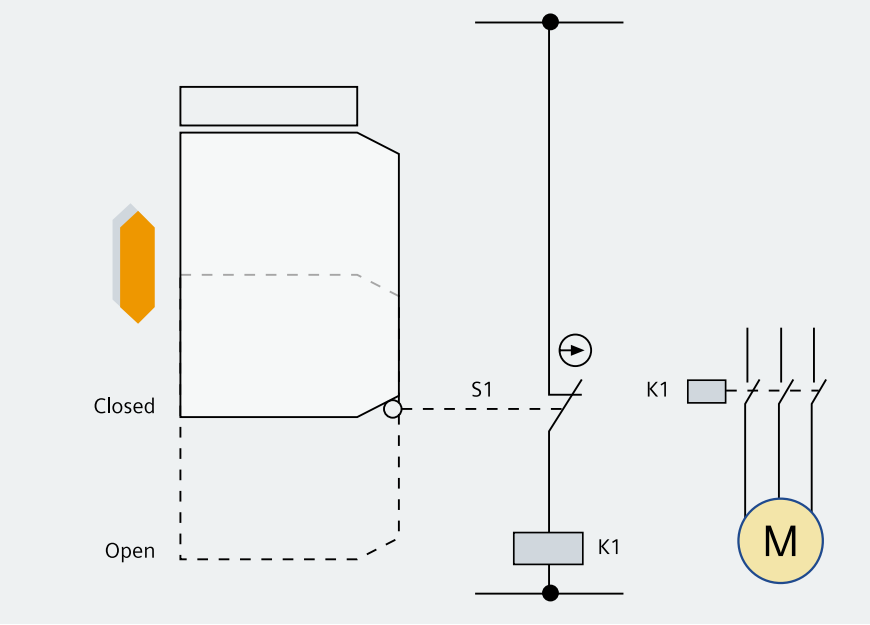


Fig. 3/3
Principle, Category 1 acc. to EN 954-1 using a protective door monitoring function as an example

Description and additional information

Requirement

The requirements of B must be fulfilled; in addition, safety-related, proven components and principles must be applied. A component has proven itself if, in the past it was widely used with successful results.

System behavior

The occurrence of a fault can result in loss of the safety-related function. The probability of a failure in Category 1 is lower than in Category B.

Principle

Selecting components
Sensors: e.g. acc. to EN 954-1
Actuators: “proven components” (e.g. contactors/circuit-breakers)

Principle, Category 2 acc. to EN 954-1

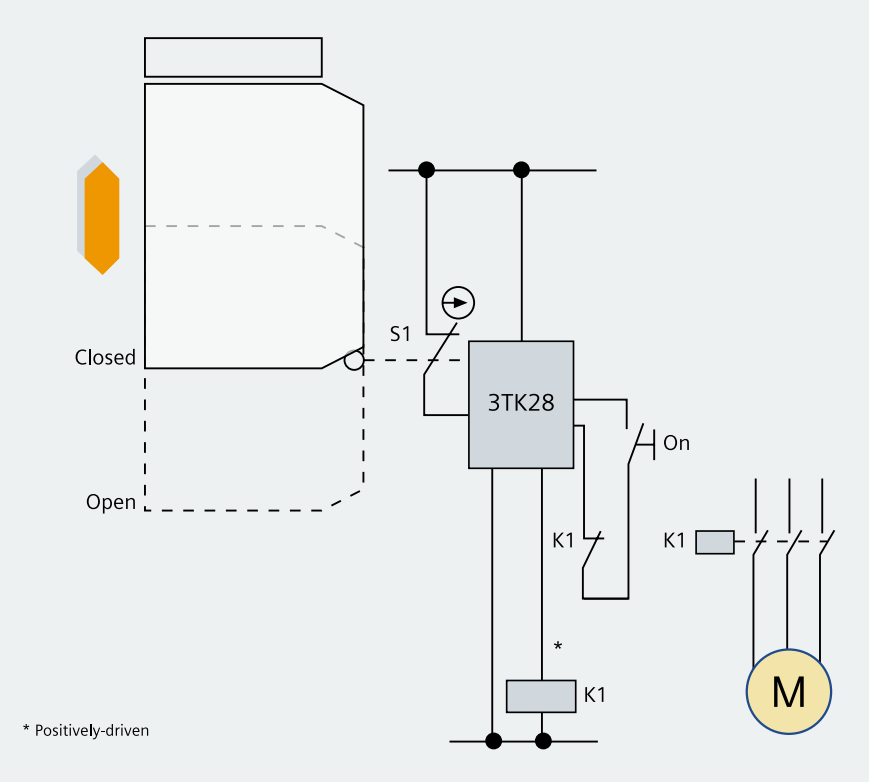


Fig. 3/4
Principle, Category 2 acc. to EN 954-1 using a protective door monitoring function as an example (the "machine control" is a standard PLC)

Using this example, Category 2 acc. to EN 954-1 can only be fulfilled, if, when the actuator fails, an alarm is automatically issued or the machine control initiates that the machine goes into a safe condition. Otherwise, a second shutdown path is required.

Principle

Structure of the control
Fault detection: e.g. using a 3TK28 safety relay or a fail-safe control (F control)
Sensors: e.g. acc. to EN 954-1, or IEC 60947-5-1
Actuators: "Proven components" (e.g. contactors)

Description and additional information

Requirement

The requirements of B and the use of proven safety principles must be fulfilled. Additional checks of the safety function must be carried-out at suitable intervals (e.g. by sporadically opening the protective door).

System behavior

The occurrence of a fault can result in the loss of the safety function between the checking intervals. The check detects that the safety function has been lost. If a fault is detected, then a safe condition must be maintained until the fault has been removed.

Principle, Category 3 acc. to EN954-1

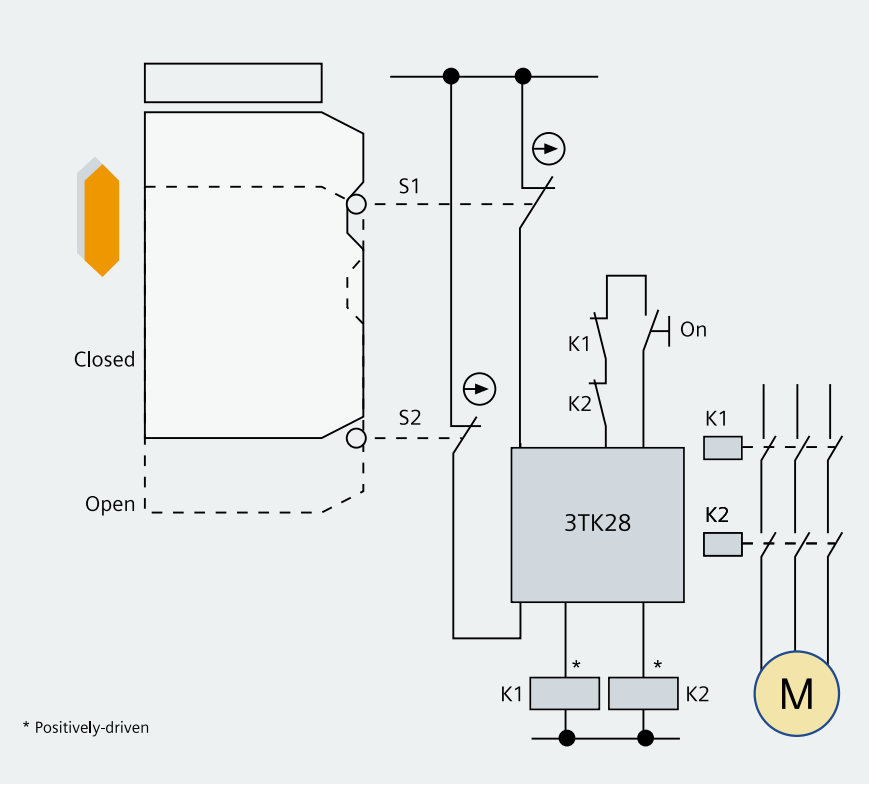


Fig. 3/5
Principle, Category 3 acc. to EN 954-1 using a protective door monitoring function as an example

Description and additional information

Requirement

The requirements of B and the use of proven safety components must be fulfilled. In Category 3, all safety-related parts must be designed so that a simple fault cannot result in the loss of the safety function. The single fault must be detected the next time that the safety function is called on. This requirement can, e.g. be achieved with redundancy (refer to Fig. 3/5).

System behavior

If a single fault occurs, the safety function is always maintained. Several, but not all faults will be detected. An accumulation of undetected faults can result in the loss of the safety function.

Principle

Control structure
Fault detection: e.g. using a 3TK28 safety relay or a fail-safe control
F-control
Sensors: Redundantly configured
Actuators: Redundantly configured

Principle, Category 4 acc. to EN 954-1

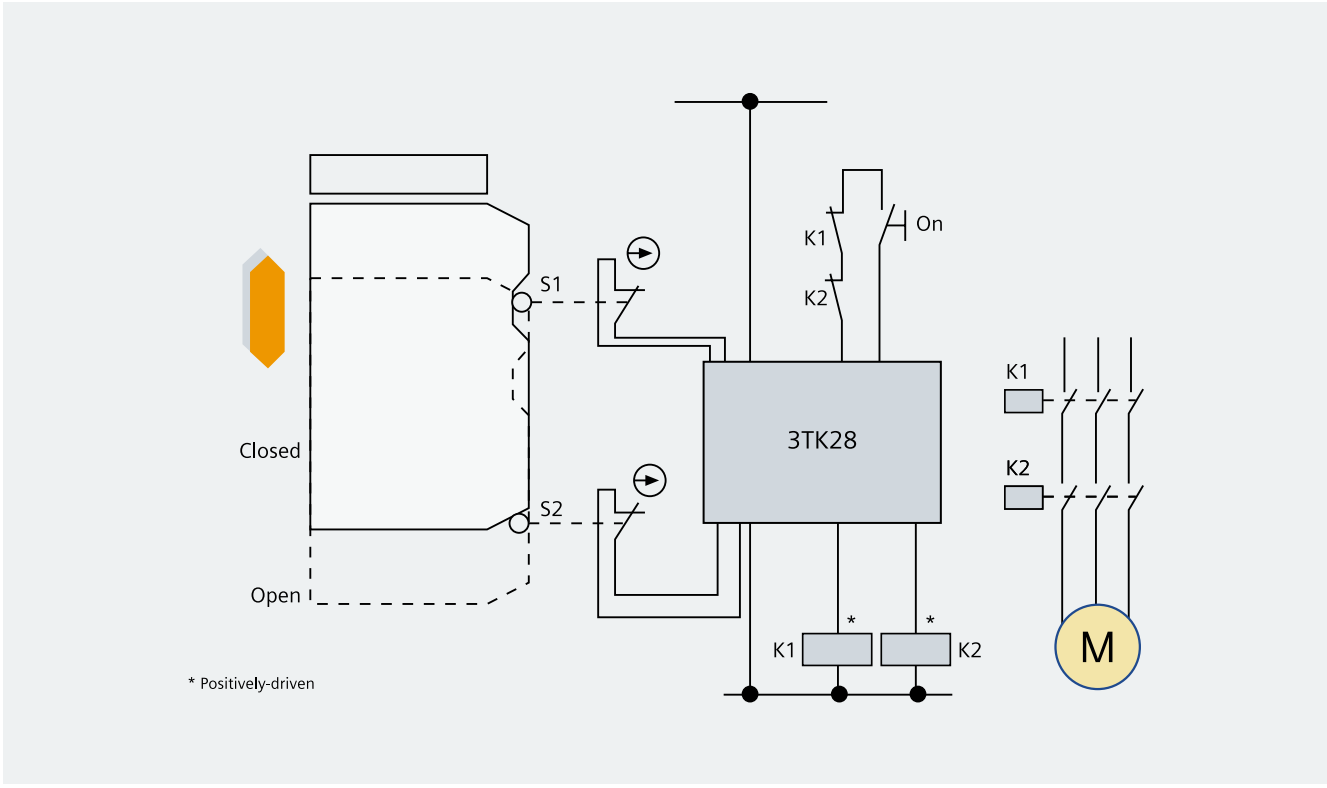


Fig. 3/6
Principle, Category 4 acc. to EN 954-1 using a protective door monitoring function as an example

Requirement

The requirements of B and the use of proven safety principles must be fulfilled.

Safety-related parts, according to Category 4, must be designed so that a single fault in each of these parts does not result in the loss of the safety function; and the single fault is detected at or before the next time that the safety function is called on - if this is not possible, an accumulation of faults may not result in loss of the safety function. Further, faults with a common cause must be taken into account, e.g. by preventing the effects of EMC.

System behavior

If faults occur, the safety function is always kept. The faults are detected in sufficient time in order to prevent loss of the safety function.

Principle

Structure of the control
Fault detection: For example, using a 3TK28 safety relay or a fail-safe control (F control) and additional monitoring, cross-fault detection and monitored start.
Sensors: Redundantly implemented and clocked
Actuators: Redundantly implemented
If the level of safety is increased using additional measures, e.g. by over-dimensioning the load contactors, this does not result in a higher category!

This does not result in fault exclusion!

Manual, monitored start and autostart (EN 954-1, EN 60204-1)

Is possible with various safety-related components (subsystem evaluation).

A safety relay can either be manually started - which can be monitored - or automatically started.

For a manual or monitored start, an enable signal is generated by pressing the ON button, after the input image has been checked and after the safety relay has been successfully tested. This function is also known as static operation and is specified for Emergency Stop command devices (EN 60204-1, conscious action).

Contrary to a manual start, the monitored start evaluates the signal change of an ON button. This means that it is not possible to manipulate the operation of the ON button.

For an automatic start, an enable signal is generated without any manual agreement, but after the input image is checked and the safety relay successfully tested. The function is also known as dynamic operation and is not permissible for Emergency Stop equipment and command devices.

Mechanically isolating protective devices (e.g. guards that cannot be entered) operate with an automatic start.

Comment: A manual start can be implemented with a safety relay with automatic start, if, in addition to the positively-driven contacts of the load contactors, an ON button is connected in series in the feedback circuit (refer to Fig. 3/11).

A manual start is possible up to Category 3 according to EN 954-1.

A manual start is permissible for an Emergency Stop command device up to Category 3 according to EN 954-1 (ISO 13849-1 rev.).

For Category 4 a monitored start must be used.

For Category 4 according to EN 954-1 (ISO 13849-1 rev.), for an Emergency Stop command device, a monitored start is required: Unexpected starting must be absolutely excluded.

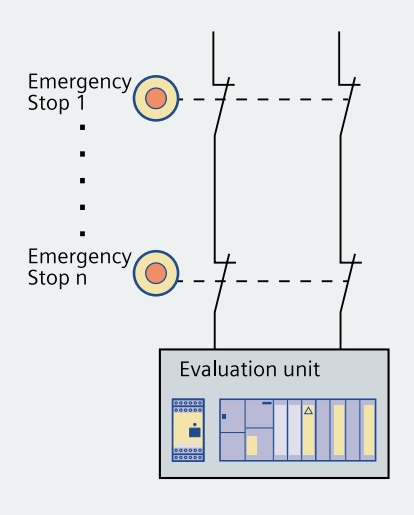


Fig. 3/7
Series circuit up to Category 4 acc. to EN 954-1 using an Emergency Stop monitoring function as an example

Description and additional information

Emergency Stop monitoring functions may always be connected in series: It can be excluded that when the Emergency Stop command device is pressed, that it simultaneously fails.

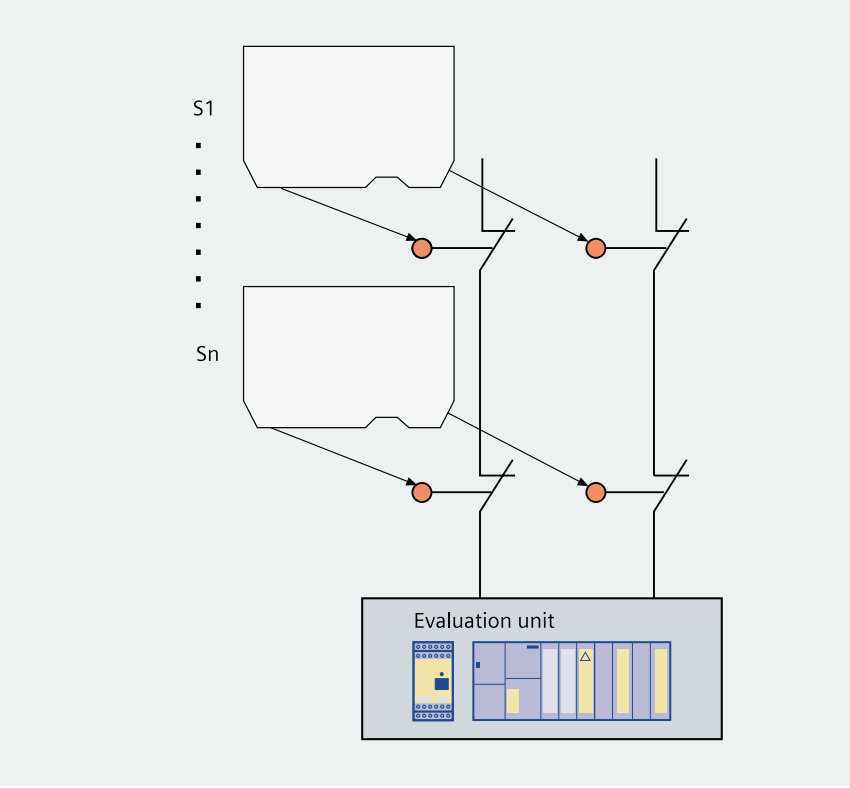


Fig. 3/8
Series circuit up to Category 3 acc. to EN 954-1 using the protective door monitoring function as an example

Description and additional information

- Up to Category 3 acc. to EN 954-1, position switches may be connected in series if several protective doors are not regularly and simultaneously opened (otherwise there would be no fault detection).
- For Category 4 acc. to EN 951-1, position switches may never be connected in series, because every dangerous fault must be detected (independent of operating personnel).

Safety-related (protected) routing, safety-related separation according to IEC 61140-1; EN 50187

- The objective is to achieve a high degree of operational safety. In order to protect against vagabond (parasitic) voltages, the various voltages along a cable or in a piece of equipment must be insulated against the highest voltage that may be present (protection against electric shock, IEC 61140).
- Between the AS Interface and V_{aux}, ASI modules must fulfill the requirements acc. to EN 50187 regarding air and creepage distances and the insulation voltage strength of the relevant components.

Conventionally connecting sensors without using safety-related communications via fieldbuses

Description and additional information

Mechanical switches such as Emergency Stop command devices, position switches or light curtains, light grids and laser scanners are used for **detection**.

SIRIUS 3TK28 safety relays are used to **evaluate** signals. The safety 3RA7 load feeder includes, in addition to the 3TK28 safety relay, redundant load contactors. These can safely shut down an actuator as single unit in Category 4 according to EN 954-1.

A **response** is directly implemented using discrete switching devices (contactors) or using PMD-Fxx modules in an ET 200S station in conjunction with motor starters (refer to Fig. 3/17) or frequency converters.

The application shown in Fig. 3/10 comprises the following subsystems:

- Detecting (two position switches each 1 channel)
- Evaluating (3TK28.., with diagnostics)
- Responding (two contactors)

The PFH_D values used for the calculation are only as an example.

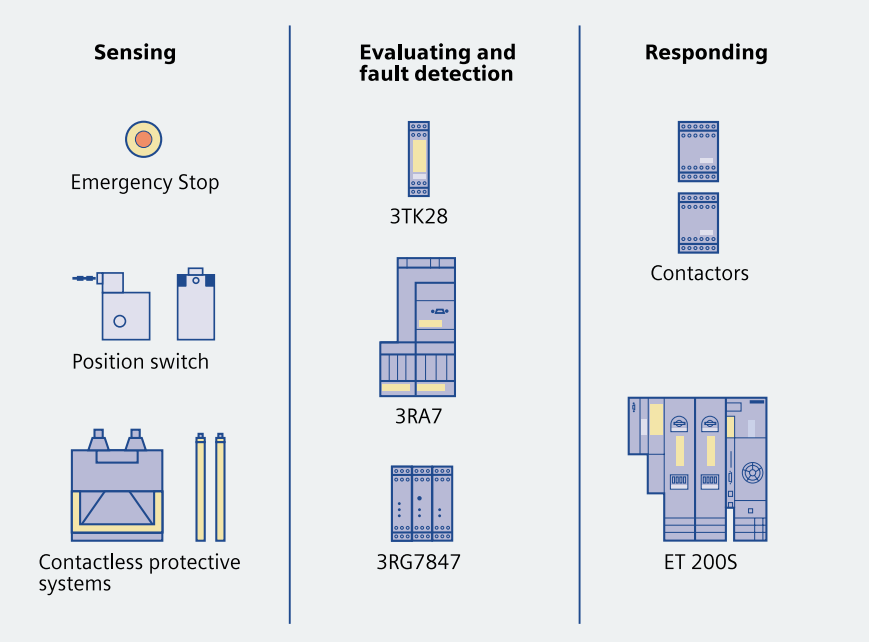


Fig. 3/9
Group diagram - directly connecting sensors (conventional)

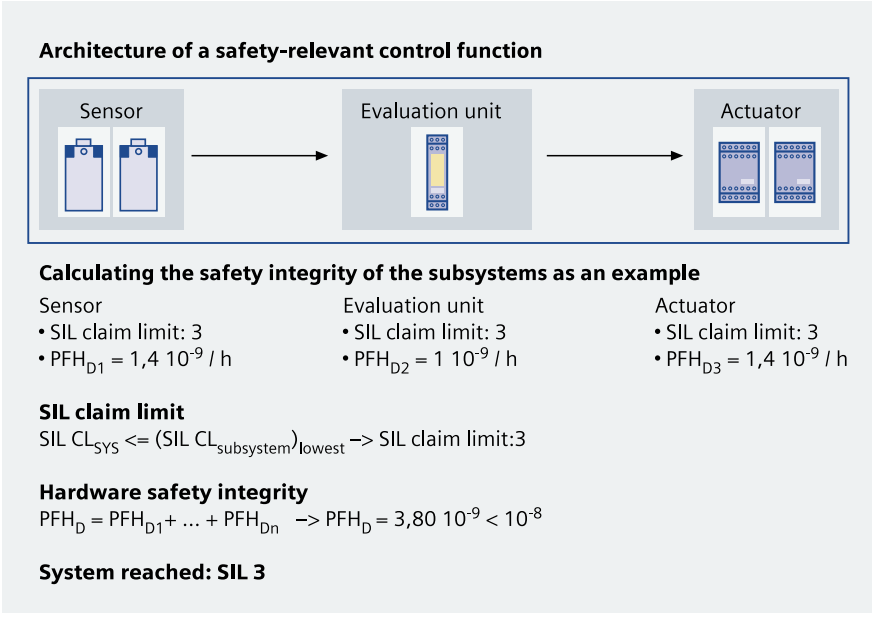


Fig. 3/10
Example of an application according to IEC 62061 that is conventionally connected without using safety-related communications

Connecting sensors/actuators without safety-related communication

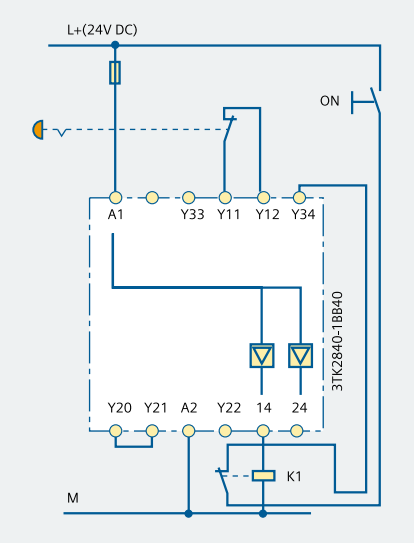


Fig. 3/11
SIRIUS 3TK2840, safety relay, Emergency Stop, Category 2 acc. to EN 954-1, single-channel with feedback circuit (the machine control is a standard PLC)

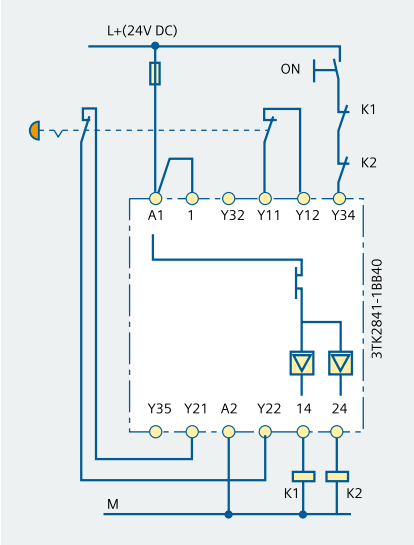


Fig. 3/12
SIRIUS 3TK2841 safety relay, Emergency Stop, Category 4 acc. to EN 954-1, two-channel with feedback circuit, monitored start with ON pushbutton

Description and additional information

- By actuating the "ON button" in the feedback circuit, the contactors K1 and K2 (actuators) are closed (energized).
  If the Emergency Stop command device is now actuated, the safety relay again opens (de-energizes) both contactors (actuators).

- For a Category 2 application, it is sufficient if the sensor (in this case, (the Emergency Stop command device) is evaluated through a single channel and the actuator (load contact) is controlled through a single channel.

- If a load contactor has a fault - e.g. because its contacts are welded - then the feedback circuit is not closed, even when pressing the ON button, and the 3TK28 does not enable its enable circuits (fault detection).

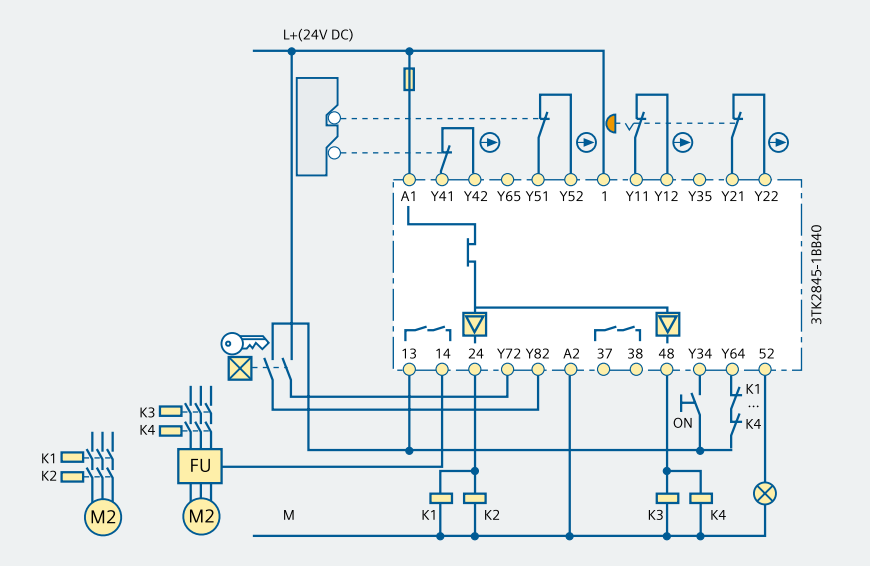


Fig. 3/13
Emergency Stop and protective door monitoring, Category 4 acc. to EN 954-1, with 3TK2845 in stop Category 0 acc. to EN 60204-1

Description and additional information

The following is implemented using the 3TK2845:

- Emergency Stop with monitored start
- Protective door monitoring with automatic start
- Key-operated switch that bypasses the protective door for service

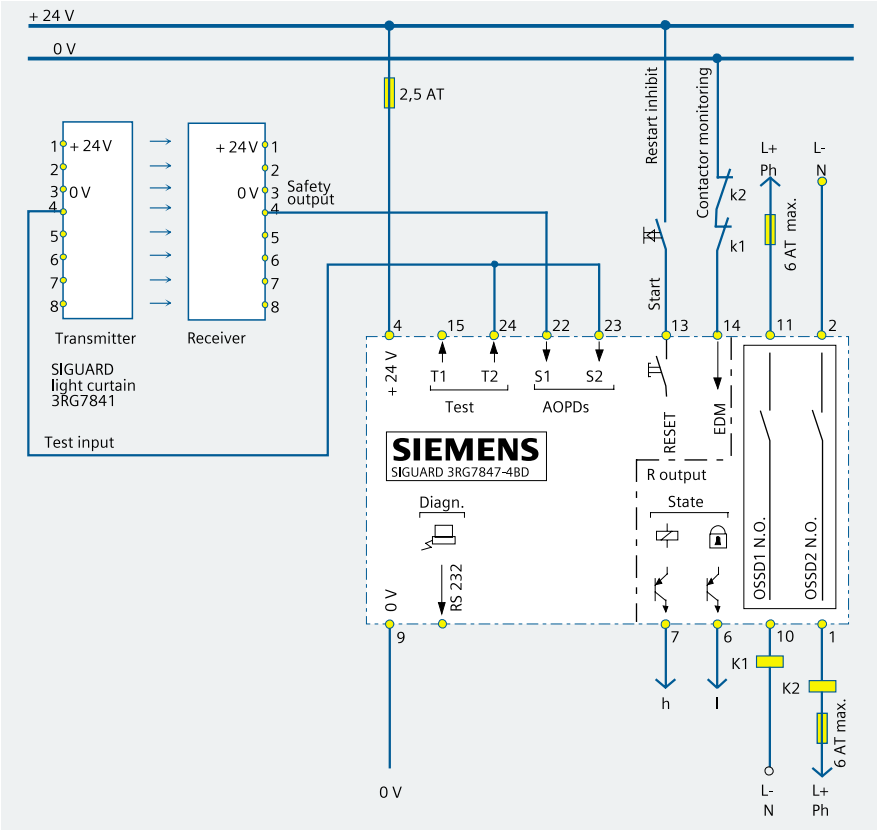


Fig. 3/14
SIGUARD 3RG7841.., light curtain monitoring, type 2 acc. to IEC 61496-1, 2 and EN 61496-1, 2, single-channel at the 3RG7847-4BD evaluation unit, manual start and feedback circuit

Description and additional information

- Sensor cables must be routed so that they are protected; only safety-related sensors with positively-opening contacts may be used as sensors.
- For type 2 protective devices, the protection function is periodically tested. The 3RG7847...evaluation unit is used to implement this test routine.

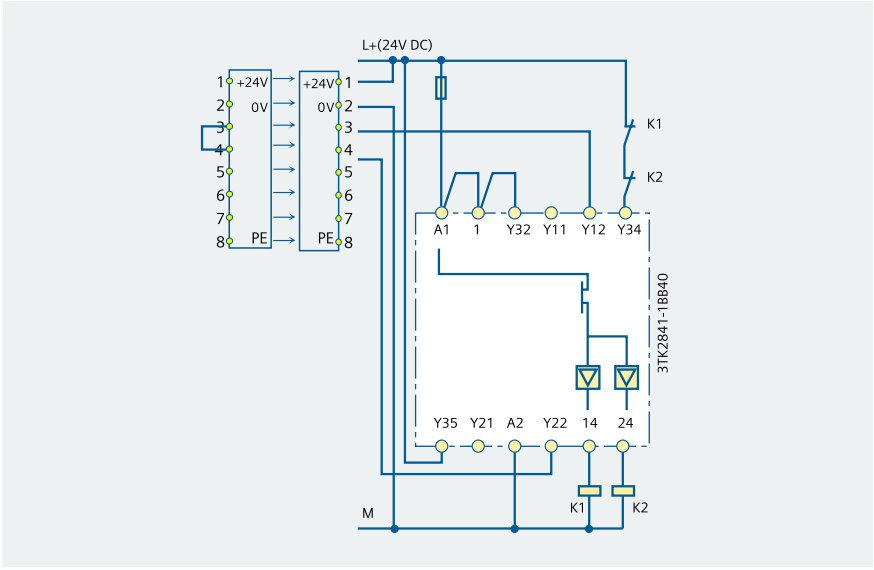


Fig. 3/15
SIGUARD 3RG7842.., light curtain/grid monitoring, type 4 acc. to IEC 61496-1, 2, two-channel connected to a SIRIUS 3TK284.., stop Category 0, acc. to EN 60204-1, autostart and feedback circuit

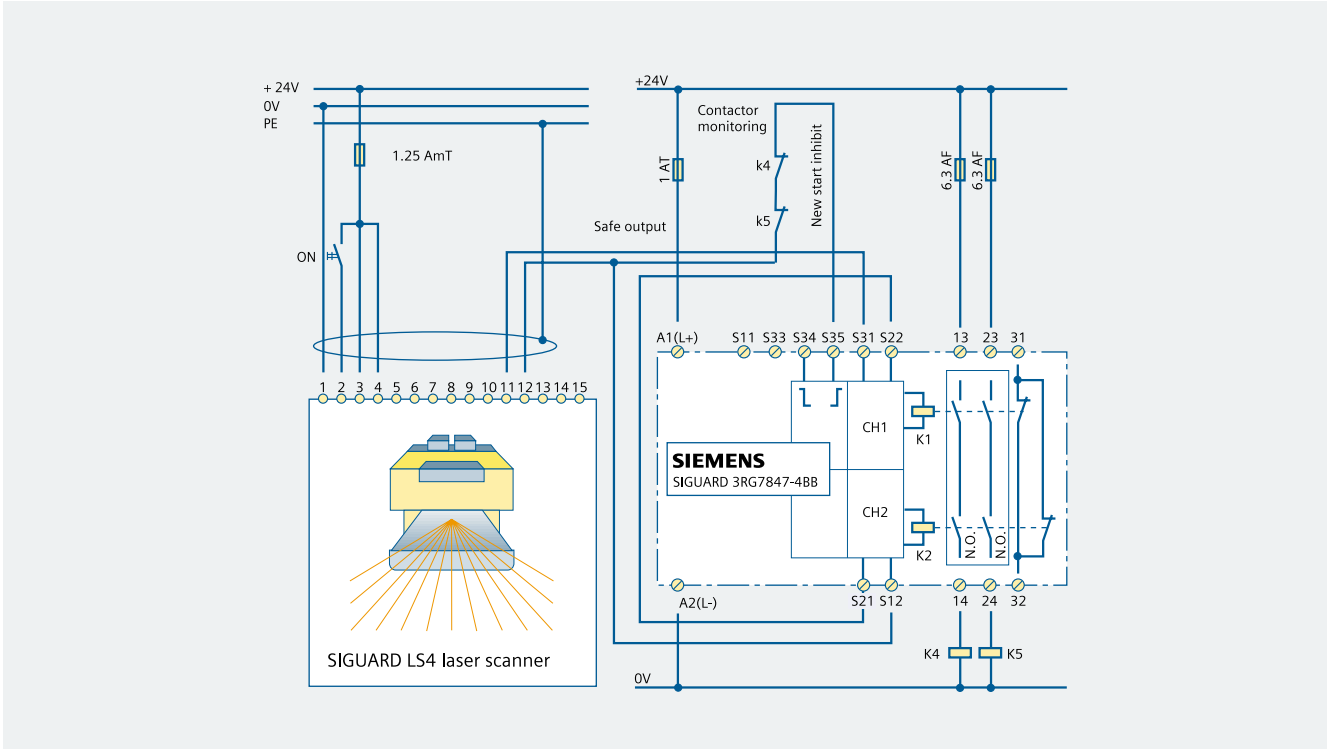


Fig. 3/16
SIGUARD LS4 laser scanner, type 3 acc. to IEC 61496-1, 2 or EN 61496-1, 2 two channel, connected to a 3RG7847-4BB, (evaluation unit) laser scanner configured for manual start, feedback circuit monitoring using a 3RG7847-4BB

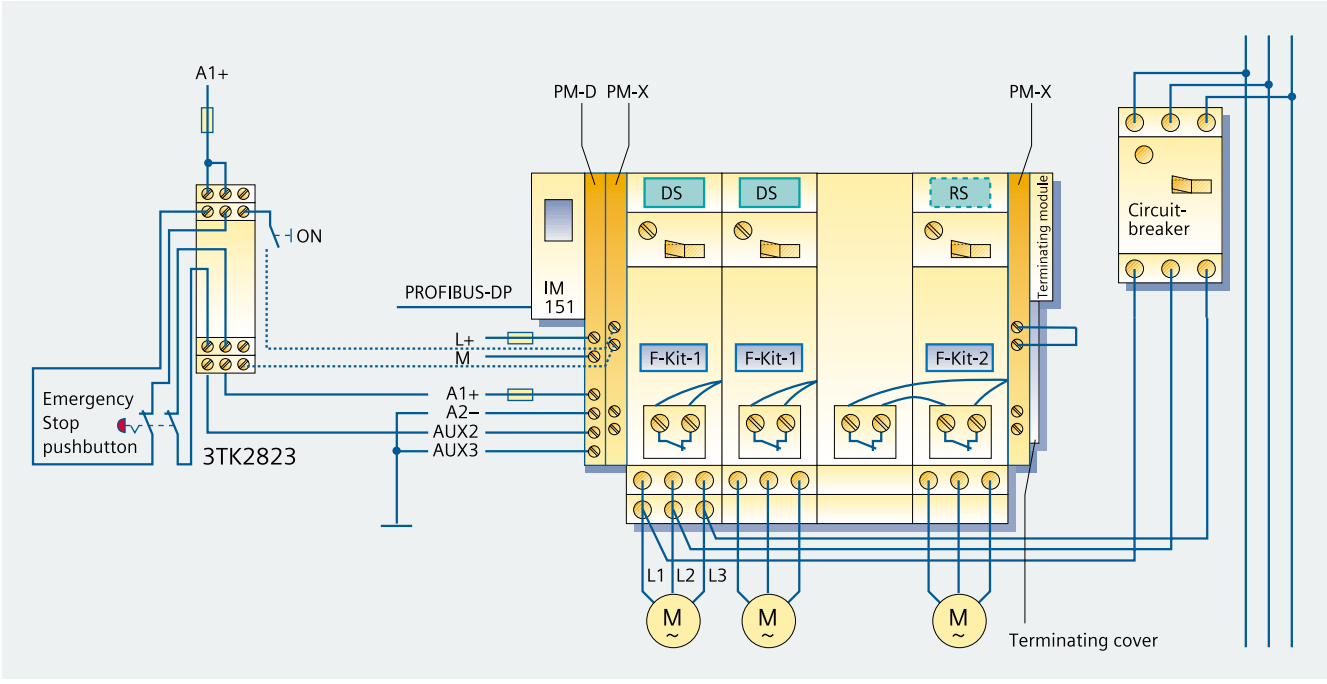


Fig. 3/17
ET 200S Motorstarter Solution Local with external Emergency Stop monitoring, Category 2 acc. to EN 954-1

Description and additional information

- If the Emergency Stop pushbutton, connected through two channels at the 3TK2823 is operated, then the actuators are shut down. This is realized by the 3TK2823 shutting down the motor starter supply voltage via the PMD module. In this case, safety is guaranteed by the 3TK2823.
- The two PM-X modules and the F kits are required to evaluate and monitor the feedback circuit.
- The 3TK2823 evaluates the feedback circuit.

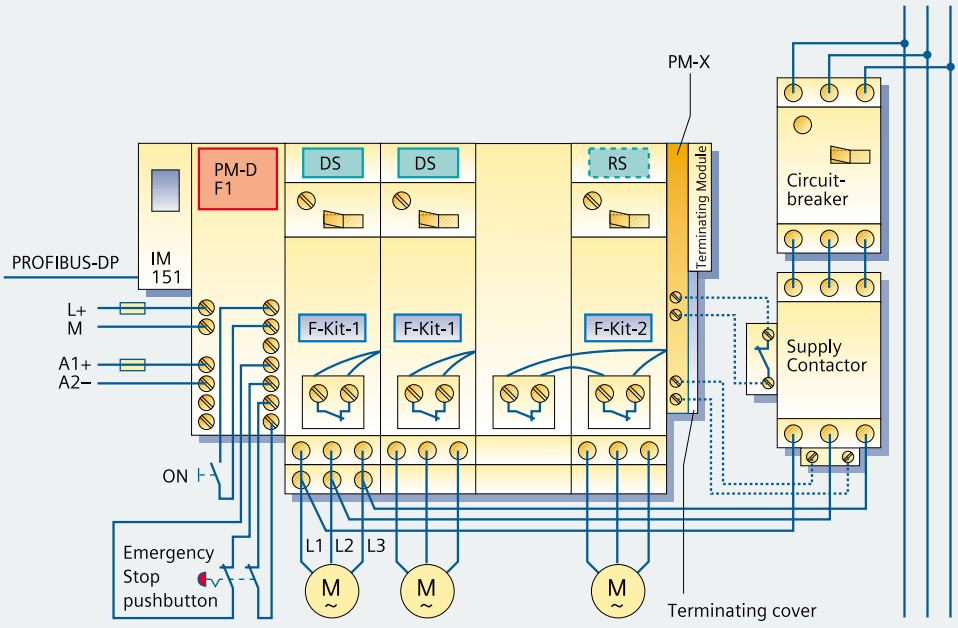


Fig. 3/18
ET 200S Motorstarter Solution Local – Emergency Stop monitoring with monitored start, Category 4 acc. to EN 954-1

Description and additional information

- If the Emergency Stop pushbutton, connected through two channels to the PM-D F1 is pressed, then the actuators are shut down. This is realized by PM-D F1 shutting down the supply voltage for the motor starter. The second shutdown path, required for Category 4 in accordance with EN 954-1, is implemented using an additional supply contactor.
- If the supply contactor is not opened, then this application is in compliance with Category 2, (also refer to Fig. 3/17). The feedback circuit is closed with the PM-X module and the F kits. The PM-X module also provides the terminals (control and feedback contact) for the supply contactor.
- The PM-D F1 module evaluates the feedback circuit.

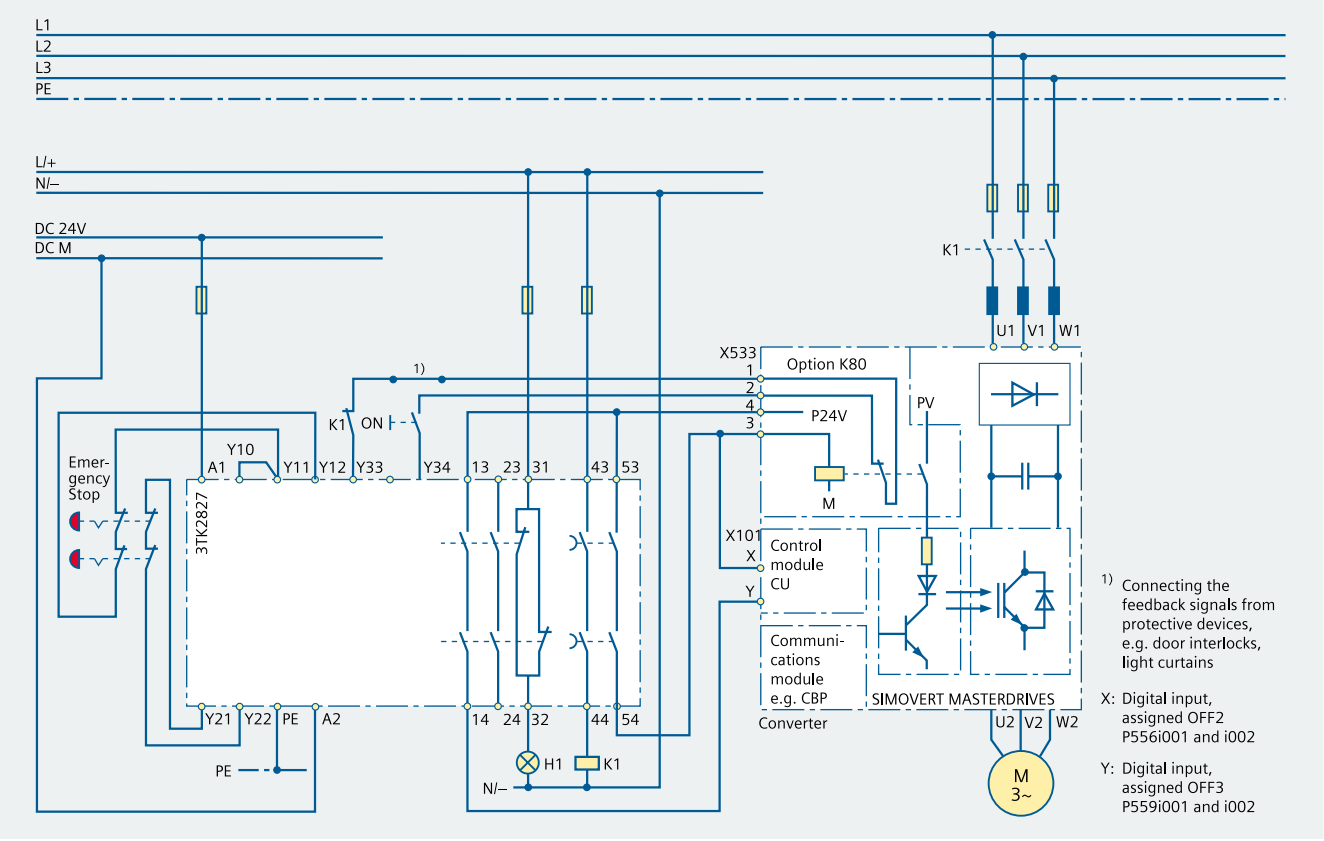


Fig. 3/19
SIMOVERT MASTERDRIVES stop Category 1, acc. to EN 60204-1, Category 3 acc. to EN 954-1; Safe standstill function with controlled drive stopping

Description and additional information

- Using this solution, for a MASTER DRIVES unit, the safe standstill with controlled motor stopping at the torque limit is implemented in conjunction with a safety relay.
- When the Emergency Stop pushbutton is pressed, then the fastest possible braking of the drive is initiated at the frequency converter using the instantaneous (non-delayed) contact of the safety relay.
- After the time, set at the safety relay has expired, the line contactor and the integrated drive relay drop out via the delayed contact. The drive is protected against undesirable restarting through two channels.
- If, due to a fault, the line contactor or the integrated relay had not dropped-out, then the safety relay cannot be switched-in again and the fault is detected (also refer to Fig. 3/47).

Connecting to AS-Interface with ASIsafe

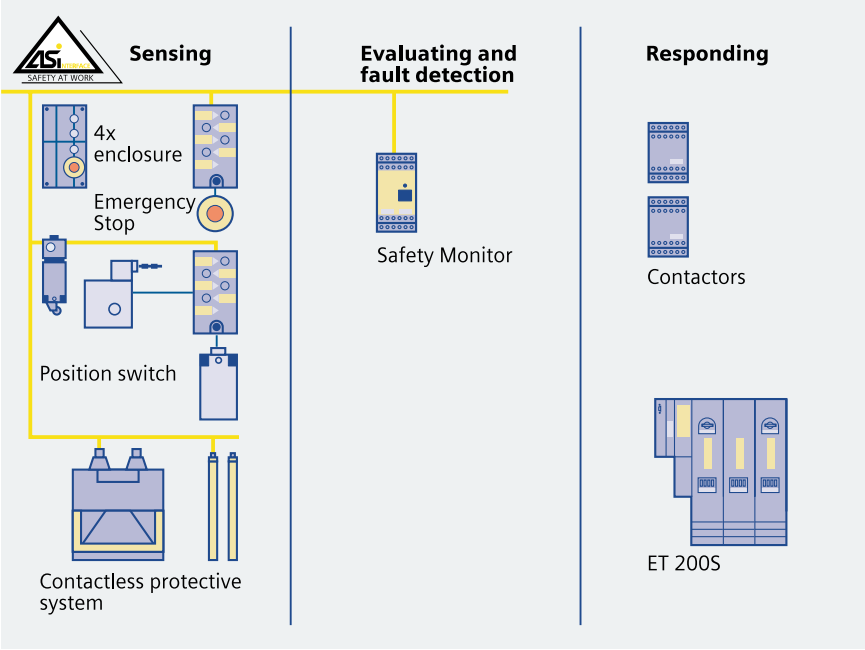


Fig. 3/20
Overview, ASIsafe

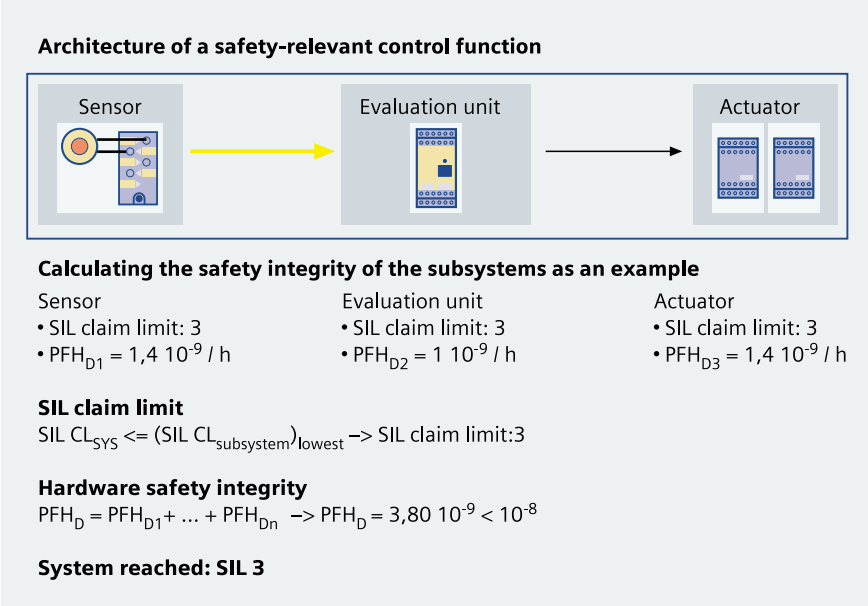


Fig. 3/21
Example of the application according to IEC 62061 when connecting to AS-Interface with ASIsafe

The application shown in Fig. 3/21 comprises the following subsystems:

- Detecting (2-channel Emergency Stop pushbutton)
- Evaluating(ASIsafe safety monitor; with diagnostics)
- Responding (two contactors)

The PFH$_D$ values used for the calculation are only an example and are not authentic values.

Connecting sensors to AS-Interface with ASIsafe

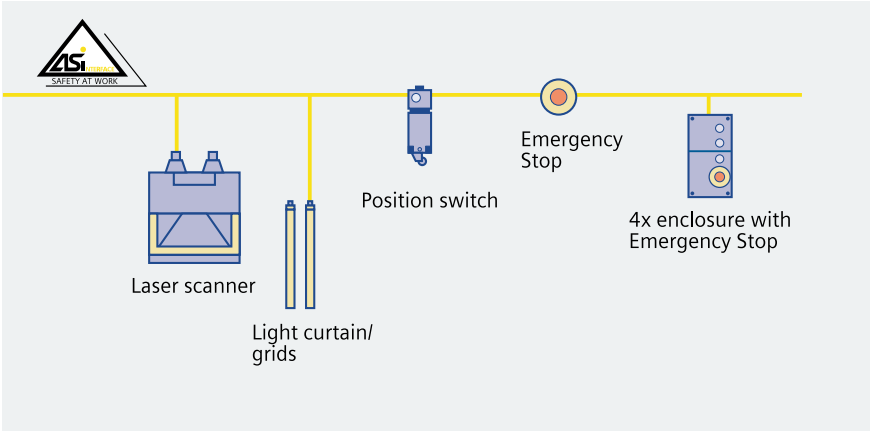


Fig. 3/22
Directly connected to ASIsafe

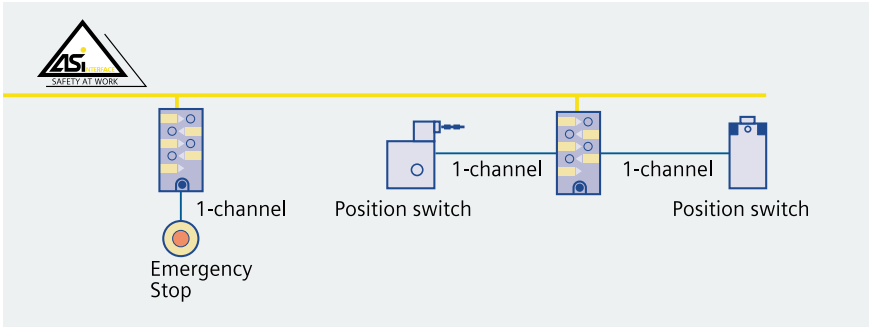


Fig. 3/23
Sensor connected via the distributed compact modules in Category 2 acc. to EN 954-1 with ASIsafe

Description and additional information

- The sensors are connected through 1-channel.
- For each compact module, two electro-mechanical sensors can be connected independently of one another acc. to Category 2 in compliance with EN 954-1.
- If only a 1-channel sensor is connected (Fig. 3/24), then pins 1 and 2 of the input that is not connected, must be jumpered.

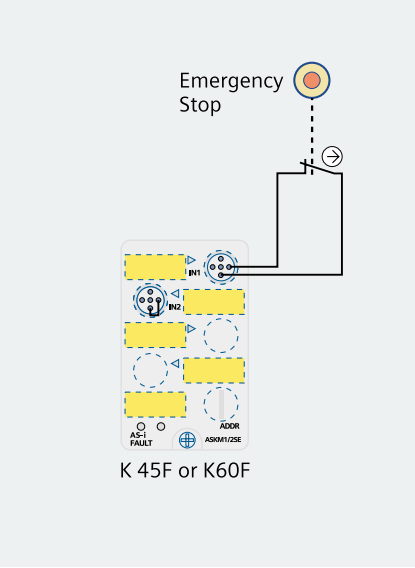


Fig. 3/24
Connecting an Emergency Stop pushbutton, Category 2 acc. to EN 954-1 with a safety compact module

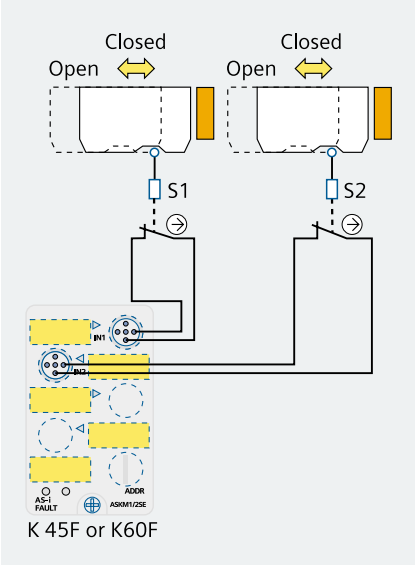


Fig. 3/25
Connecting two protective door monitoring circuits, Category 2 acc. to EN 954-1 to a safety compact module

Description and additional information

- Using a compact module, two protective doors can be monitored in Category 2 acc. to EN 954-1. The evaluation in this case is realized independently.

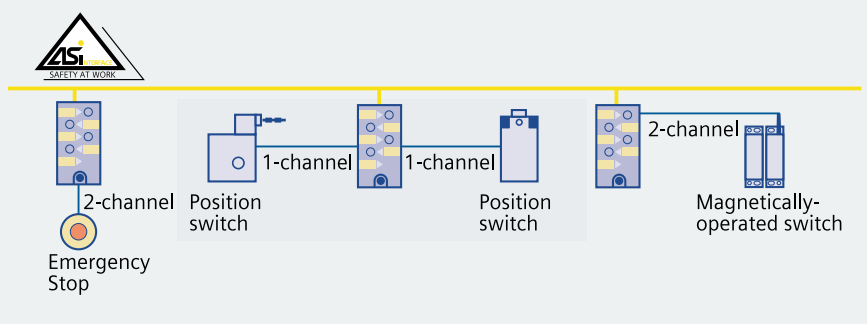


Fig. 3/26
Connecting a sensor via the distributed safety compact module, Category 4 acc. to EN 954-1 with ASIsafe

Description and additional information

- The sensors are connected through 1 channel with crosswise data comparison or 2 channels.
- For each compact module, a 2-channel, electro-mechanical sensor can be connected acc. to Category 4 in compliance with EN 954-1.
- If input 2 is not used, then this must be closed using an M12 cap in order to guarantee the IP67 degree of protection.

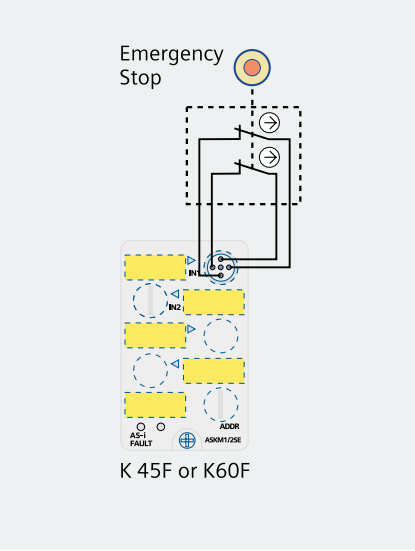


Fig. 3/27
Connecting an Emergency Stop push-button, Category 4 acc. to EN 954-1 to a safety compact module

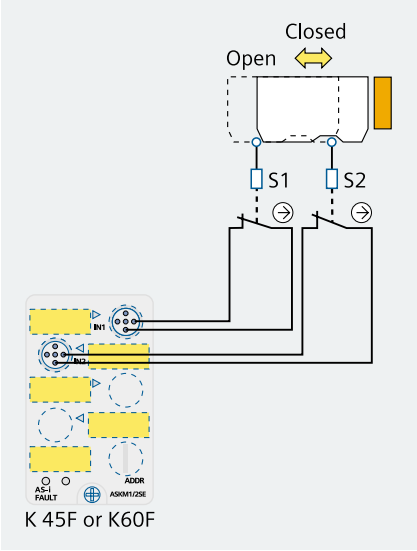


Fig. 3/28
Connecting a protective door monitoring, Category 4 acc. to EN 954-1 to a safety compact module

Description and additional information

- Using a compact module, a protective door can be monitored acc. to Category 4 in compliance with EN 954-1.

Connecting an actuator to the AS-Interface with ASIsafe

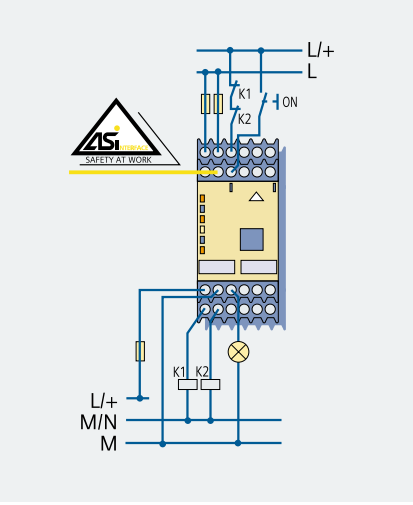


Fig. 3/29
Connecting an actuator, Category 4 acc. to EN 954-1 with ASIsafe using as an example a safety monitor with an enable circuit

Description and additional information

- The ASIsafe safety monitor evaluates all safety slaves and the feedback circuit of contactors (K1, K2).

The detailed principle of operation is described in Chapter 4.2.

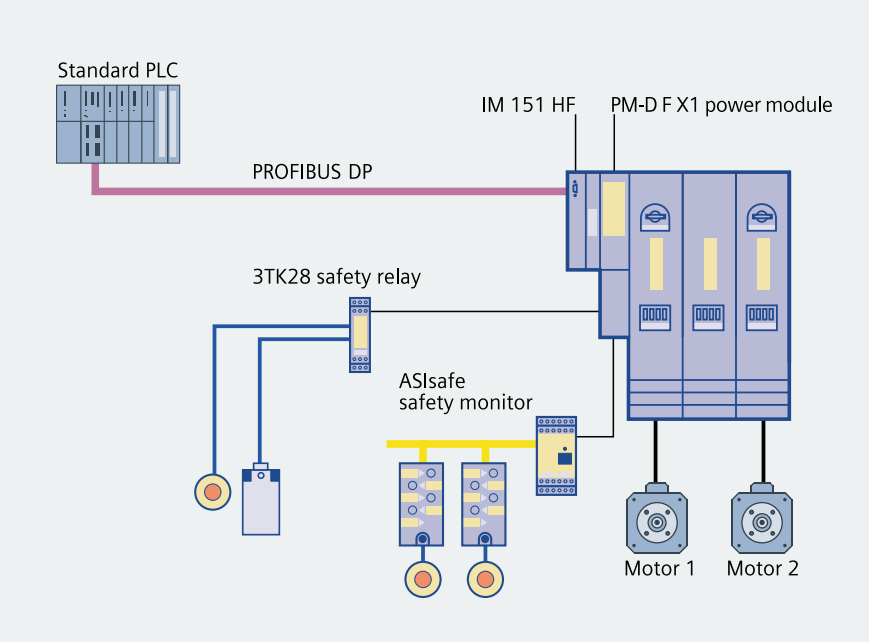


Fig. 3/30
ET 200S Motor Starter Solution Local "shut down using an external safety system" in Category 4 acc. to EN 954-1

Description and additional information

- The sensor signals are monitored using external, safety-related evaluation units, e.g. safety relays or ASIsafe.
- The enable circuits of the external safety-related evaluation units are each connected to one of 6 safety-related segments; this means that the fail-safe motor starter(s) are shut down in a safety-related fashion.

Connecting to PROFIBUS with PROFIsafe

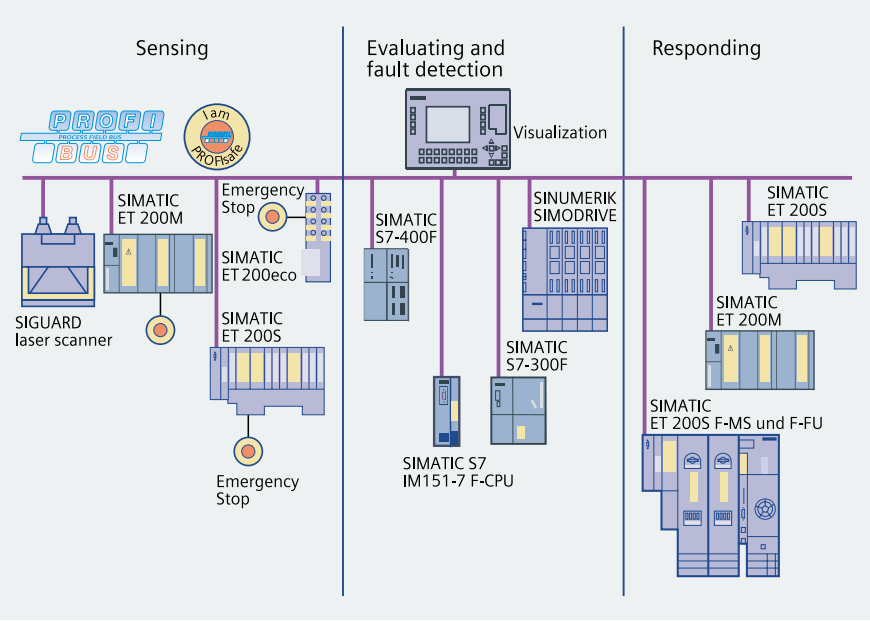


Fig. 3/31
Group diagram, connecting sensors/actuators to the PROFIBUS System

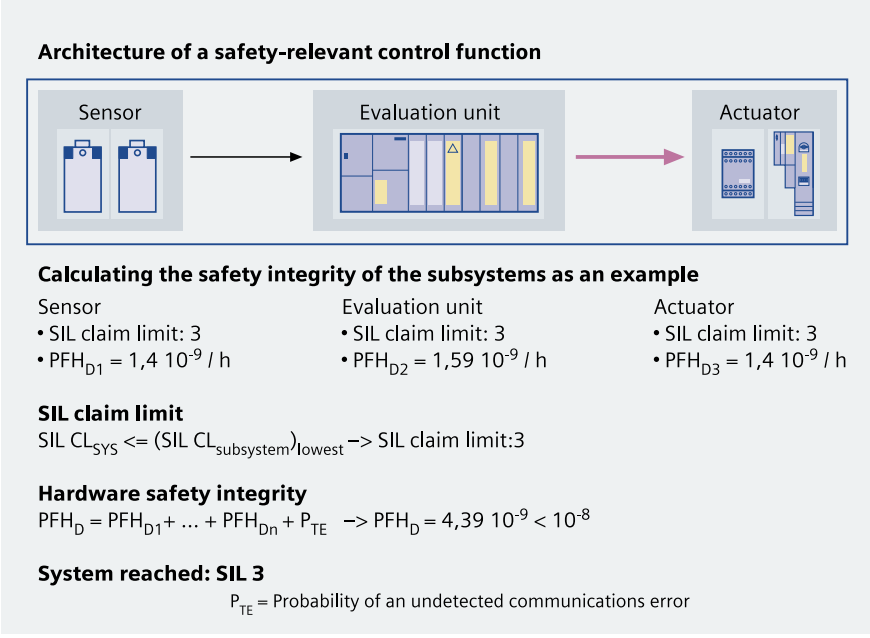


Fig. 3/32
Example of the application acc. to IEC 62061 when connecting to PROFIBUS with PROFsafe

The application shown in Fig. 3/32 comprises the following three subsystems:

- Detecting (two position switches, 1-channel, with an ET 200M F-DI module, with diagnostics)
- Evaluating (the F control, CPU S7-315F with diagnostics)
- Responding (two contactors, with an ET 200M F-DO module, with diagnostics)

The safety-related communications (PROFIsafe) is incorporated in the calculation as P_{TE}.

The PFH_D values used for the calculation are only an example and are not real values.

Directly connecting sensors to PROFIBUS with PROFIsafe

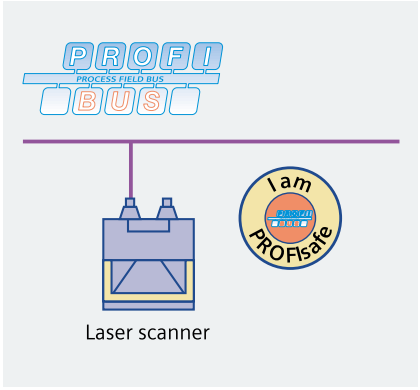


Fig. 3/33
Directly connecting sensors to PROFIBUS

Description and additional information

- For the direct sensor connection shown here, there is no additional wiring required. Every device (slave) is assigned a bus address.

Connecting a sensor to fail-safe SIMATIC input modules

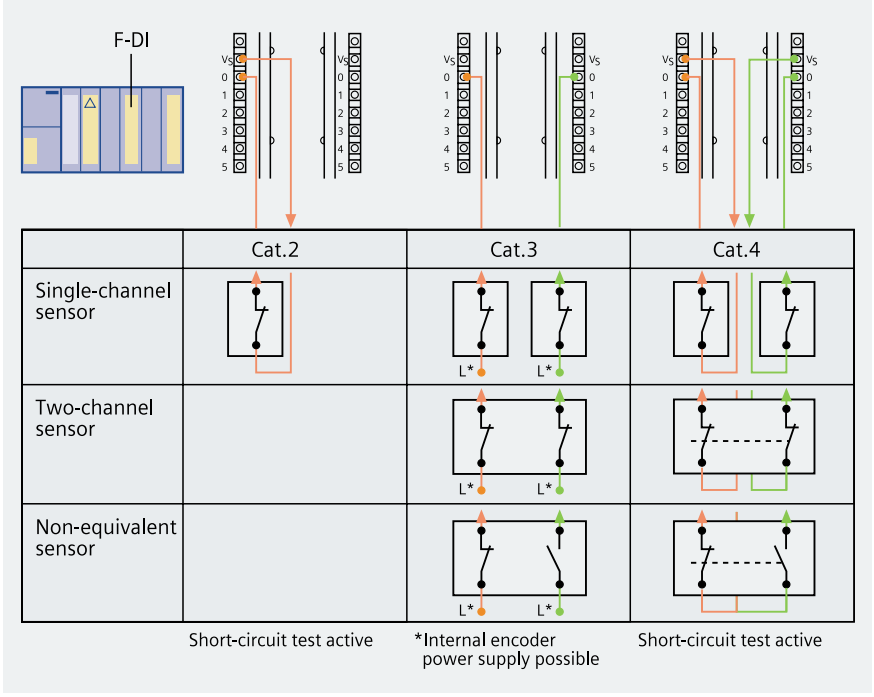


Fig. 3/34
Connecting safety-related sensors. Typical connection SM326 24DI / ET 200M

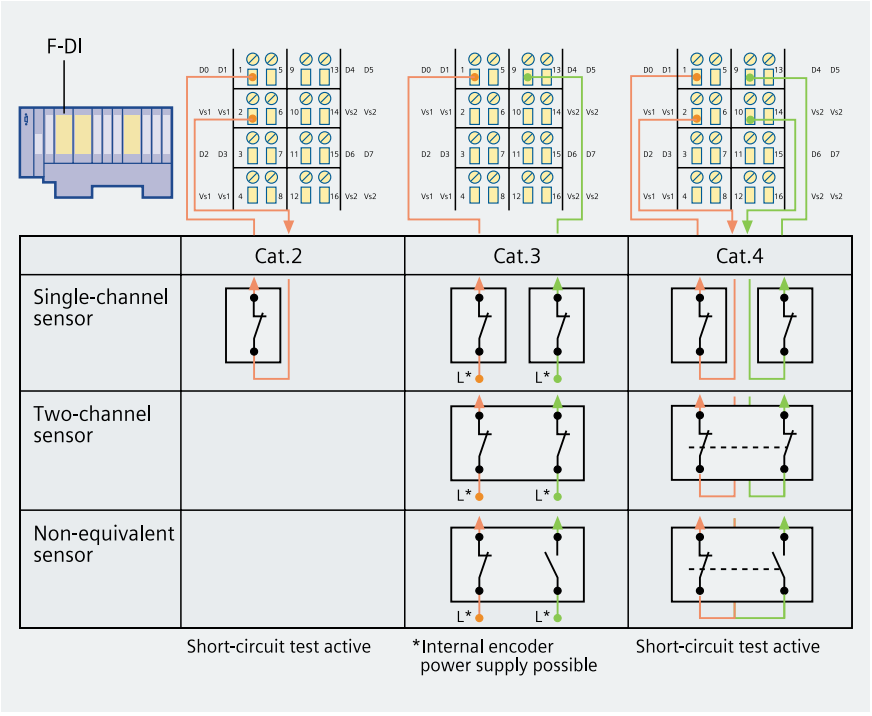


Fig. 3/35
Connecting safety-related sensors. Typical connection 4/8 F-DI / ET 200S

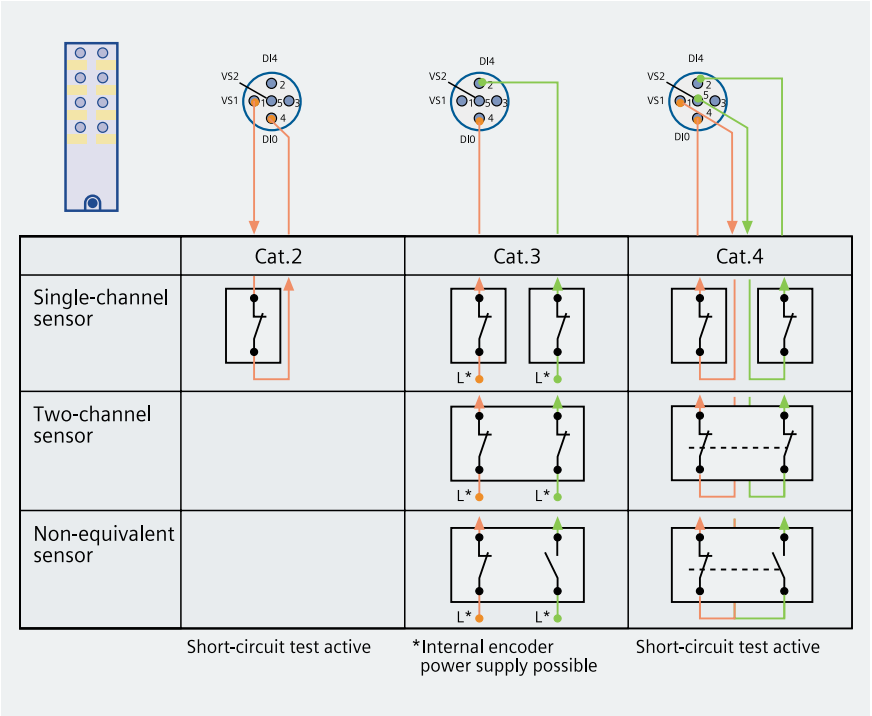


Fig. 3/36
Connecting safety-related sensors. Typical connection 4/8 F-DI / ET 200eco

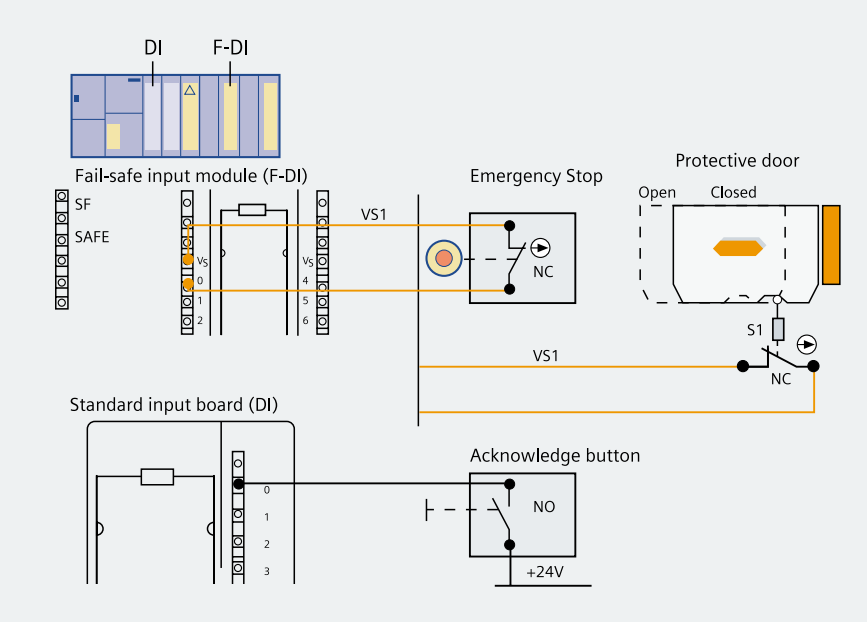


Fig. 3/37
Connecting sensors through fail-safe inputs of the ET 200M F I/O – using as an example, Emergency Stop, protective door monitoring and acknowledgment in Category 2 acc. to EN 954-1

Description and additional information

- In this case, the safety F input module is used to implement the fault monitoring function.
- When the acknowledge button is pressed, this may not result in the plant or system restarting.

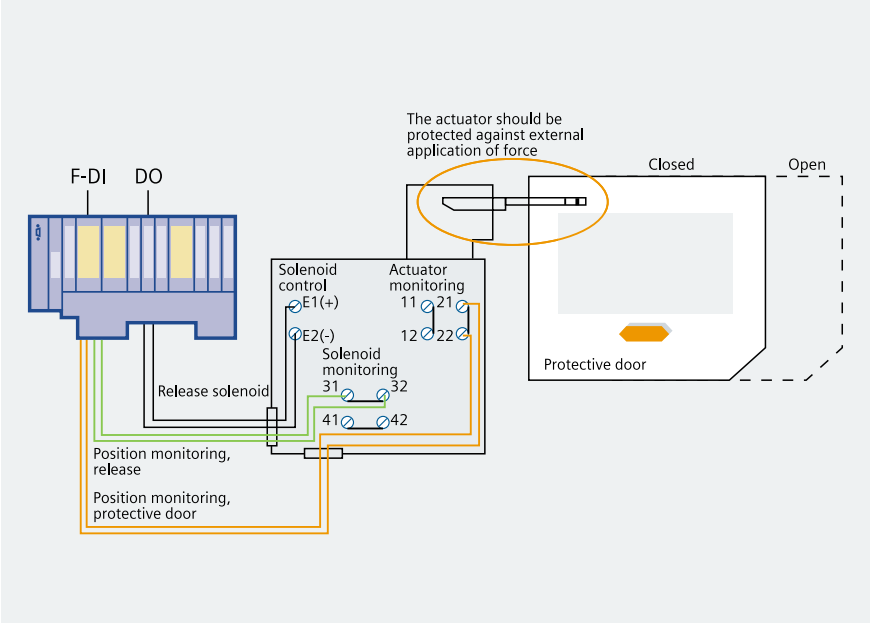


Fig. 3/38
Connecting sensors via fail-safe inputs of the ET 200S F I/O – an example of protective door monitoring with tumbler mechanism in Category 3 acc. to EN 954-1

Description and additional information

The special feature associated with an application with a protective door is the coupling with additional process signals via the “safe programmable logic”. Generally, the release must be safely prevented until all of the process parameters are in a safe condition. For example, it is only permissible that the protective door is opened, if

- A spindle that is running down has reached a non-hazardous speed or has come to a complete standstill.
- A vertical axis after the brake test with a defective brake has been moved into a safe position (stop position clamped position).
- Units with hazardous energy levels have been brought into a safe condition, e.g. laser or hydraulic systems.

For category 3 according to EN 954-1, when using an individual position switch, it must be excluded that the actuator breaks. If it cannot be completely excluded that the actuator cannot be broken, then a second position switch must be additionally used (also refer to Fig. 3/42).

Non-safety relevant control of the solenoids

of the tumbler mechanism in a non-safety relevant fashion is possible up to Category 3 acc. to EN 954-1.

Safety-related control of the solenoids

of the tumbler mechanism in a safety-related fashion from Category 4 acc. to EN 954-1.

The objective of a tumbler mechanism is to maintain the isolating protective device (e.g. guard) in the closed position. Further, the protective device is connected to the machine control so that the machine cannot start if the protective device is not closed and is interlocked. The isolating protective device (e.g. guard) is kept interlocked until there is no longer any danger of injury.

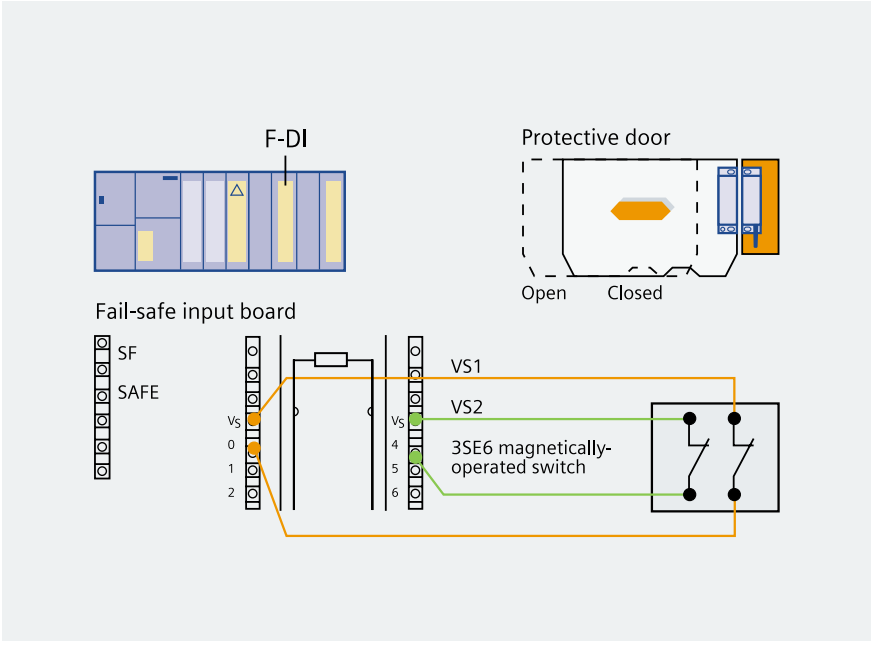


Fig. 3/39
Connecting sensors via fail-safe inputs of the ET 200M F I/O – using as an example fail-safe protective door monitoring with magnetically operated switches in Category 4 acc. to EN 954-1

Comment:

Up to Category 3 according to EN 954-1, the tumbler mechanism does not have to be controlled in a safety-related fashion; however, for Category 4 acc. to EN 954-1, this must always be done in a safety-related fashion. The position monitoring of the interlocking device (solenoid) must, from Category 3 according to EN 954-1 onwards, be realized individually, and may not be connected in series with the monitoring function of the separate actuator (due to the poor fault detection level).

Description and additional information

- The contactless protective door monitoring comprises a coded solenoid and a switching element (reed contacts).
- For Category 4, the internal voltage of the fail-safe modules must be used as power supply. The sensors are evaluated through two channels - in this case, the short-circuit test in the module must be activated.
- Non-equivalent magnetically operated switches can be connected to the fail-safe inputs of the SIMATIC S7 300F/400F.
- Up to Category 4, acc. to EN954-1, it is also possible to connect magnetically operated switches to ASIsafe or to a 3TK284x.

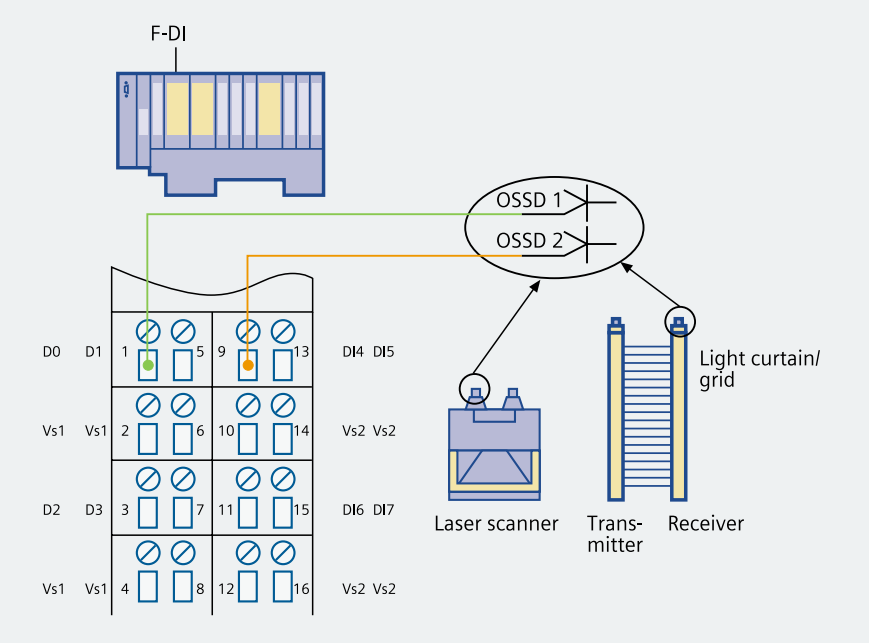


Fig. 3/40
Connecting sensors via fail-safe inputs of the ET 200S F I/O – using as an example a contactless protective device type 3 and 4 acc. to IEC 61496-1, 2 or EN 61496-1, 2

Description and additional information

- Instead of a light curtain, light grid or the light barrier, a laser scanner can also be directly connected (laser scanners, due to their operating principle, are permitted up to Category 3 acc. to EN 954-1).
- On the fail-safe module, the evaluation must be realized through 2 channels. The necessary test for short-circuit and cross-circuit faults is implemented by the contactless electro-sensitive protective equipment. This means that this test must be disabled in the associated module.
- Supplementary functions such as restart and contactor monitoring - but also cyclic operation or muting can be implemented using the 3RG7847.. evaluation units or, as shown here, using a safety-related controller e.g. SIMATIC S7-300F/400F.

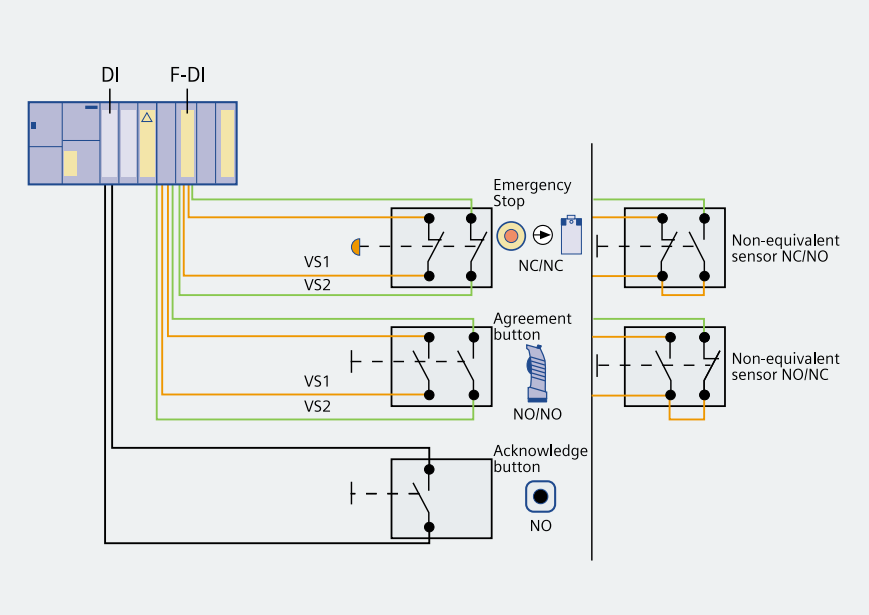


Fig. 3/41
Connecting sensors via fail-safe inputs of the ET 200M F I/O – using as an example Emergency Stop, agreement button and acknowledgment in Category 4 acc. to EN 954-1

Description and additional information

- The Emergency Stop acknowledge button is connected through a single channel to a standard module and is evaluated in the safety-related program using a signal edge.

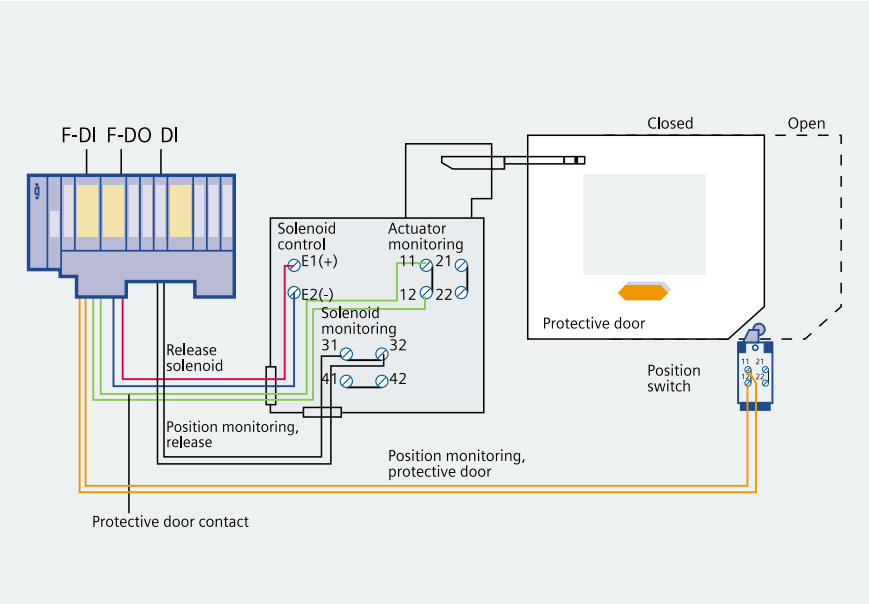


Fig. 3/42
Connecting sensors via fail-safe inputs of the ET 200S F I/O – using as an example protective door monitoring with tumbler mechanism in Category 4 acc. to EN 954-1

Description and additional information

- The connection for Category 4 acc. to EN 954-1 differs to that of Category 3 (Fig. 3/38) as a result of the second position switch and the safety-related connection of the solenoids.
- Up to Category 4 acc. to EN 954-1 it is also possible to connect a door tumbler mechanism to ASIsafe or to 3TK284x safety relays.

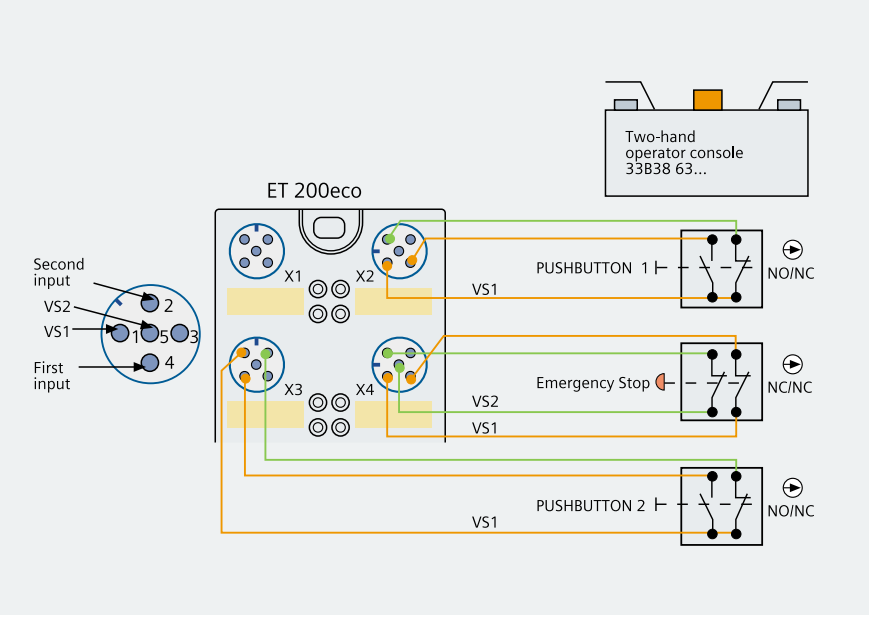


Fig. 3/43
Connecting sensors via fail-safe inputs of the ET 200eco F I/O – using as an example a two-hand operating console, Category 4 acc. to EN 954-1

Description and additional information

- For Category 4, the internal voltage of the fail-safe modules must be used as power supply. The sensors are evaluated through two channels - in this case, the short-circuit test in the module must be activated.
- The discrepancy time between the two actuated pushbuttons should be set in accordance with EN 574.
- Up to Category 4 according to EN 954-1, a two-hand operating console can also be directly connected to ASIsafe or to a 3TK284x safety relay.

Connecting actuators to PROFIBUS with PROFIsafe

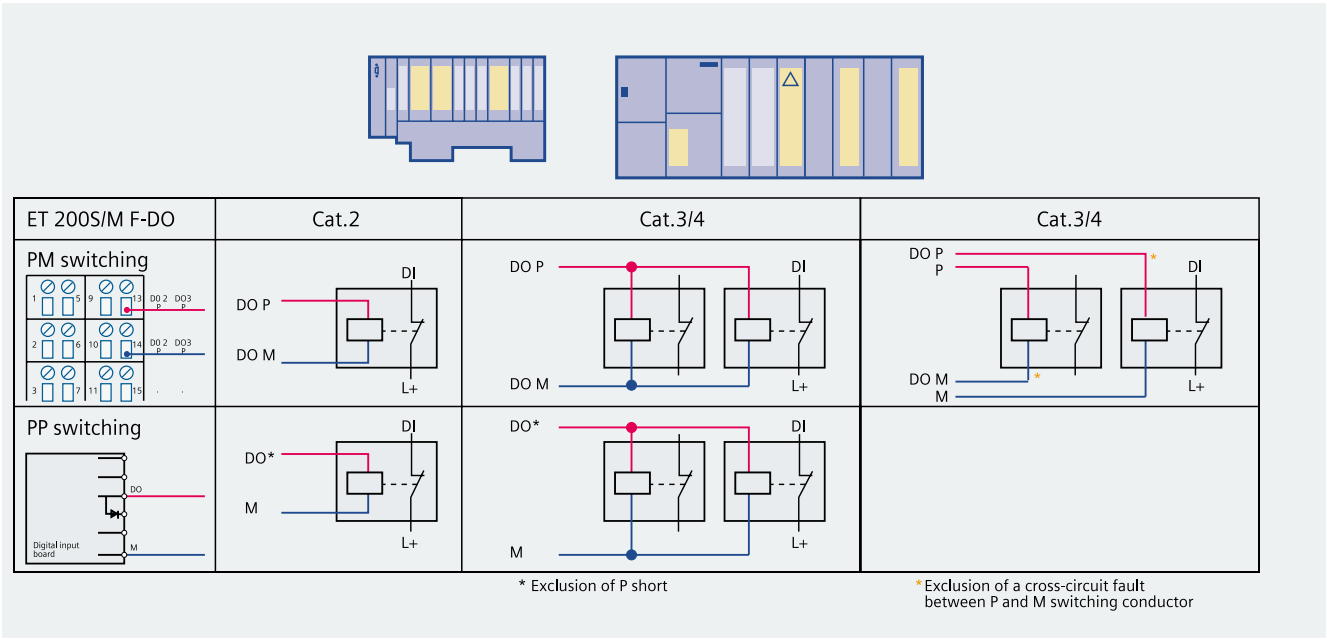


Fig. 3/44
Connecting safety-related actuators, plus-minus /plus-plus switching

Feedback signal from the load circuit

- The feedback signal from the load circuit should be derived as directly as possible from the associated process quantity. This is realized, e.g. for contactors, by feeding back a positively-driven opening contact. The feedback does not have to be safety-related!
- However, it is preferable to have a direct feedback signal of the hydraulic pressure using a pressure sensor or a feedback signal from the moved mechanical system (endstop) via a Bero rather than using an indirect feedback signal from the hydraulic valve.
- The F-DO monitors the control cables of the actuator - if a fault occurs, the outputs are switched into a safe condition.

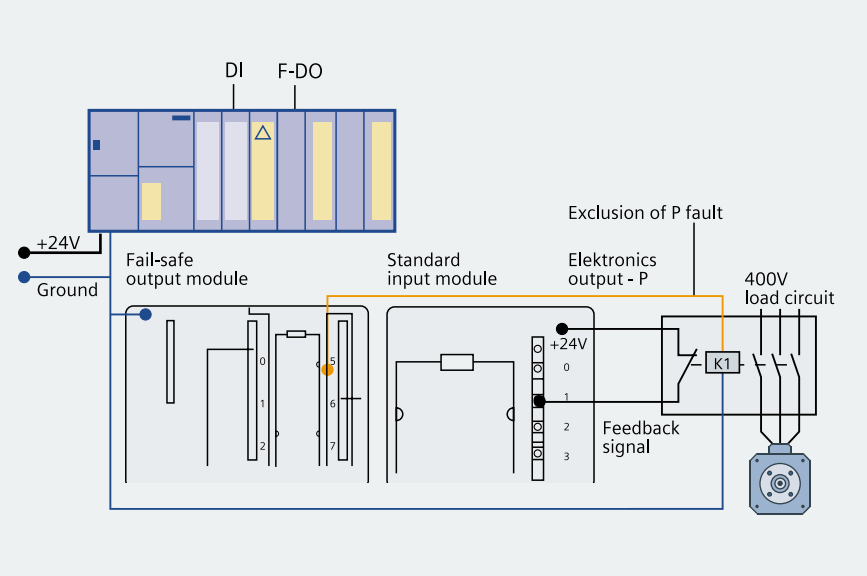


Fig. 3/45
Disconnecting an actuator via fail-safe outputs of the ET 200M F I/O in Category 2 acc. to EN 954-1

Description and additional information

- An actuator shutdown circuit using an ET 200M F output is shown in Fig. 3/45. The required feedback signal of the contactor is connected to a standard input of a digital input module through a single channel via the positively-driven contact and is dynamically (in time) monitored in the fail-safe program.

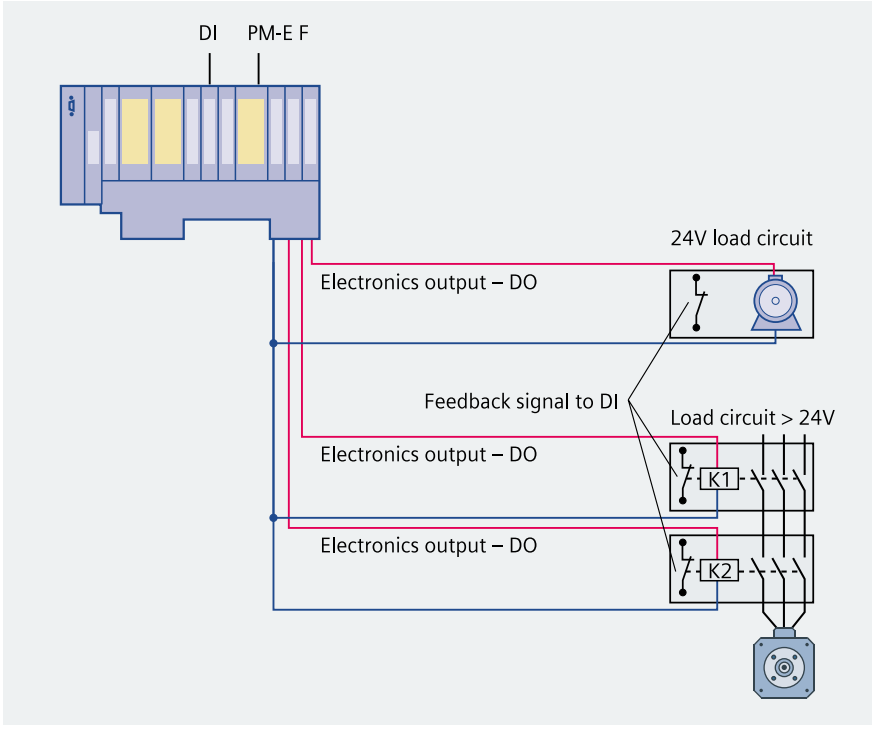


Fig. 3/46
Disconnecting actuators via standard outputs of the ET 200S F I/O – using as an example, group shutdown, Category 3 acc. to EN 954-1

Description and additional information

- Operational switching is realized using standard outputs that are inserted after the PM-E F module.
- The PM-E F module supplies the following standard modules with power.
- If an Emergency Stop is issued, then the contactors are safely de-energized via the PM-E F module. This is realized by this module disconnecting the power supply voltage (P and M) for the standard outputs.
- For the safety-related shutdown it is only permissible to use standard modules after the PM-E F.

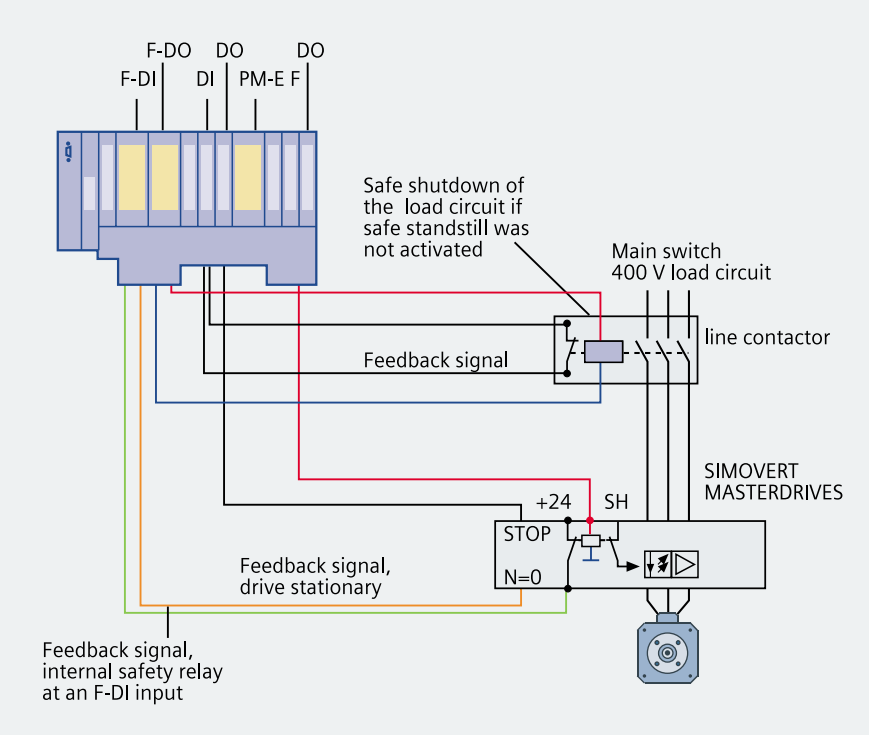


Fig. 3/47
Shutting down an actuator via standard outputs of the ET 200S F I/O – using as an example SIMOVERT MASTERDRIVES stop Category 1, acc. to EN 60204-1, in Category 3 acc. to EN 954-1; safe standstill function with controlled drive stopping

Description and additional information

- Safe standstill:
  The safe standstill function (SH) prevents a connected motor from unexpectedly starting from standstill. Safe standstill should only be activated after the drive has come to a standstill, as otherwise it loses its capability of braking.

- The drive is braked as quickly as possible via an input of the frequency converter (STOP). Safe standstill is activated after the drive comes to a complete standstill, or, at the latest after a defined maximum monitoring time.

- The positively-driven feedback signal contacts of the relay integrated in the frequency converter, must be evaluated in the F control so that if the relay functions incorrectly, (e.g. the contacts weld), then this is detected and the higher-level line contactor is de-energized.

- STOP and safe standstill are addressed via a standard output module after the PM-E-F.
  In the fail-safe program section, the power rail of the PM-E-F is shut down as soon as the safe standstill function was activated (also refer to Fig. 3/19).

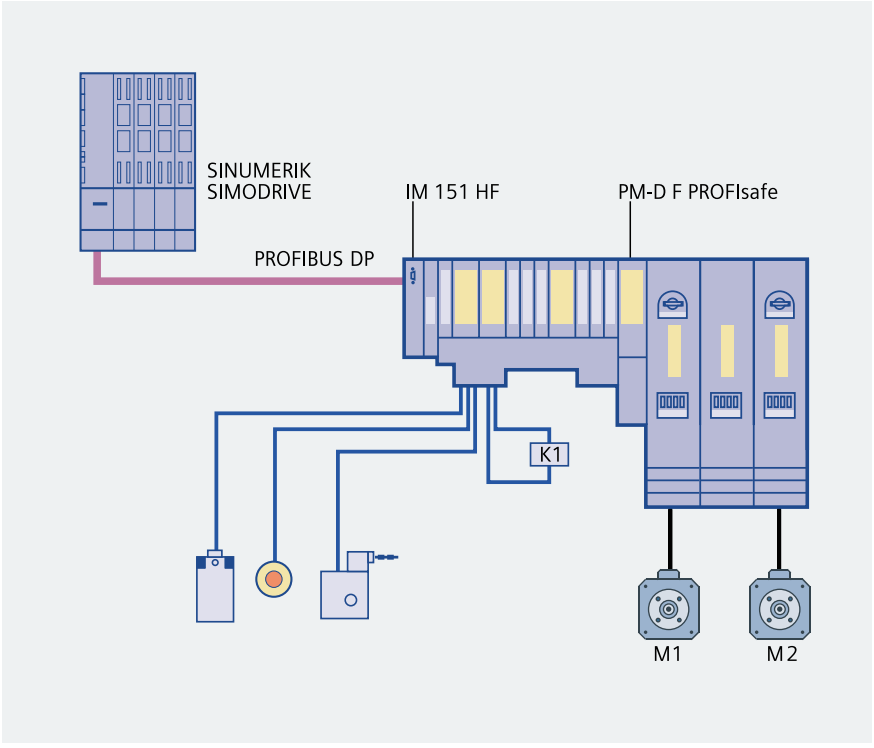


Fig. 3/48
Shutting down an actuator – using as an example, the ET 200S F I/O in Category 3 acc. to EN 954-1 at the SINUMERIK 840D PROFIsafe

Description and additional information

- Depending on the required category, the sensors and actuators are connected to the fail-safe I/O of the ET 200S either through one channel or two channels and transferred to the SINUMERIK master via PROFIsafe.
- Depending on the requirement, the SINUMERIK master directly shuts down the motor starter via the PM-D F PROFIsafe and the fail-safe outputs.

Category 3 according to EN 954-1 is reached using this example as the SINUMERIK master is certified acc. to Category 3.

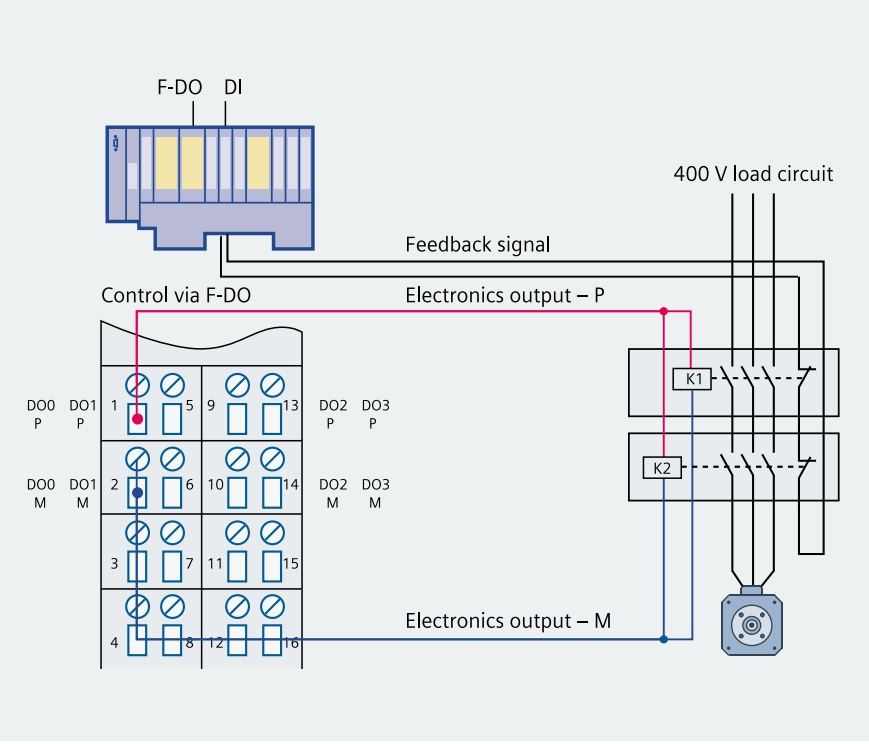


Fig. 3/49
Shutting down an actuator via fail-safe outputs of the ET 200S F I/O – using as an example shutting down an actuator, Category 4 acc. to EN 954-1

Description and additional information

- The example in Fig. 3/49 shows an actuator shut down using only one ET 200S F output.
- The required feedback signal of the contactors is connected to the standard input of a digital input module through a single channel via the positively-driven contacts and dynamically (in time) monitored in the fail-safe program.

Versions

- An ET 200S PROFIsafe motor starter replaces the discrete circuit through two load contactors (refer to Fig. 3/50).

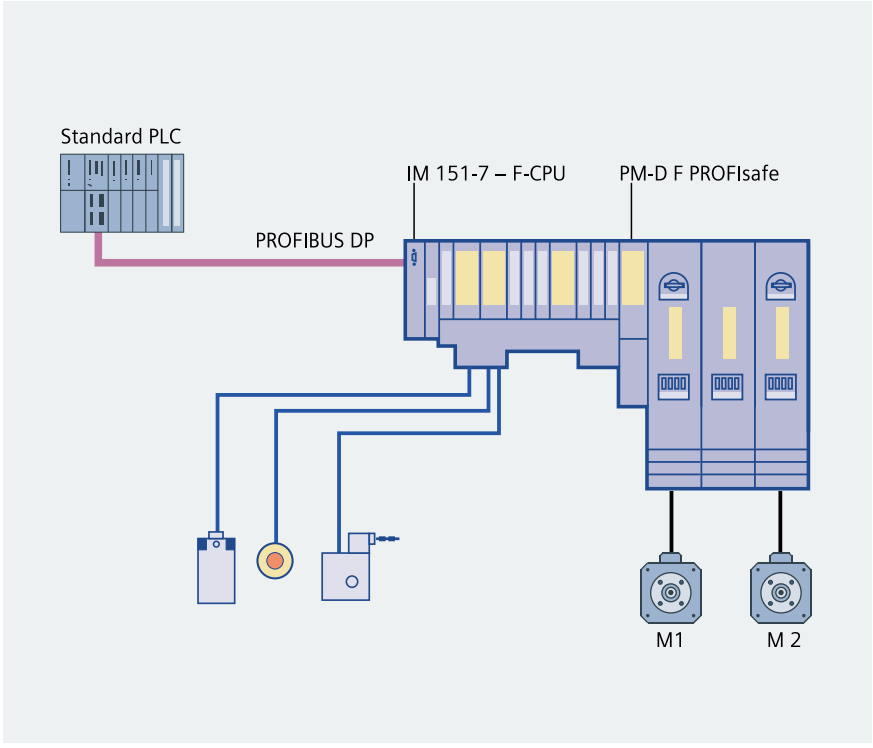


Fig. 3/50
Shutting down an actuator via a "local safety island" –
using as an example the IM 151-7 F-CPU in Category 4 acc. to EN 954-1

Description and additional information

- In the example, the sensor is monitored decentrally in an ET200S station.
- Depending on the requirement, the F-CPU (IM 151-7 F-CPU) shuts down the motor starter in safety-related fashion. This is realized by the PM-D F PROFIsafe receiving a shutdown command and disconnecting one or several safety groups to which the motor starter is connected through hardware and is parameterized through the software.

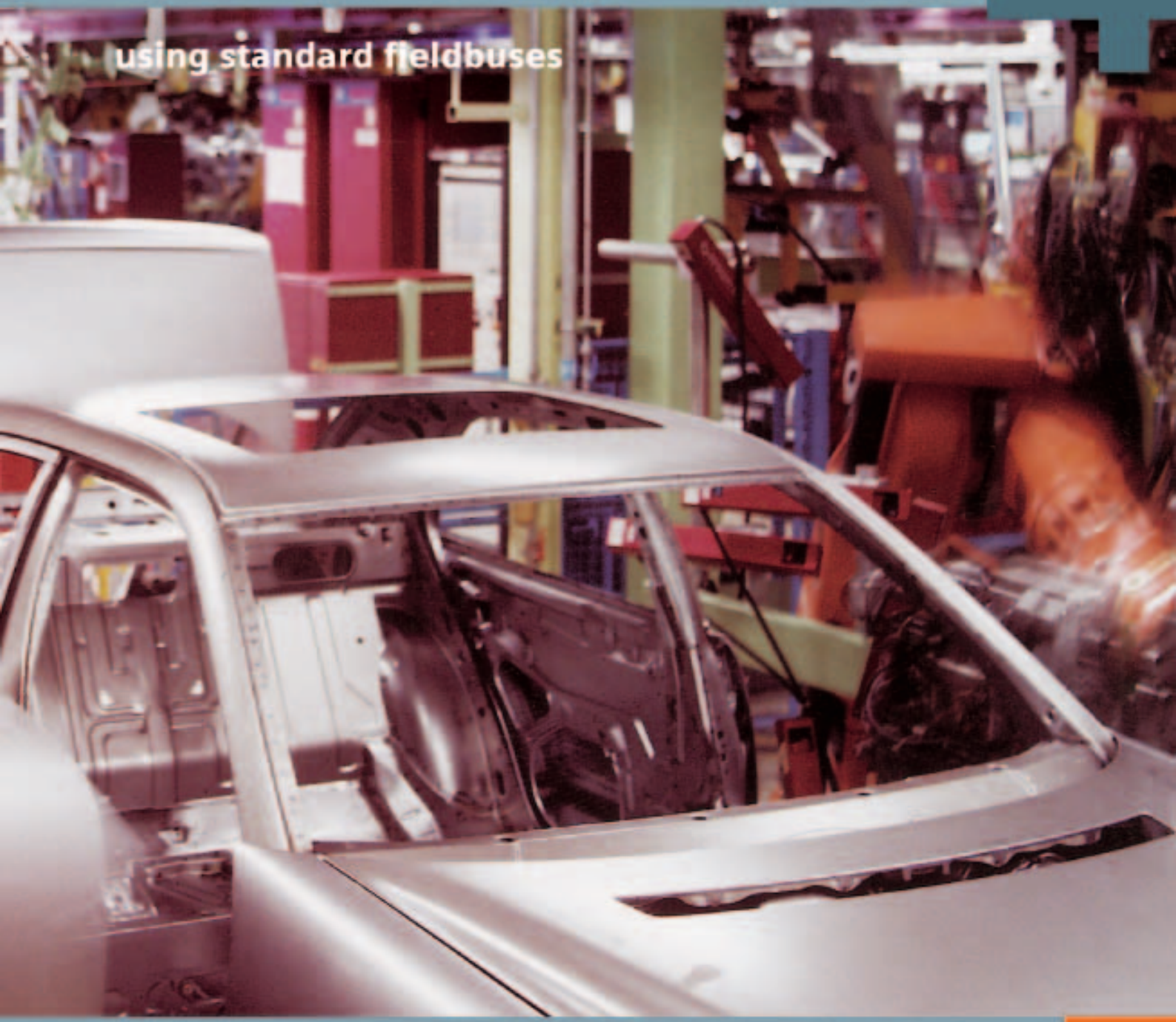
Versions

- If the sensor signals are entered in a distributed fashion, e.g. using ASIsafe and monitored by the ASIsafe Monitor, then the safety groups can be selectively switched using the safety-related outputs of the monitor using a PM-D F-X1 module. In this case, an F-CPU is not required (refer to Fig. 3/30).

Fail-safe communications

using standard fieldbuses

4



4 Fail-safe communications using standard fieldbuses

Fail-safe communications using standard fieldbuses with PROFIsafe and ASIsafe

Selecting the correct installation technology is an important step in reducing costs. In standard technology, the move to distributed concepts and the use of modern fieldbuses have already resulted in significant cost savings. In the future, further cost savings will be achieved by transferring additional safety-related signals along existing standard fieldbuses.

Overall system with integrated safety

By placing safety-related communications on these proven standard fieldbuses, plant and system engineers can work more cost-effectively in the standard automation environment as well as in safety technology. This is because they can use the same engineering tools and methods. Contrary to concepts which use special buses to transfer safety-related data, in this case, there is data transparency between the standard and safety-related part of an overall plant or system without any additional interfaces.

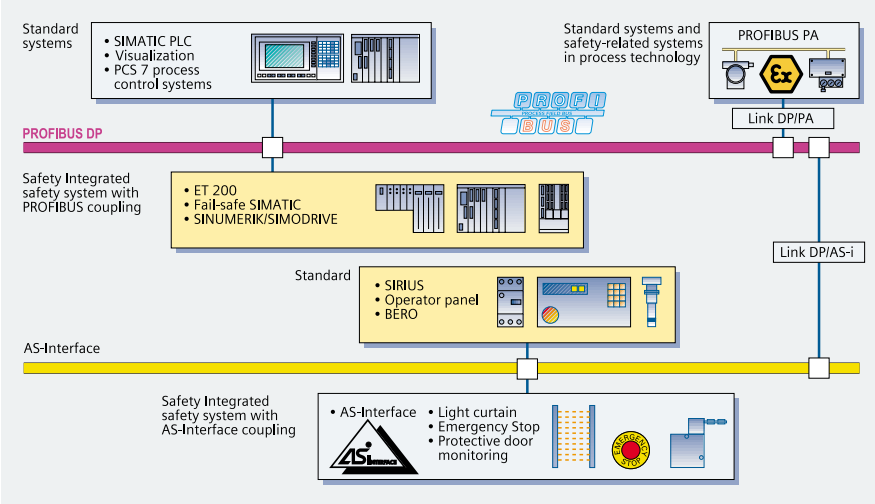


Fig. 4/1
The basic principle of "Safety Integrated":
A unified automation system with integrated safety functions

4.1 PROFIsafe

PROFIsafe and PROFIBUS stations co-exist on the same cable

The main stipulation when defining the PROFIsafe profile was that safety-related and standard communications

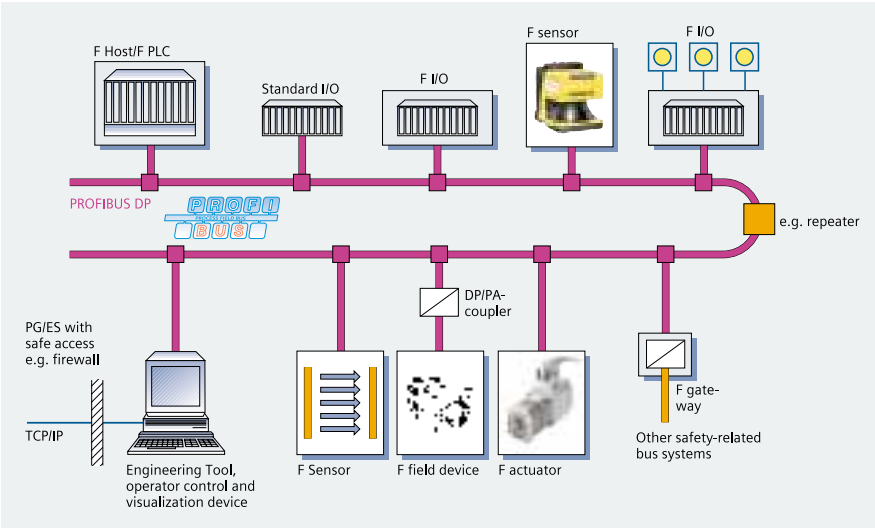


Fig.4/2
PROFIsafe and PROFIBUS nodes co-exist on the same cable

should co-exist on one and the same bus cable. The required safety should still be able to be implemented using a single-channel communications system, however, the optional strategy of increased availability by having redundant data channels was not to be excluded.

Safety-related communications via PROFIBUS-DP using PROFIsafe

The Profibus User Organization (PNO) published, in the Spring of 1999, Directives for safety-related communications on Standard Profibus under the PROFIsafe trademark. This was the result of a working group and has also been acknowledged by the BGIA [Germany Regulatory Body] and the TÜV [German Inspectorate] in the form of evaluation reports.

From the very start, the goal of the working group was to involve as many possible partners in defining and generating a solution and to make the result available in an open form. In addition to manufacturers of safety-related systems, there were more than 25 renowned national and international manufactures of safety-related sensors and actuators, machine tools plants, end users and universities represented. Intermediate and final results are continually harmonized with the TÜV and the BGIA. Some significant support also came from the Verein Deutscher Werkzeugmaschinenfirmen [Association of German Machine Tool Manufacturers]. As a result of safety-related scenarios that were jointly discussed, a quasi "standardized" complete requirement profile for distributed safety-related technology was created. The PROFIsafe concept was able to be continually mirrored against this.

Further, there was the requirement to integrate even more complex devices associated with optical safety systems, e.g. laser scanners and light curtains.

Features/benefits

The following sections show how PROFIsafe fulfilled all of the specified requirements.

Safety-related plant and systems can be flexibly implemented

Safety-related plants and systems can be extremely flexibly implemented using PROFIsafe. On one hand, a single-cable solution with combined standard and safety automation is possible in one CPU. On the other hand, two CPUs and two separate bus cables can also be used. The "homogeneous solution" with a single bus system naturally offers many advantages - especially when it comes to engineering.

Technical advantages of PROFIsafe

PROFIsafe uses standard communication components that have been introduced - such as cables, ASICs and software packages. The safety-related measures are encapsulated in the safety-related communication end stations. There are no restrictions regarding the baud rate, number of bus stations (bus nodes) or the data transfer system as long as the required response times of the automation application permit this. Further, PROFIsafe has the advantage that users do not have to apply any special measures when it comes to bus cables, shielding, bus couplers, etc.

The PROFIsafe protocol detects any communication errors. PROFIsafe ensures that the values are correctly transferred in the telegrams and that the telegrams are received within a defined time. Further, PROFIsafe also allows complex safety-related terminal devices to be connected - that either require extensive parameterization or can supply complex data.

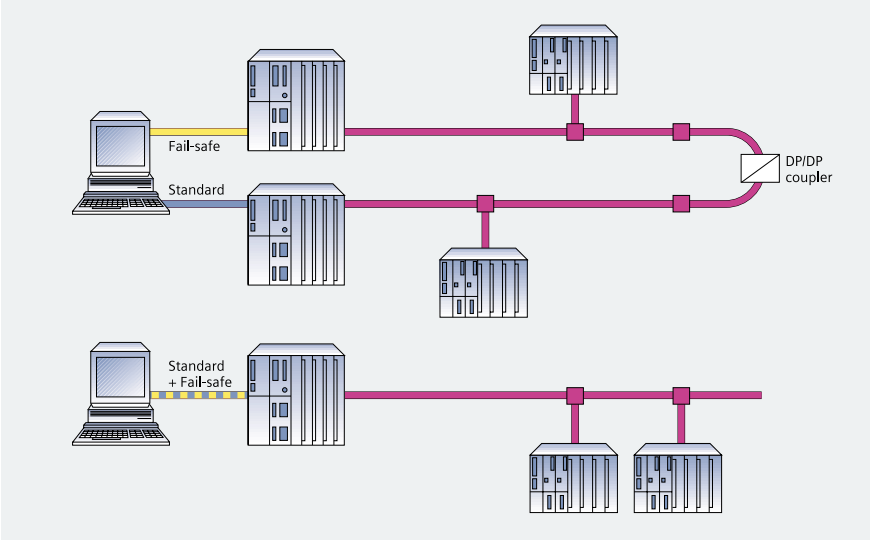


Fig. 4/3
Versions for safety-related systems (below: One bus system for standard and safety automation, top: Separate standard and fail-safe bus system)

PROFIsafe applications

PROFIsafe is always used if, for distributed plants and systems, it is necessary to have safety-related communications via PROFIBUS. This is especially the case if safety-related devices are to be connected to an existing bus without having to make complex and costly hardware modifications.

PROFIsafe-capable products

Back in 1999, the SIMATIC S7-414FH and S7-417FH (refer to Chapter 7) with distributed fail-safe ET 200M I/O were introduced as the first PROFIsafe products. They can also be used in redundant architectures. This additionally guarantees the highest degree of availability which makes them predestined for process automation. Further, additional fail-safe PLCs are available in the form of the SIMATIC S7-315F, S7-317F and S7-416F (refer to Chapter 7). They are mainly used in production technology. In addition to the ET 200M, the ET 200S and ET 200eco round-off the range of fail-safe I/O.

Further, there are also fail-safe light curtains and laser scanners.

These are complemented by complex sensors and actuators and contactless protective devices from our SIGUARD Safety Integrated range with direct connection to PROFIBUS/PROFIsafe. The fail-safe SINUMERIK 840D can be connected in the same way.

Which safety levels does PROFIsafe achieve?

The PROFIsafe Directive was already developed according to the Standard IEC 61508. Its mentor was the prEN 50159-1 that provided similar solution strategies for the railway sector. Additional relevant Standards and regulations were also taken into account. Safety Integrity Level 3 (IEC 61508), Category 4 (EN 954-1) is reached.

PROFIsafe in the 7-layer communications model

With the PROFIsafe profile, the safety-related measures are located above layer 7 of the ISO/OSI communications model. This meant, an additional layer was required which handles the safety-related provision and conditioning of the net data. In a safety-related field device, this function can be handled, e.g. by its firmware.

Just the same as for standard operation, the process signals and process values are packaged in the appropriate net telegrams. For safety-related data, they are only supplemented by safety information.

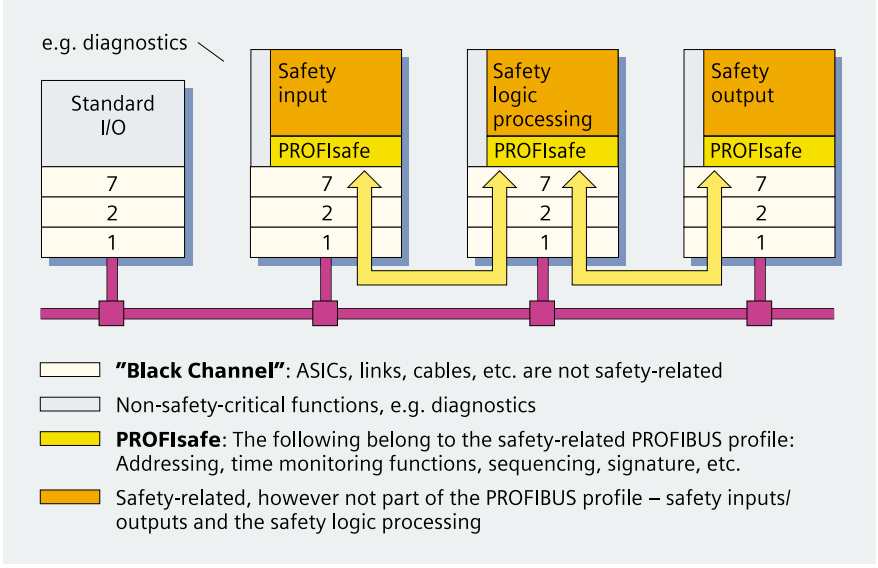


Fig. 4/4
PROFIsafe safety layer above the OSI model

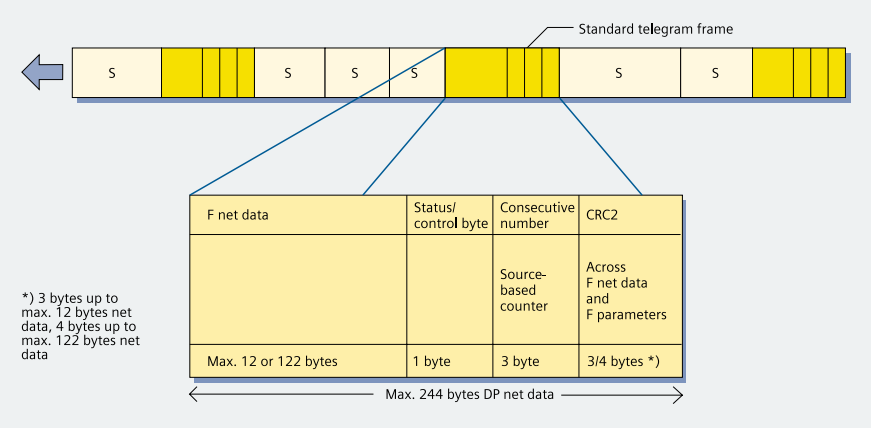


Fig. 4/5
PROFIsafe telegrams simply packaged in standard telegrams

A standard "Master-Slave mode" mechanism from PROFIBUS is used to send safety-related telegrams. A master, which is generally assigned a CPU, exchanges telegrams with all of the configured slaves.

PROFIsafe functions

PROFIsafe allows safety-related communications by being able to control any communications error; in so doing, the safety on PROFIBUS is continually monitored.
PROFIsafe also allows complex terminal devices to be connected by using the appropriate expanded protocol.

Possible communication errors

A whole series of errors can occur when sending telegrams. Telegrams can get lost, be repeated, additionally inserted, appear in the incorrect sequence or with a delay. Data can also be corrupted. In addition, incorrect addressing is possible which means that a standard telegram is incorrectly received by a safety-related device and poses as a safety telegram (masquerade).

PROFIsafe mechanisms for safety-related communications

The possible fault causes and the counter-measures selected for PROFIsafe, are entered in a matrix in Fig. 4/6. These include

- The consecutive number of the safety telegrams,
- An expected time with acknowledgment,
- An ID for the sender and receiver ("solution word") and
- An additional data security check (CRC – cyclic redundancy check).

Using the consecutive number, a receiver can recognize whether it received all of the telegrams in the correct sequence.

Measure: / Error:	Consecutive number (sign of life)	Expected time with acknowledgment	ID for sender and receiver	Data security
Repeat	x			
Loss	x	x		
Insertion	x	x	x	
Incorrect sequence	x			
Net data corruption				x
Delay		x		
Masquerade		x	x	x
FIFO error within the router		x		

Fig. 4/6
Possible communication errors and how they can be detected using PROFIsafe functionality

In safety-related systems, it isn't enough that a telegram transfers the correct process signals or values, but these must also be received within a defined time (fault tolerance time), so that the particular device can automatically and locally initiate the safety-related response when necessary. To realize this, the stations have an adjustable time-out function, which is restarted after a safety-related telegram has been received.

The 1:1 relationship between a master and slave makes it easier to recognize incorrectly routed telegrams. Both of these have a unique ID in the network ("solution word"), which can be used to check the authenticity of a telegram. Data integrity using CRC plays a key role. In addition to the data integrity of the transported net data, CRC is also responsible for the integrity of the parameters in various terminal devices.

The data integrity measures and the reliability of the standard PROFIBUS were not used for the proof of safety. This meant that the proof of safety for PROFIsafe was somewhat more time consuming and complex, but has the advantage that users do not have to apply any special measures regarding bus cables, shielding, bus couplers, etc. for PROFIsafe.

SIL monitor for safety monitoring on PROFIBUS

A Markov model is specified in prEN 50159-1. In a slightly expanded form, this can be used to calculate the residual error probability of safety circuits. It assumes three essential causes of corrupted messages which must all be detected by the two data integrity devices: Failures in ASICs and drivers, electromagnetic disturbances and a special case where only the safety devices in the bus ASIC have failed. Without specific measures, special proof would have to have been provided for every bus configuration.

This would represent a significant restriction for an open standard fieldbus such as PROFIBUS.

Thus, a mechanism was created that guarantees that the SIL levels are maintained over the lifetime of a distributed, safety-related automation solution - and that independent of the components used and the configuration: A patented SIL monitor. This is implemented in the software. This monitor takes into account all of the conceivable consequences arising from errors/faults, and initiates a response if the number of faults or disturbances exceeds a specific level per unit time. The number of permissible faults/errors per unit time depends on the selected SIL stage.

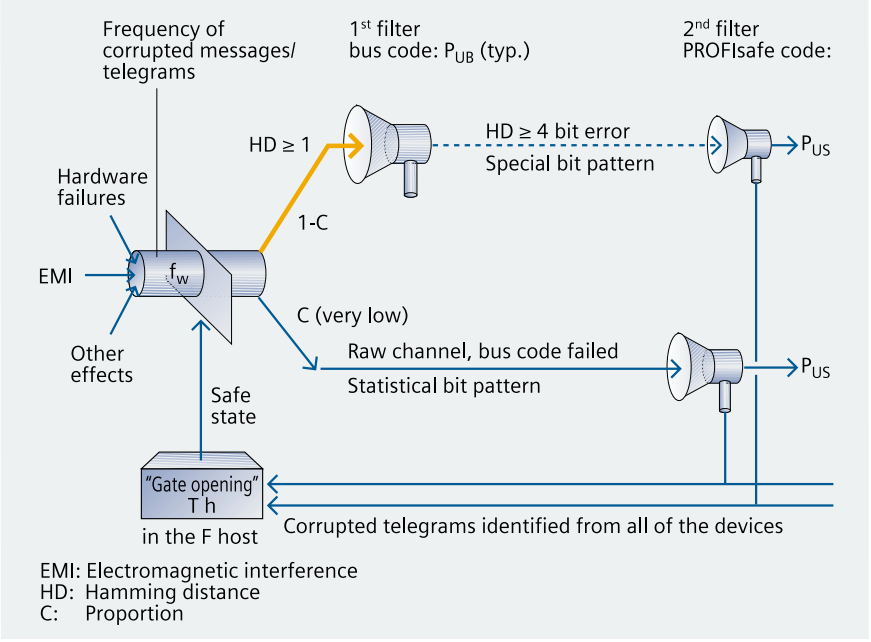


Fig. 4/7
Patented SIL monitor continually monitors the functional safety of PROFIsafe

Connecting complex terminal devices to PROFIsafe

As a result of the various discussions, the working group members quickly saw that a pure profile description would not be adequate for fast implementation in many "PROFIsafe products". Especially optical safety-related technologies, e.g. utilizing laser scanners and light curtains require a high number of parameters which demand special handling in the teach-in phase. The working group described solutions in the Guidelines, which could be applied for these and additional complex devices. PROFIsafe components can be parameterized and diagnosed using a PC directly connected to PROFIBUS – as is usual for PROFIBUS.

In order to make it simpler to engineer safety-related circuits, the engineering tools have access to all of the necessary parameters. When calculating the overall response times of the safety process, manufacturers must specify the processing times of sensors and actuators in the GSD (master device data) data sheets.

PROFIsafe interacting with TIA

This means that PROFIsafe provides a high degree of integration and standardization for safety technology, similar to the standard automation solutions on PROFIBUS. This is completely in line with the philosophy of "Totally Integrated Automation" (TIA), and creates significant flexibility when solving even more complex tasks.

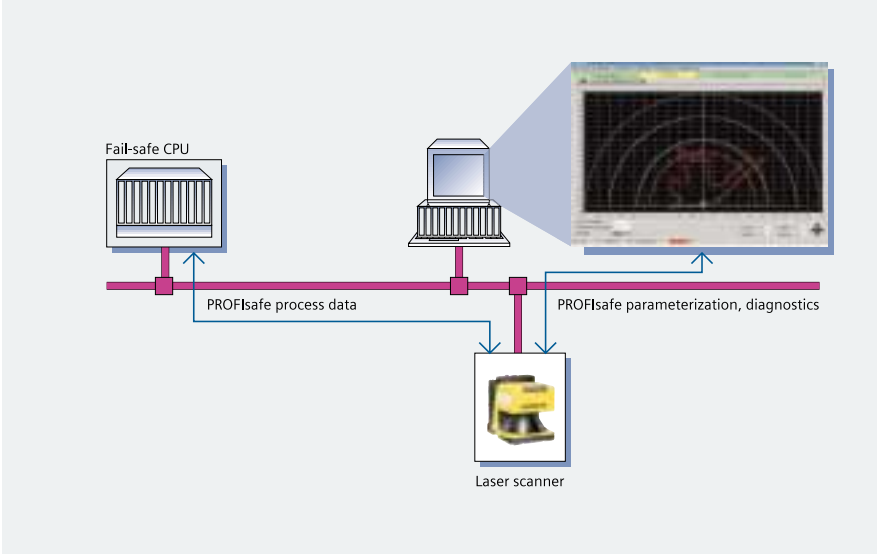


Fig. 4/8
Parameterizing and troubleshooting PROFIsafe components

4.2 ASIsafe

The AS-Interface system

Overview

The AS-Interface Safety concept (in the following abbreviated as "ASIsafe") allows safety-related components to be directly integrated into an AS-Interface network for fail-safe protection of man, machine and the environment. These safety-related components include Emergency Stop command devices, protective door switches and safety light grids.

Using ASIsafe, it is possible to shut down in safety-related fashion up to Category 4
(EN 954-1) or SIL3 (IEC 61508). This can be done but still keeping the advantages of simple wiring at a favorable cost.

The following advantages are obtained for machines and plant builders as a result of ASIsafe:

- Safety-related components can be simply integrated into the standard automation
- Favorably-priced design as neither fail-safe PLC nor a special master are required
- Safety systems can be more quickly configured using AS interface thanks to the flexible wiring
- Integrated diagnostics using AS interface increases the-service-friendliness of the system and allows fast troubleshooting. This significantly reduces downtimes.

This means that simple engineering and commissioning of AS-Interface also permits this to be achieved for safety-related technology.

Customer benefits

- Safety-related systems can be quickly configured thanks to the extremely flexible topology and simple connection system of AS-Interface.
- Minimum service times and down times thanks to the integrated diagnostics.
- Especially favorably-priced systems are possible without fail-safe PLC and without special master.
- Safety and non-safety data on one bus allow seamless, integrated automation solutions.
- The AS-Interface can be very easily configured with just a push of the knob on the master.
- Highest degree of safety: Certified up to Category 4 acc.to EN 954-1 and SIL3 acc. to IEC 61508.
- Safety systems can be simply engineered using straightforward, graphic software (“asimon”).
- Existing systems can be simply expanded.
- Certified by the German Technical Inspectorate and UL

Advantages

Advantages with respect to conventional safety technology:

- Shorter downtimes thanks to the integrated diagnostics.
- Higher flexibility by programming instead of hard-wiring the safety-related logic.
- Mounting and installation are significantly simpler, as, for example, no complicated feedback wiring is required for distributed shutdown operations.
- A solution can be simply duplicated on several machines/plants by copying the safety program.
- The safety logic can be simply modified by making the appropriate program changes.
- Only one interface to the HMI system - therefore seamless diagnostics.
- Reduced design and configuration times and costs thanks to the integrated diagnostics: The status of the safety system does not have to be signaled to the control using special I/O modules.
- Lower number of spare parts as the safety logic, programmed as user software, replaces the widest range of hardware.
- Fast overview of the safety functionality of the plant/system using a straightforward, graphic tool. This eliminates complex switching analyses when plants and systems are expanded.
- If, as a result of acceptance tests by the Germany Technical Inspectorate, additional safety measures are required, the flexibly wiring and configuring makes it simple to integrate additional safety-relevant components.

Advantages over other safety field buses:

- Neither a fail-safe PLC nor a special master are required
- Simple, non-shielded 2-conductor cable simplifies installation and also speeds it up
- The well-proven insulation displacement technique eliminates the time-consuming procedure of stripping insulation and assem bling bus cables
- Only one AS-Interface cable for safety and non-safety relevant communications
- Therefore only one interface to HMI systems
- The program blocks do not have to be additionally accepted by the German Technical Inspectorate.
- Extremely simple programming using graphic hardware-oriented tool (refer to Section 4).
- Hardware - such as Emergency Stop command devices, protective door switches and safety-related light curtains - can be directly incorporated using the integrated AS-Interface slave

Highlights

- Lower engineering costs
- Extremely straightforward and fast commissioning
- Lower costs as a fail-safe control is not required
- More efficient in operation thanks to the integrated diagnostics
- 40 ms response time

The following benefit from ASIsafe:
- Machinery and plant builders thanks to the cost savings, and
- Plant operating companies thanks to the higher plant availability and high degree of flexibility

Applications

ASIsafe has already been successfully used in many applications spanning all industry sectors.

For instance, the following applications were successfully secured using ASIsafe:

- Transport of goods on conveyor belts
- Presses
- Machining centers in the automobile industry
- Machine tools
- Escalators
- Paper machines
- Packaging machines in the food and beverage industry

Principle design and function

The basic design of an ASIsafe system is shown in the following diagram

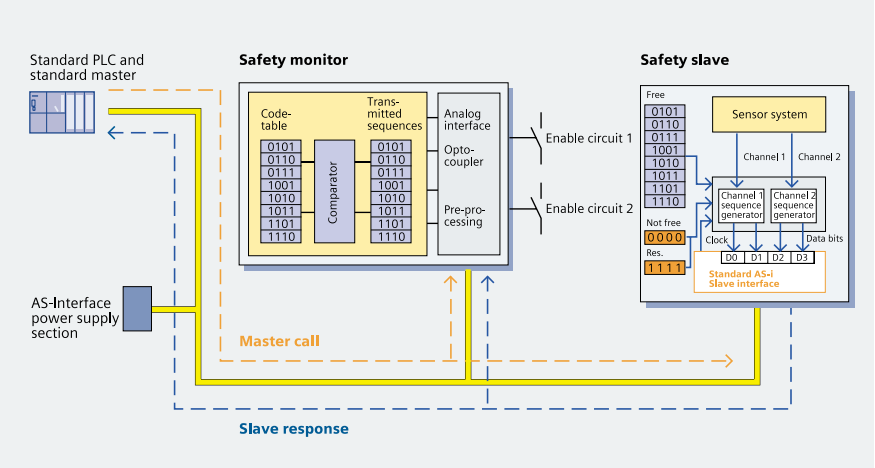


Fig. 4/9
Basic ASIsafe structure

A conventional AS-i network comprises a control/master, power supply unit, yellow AS-i cable and various slaves. Just two additional components are required for safety-related applications: A Safety Monitor and safety slaves.

A dynamic safety data transfer protocol forms the basis for secure data transfer.

In the factory, a code table is saved in every safety slave. This means that the safety monitor can uniquely identify it. Every safety slave must be parameterized in the safety monitor by the user acknowledging the prompt “teach-in safety slave”. Its associated code table is then saved in the comparator of the safety monitor. Each time that the master calls, a check is made by the comparator as to whether the expected code values match the actual code values.

If deviations occur or monitoring times are violated (watchdog), safe shutdown is initiated at the Safety Monitor through dual-channel enable circuits.

The code value “0000" is reserved for specific stopping. For example, if an Emergency Stop button is pressed, “0000" is sent to the safety monitor. This then initiates a safety-related shutdown via the appropriate enable circuit.

The safety monitor receives the safety-related code tables with the master interrogation, typical for the AS-Interface. The information is only sent to the master PLC - but it does not have an active role. For example, the information can be additionally evaluated for diagnostic purposes using the plant or system control.

Safety monitor functions

The AS-Interface safety monitor evaluates the safety-related inputs of the safety slaves and the inputs from the feedback circuit (refer to Fig. 4/10). Using logic blocks, it logically combines this information. This is used to determine the safety output of the enable circuit of a safety monitor.

In so doing, the safety monitor starts differently depending on the parameterized start blocks.

The AS-Interface safety monitor has a wide range of function blocks that allow the widest range of system configurations.

Functions of the safety monitor

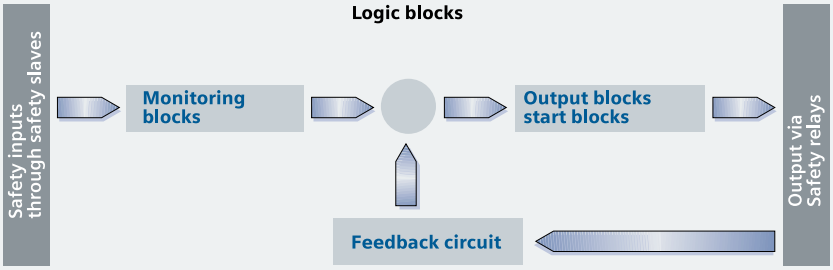


Fig. 4/10
Safety monitor functions

Monitoring blocks:

The safety-related slaves can be parameterized using the following monitoring blocks:

In addition, all monitoring blocks can be parameterized for starting tests and local acknowledgment.

Monitoring blocks	Function	Examples
Two-channel, positively-driven	Two redundant contacts; must be simultaneously actuated	Emergency Stop acc. to Category 3/4 (EN 954-1)
Two-channel dependent	Two redundant contacts; Both must be opened/closed after a synchronization time	Two-hand operations; Protective doors with two safety switches
Two-channel dependent with de-bounce	Two redundant contacts; Both must opened/closed after a de-bounce and synchronizing time	Slow-action switches Switch with high bounce times
Two channel conditionally dependent	Two redundant contacts; One contact is used for monitoring, the second contact is used for interlocking and monitoring	Door switch with interlocking
Two-channel independent	Two independent switching signals act on the inputs of a safety slave	Protective door monitoring acc. to Category 2 (EN 954-1)
Standard slave	Operational switching	-
Button	Local acknowledgment of several blocks	Common acknowledgment of light grids
NOP (No Operation)	Space retainer for a block to keep the block indices	The same, expanded diagnostics can be kept for different plant configurations

Table
Safety classes for the various configurations

Logic operation blocks:

The following functions can be selected to logically combine the safety-related inputs:

- AND
- OR
- Flip-flop
- Switch-in and switch-out delay times up to 300 s
- Pulses

Feedback circuit blocks:

These blocks allow the state of the downstream motor contactor to be monitored for dynamic checking (online).

Using these blocks, it is also possible to remotely reset the safety monitor when faults occur

Output blocks:

These blocks define how a safe standstill should be implemented. The following can be set:

- Stop Category 0 (immediate stop)
- Stop Category 1 (delayed stop up to 300 s)
- Door tumbler mechanisms with and without standstill monitor (for two conditional enable circuits of a monitor)

Starting blocks:

These blocks allow a plant or system to start in a defined fashion.
The following settings are possible:

Automatic restart

- Monitored start with an acknowledgment using a standard AS-i slave
- Monitored start using a start input at the safety monitor
- Monitored start using an acknowledgment signal from a safety-related AS-i slave

The safety system is simply and intuitively parameterized: The blocks are dragged & dropped into the appropriate enable circuit of the safety monitor.

By double-clicking on the appropriate block, this can be further configured using a dialog window that is then displayed.

ASIsafe is simply configured using asimon

Every monitor can be simply configured with the PC using the asimon configuring software. The PC is connected to the Safety Monitor using an appropriate cable.

The safety logic is parameterized by dragging & dropping.

To do this, for each safety function, the appropriate graphic safety components are simply dragged from the catalog into the enable circuit of the safety monitor to be tripped (refer to Fig. 4/11). In so doing, the operating modes as well as additional functions such as door tumbler mechanisms, stop Category 0 and 1, contactor monitoring, restart inhibit, local acknowledgment and agreement button can be set.

AND and OR logic blocks are also available.

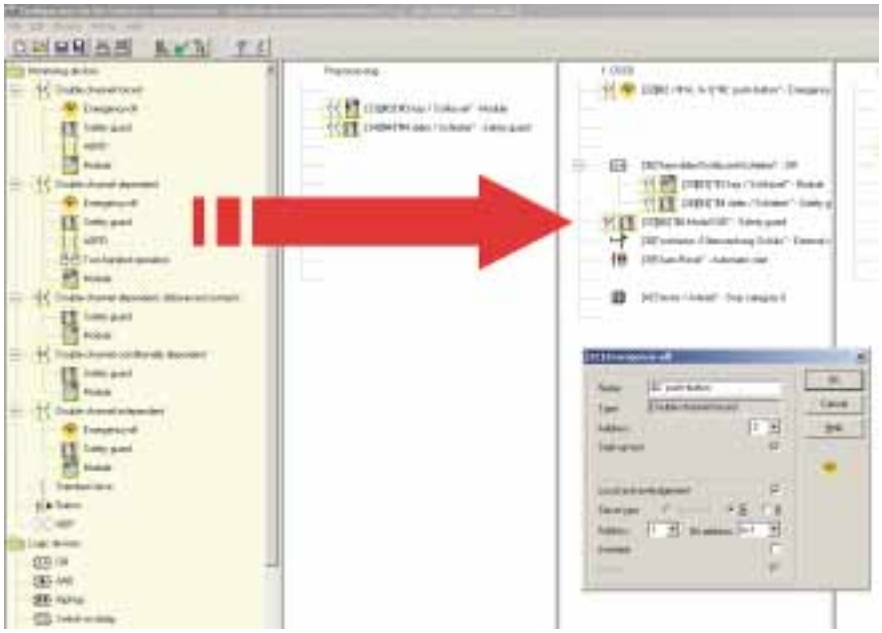


Fig. 4/11
asimon configuring software

Connecting safety-related signals between two AS-Interface networks

Safety-related data can be exchanged between two ASIsafe networks.

To do this, an enable circuit of a safety monitor from network 1 is connected to a safety-related input at a module from network 2.

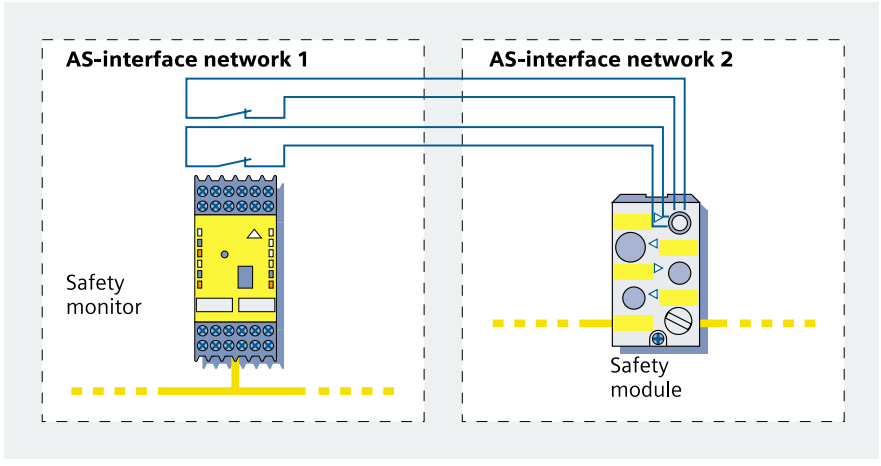


Fig. 4/12
Exchanging safety data between two ASIsafe networks

Grouping safety signals using ASIsafe

ASIsafe allows groups of safety-related signals to be formed.

The diagram shows a network which includes, in addition to standard components, two Safety Monitors, each with a 2-channel enable circuit and four safety-related slaves. For instance, each monitor is assigned a section of the plant or system which can then be powered-down via an appropriate enable circuit.

A PC is used to assign the safety-related slaves to the Safety Monitors.

The example is configured so that the safety module and Emergency Stop 1 act on safety monitor 1. This means that if, for example, Emergency Stop 1 is pressed, then the plant section, assigned to the monitor is shut down via the appropriate enable circuit.

Emergency Stop 2 acts on both safety monitors. This means that when Emergency Stop 2 is pressed, both plant sections are shut down.

Emergency Stop 3 only acts on safety monitor 2 and shuts down the plant section assigned here.

As shown in the example, several safety monitors can be used in one AS-Interface network. This means that not only can safety-related signals be grouped together, but it is also possible to combine various operating modes in a single network.

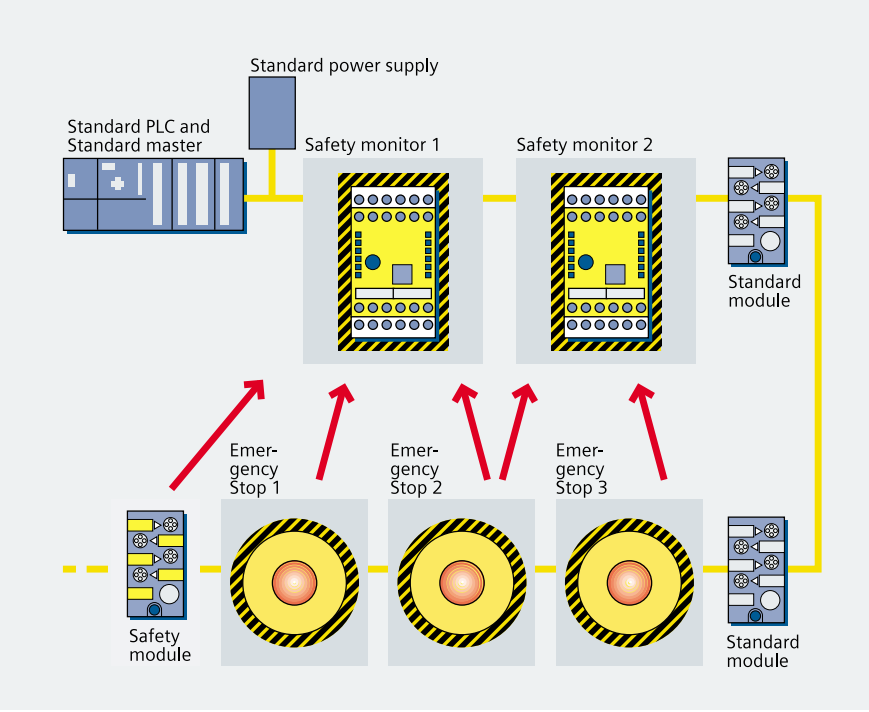


Fig. 4/13
Forming groups of safety components

Integrating into TIA

AS-Interface networks with ASIsafe

An ASIsafe network with Safety at Work components can be subordinate to a distributed ET 200S I/O station. In this case, an enable circuit of a safety monitor is wired-into the safety circuit of the ET 200 S. The response time of the ET200S SIGUARD of 20 ms is added to the response time of ASIsafe (max. 40 ms).

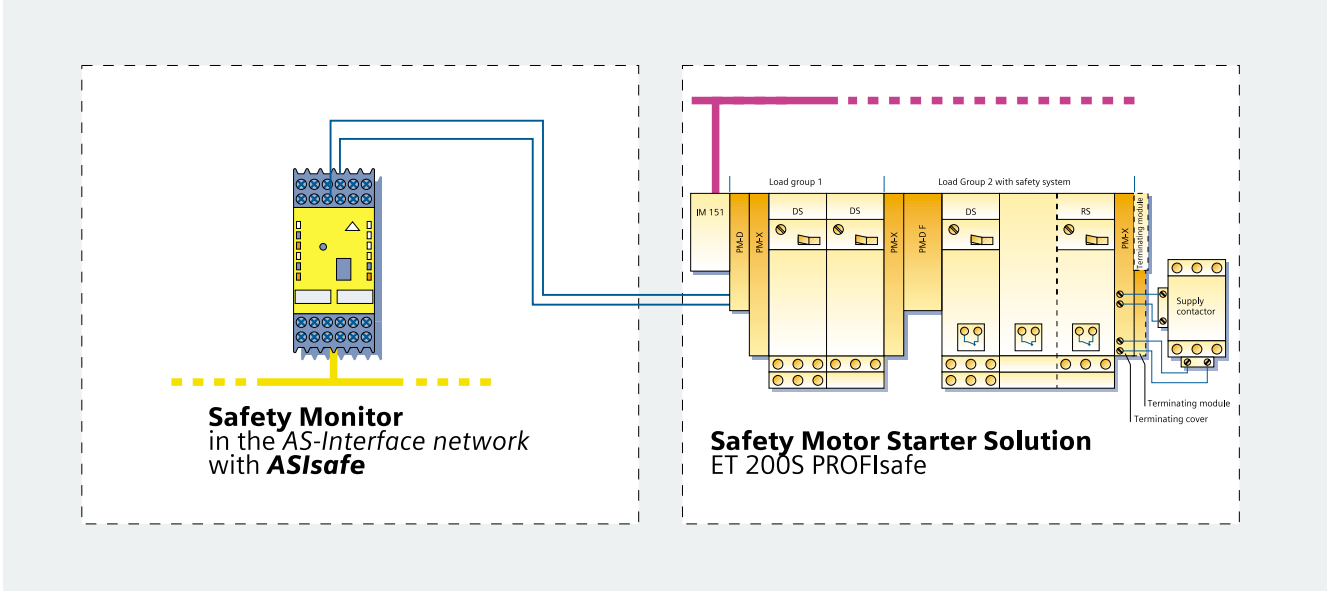


Fig. 4/14
ASIsafe under ET 200S Motorstarter

Simple diagnostics

If a safety slave is initiated, then it transfers “0000”.

This information is available at the master and can be simply evaluated by the control.

Detailed diagnostics

In addition to the pure asimon configuration software, Siemens also supplies function blocks for the S7-200 and S7-300 on the ASIsafe CD-ROM. This allows detailed diagnostics to be carried-out for all of the parameterized blocks (refer to Fig. 4/15).

To do this, an AS-i address must be assigned at the safety monitor using the configuration software. The evaluation is made using function blocks in the PLC.

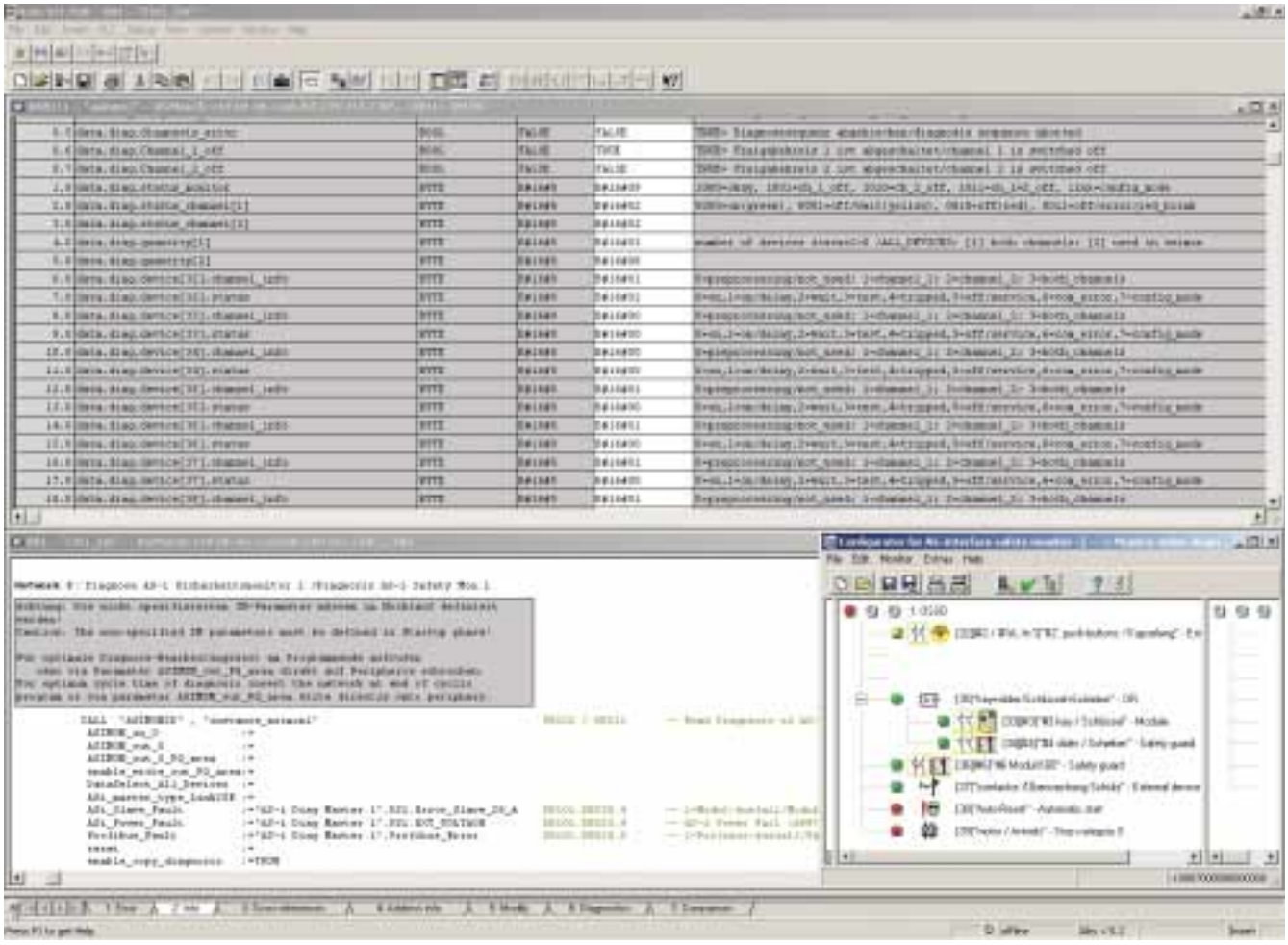
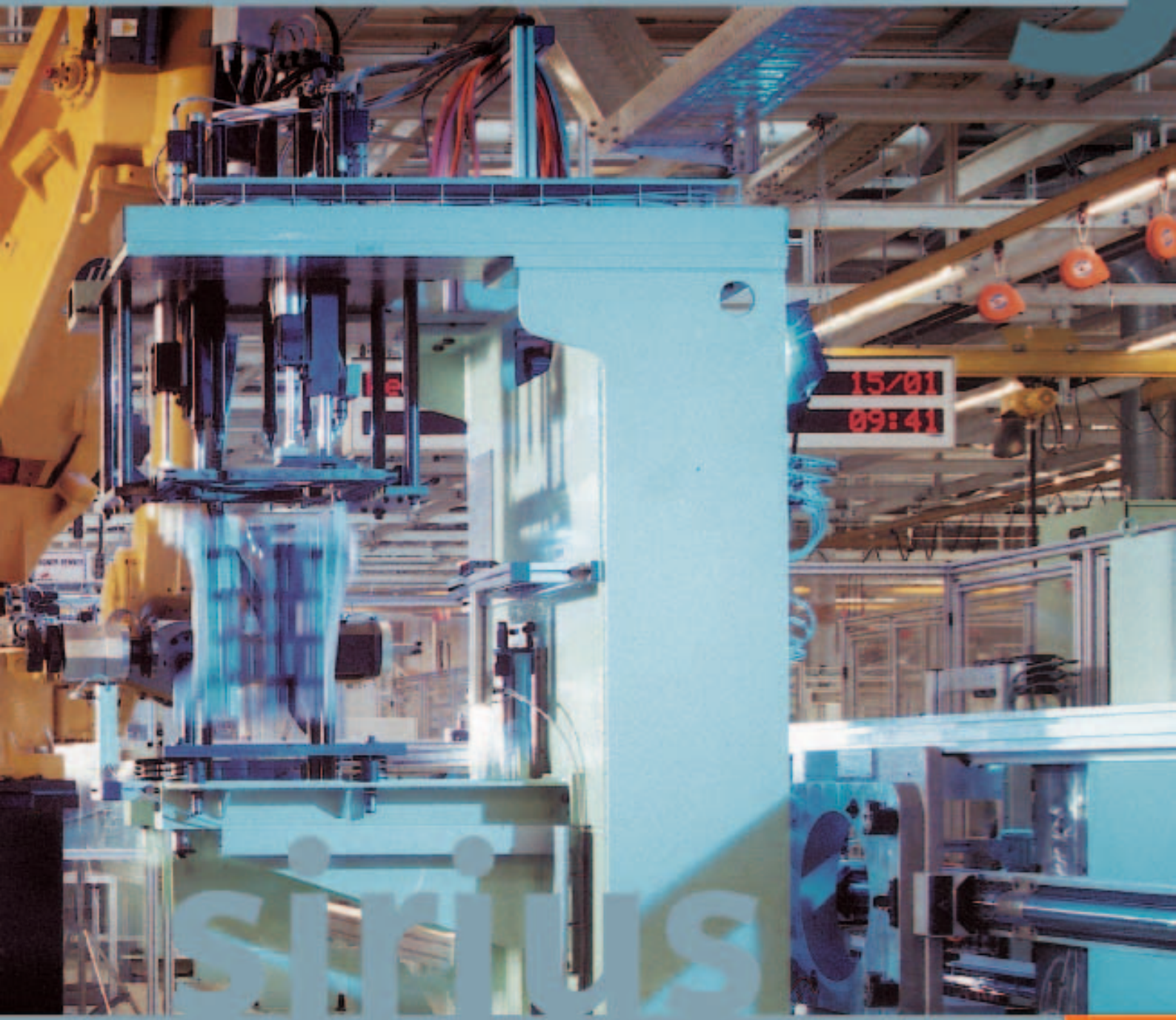


Fig. 4/15
Function block for detailed diagnostics of the ASIsafe network in the PLC

Safety industrial controls

5



5 Safety industrial controls

5.1 SIRIUS position switches

Overview

SIRIUS position switches are used to

- Detect the position of moving machine parts and components
- Detect and sense hazardous motion of machine parts and components
- Monitor protective devices with joints such as swiveling doors, hatches, etc.
- Monitor protective devices that can be laterally shifted - such as sliding doors, protective meshes etc.

Features

SIRIUS position switches offer

- A comprehensive range of products with standardized enclosures and operating mechanisms/actuators
- Simple to mount solutions to detect and monitor hazardous motion and access areas.
- Standardized device mounting acc. to Standard EN 50041 and EN 50047
- Maximum protection against tampering and manipulation of the protective devices - e.g. using multiple coded, separate actuators
- Protective devices are monitored up to Category 4 acc. to EN 954-1
- Integrated in the ASIsafe bus system
- High degree of protection, even for standard products

Applications

SIRIUS position switches are used, among other things, for the following tasks:

- In the plant and machinery area to monitor protective barriers and access hatches on printing machines.
- Position switches with tumbler mechanism are predominantly used to monitor parts of the machine with increased potential hazard - such as robot cells. A protective door is safely locked until the machine comes a standstill.
- A plant or system is safety shut down when it reaches the appropriate end stop, e.g. for elevators and escalators.
- Protective doors are monitored using magnetically-operated switches that are immune to manipulation when the switch is mounted so that it is covered - this also plays a significant role in areas requiring cleaning and disinfection.

Standard position switches

Thanks to the wide variety of actuators, enclosures and contact systems that are required in the field, SIRIUS 3SE position switches are convincing in almost every application.
With positively opening contacts.
Versions with dimensions, mounting points and characteristic values are available that are in compliance with Standards EN 50041 to EN 50047.

As a result of their significantly lower switching distance and precise switching points, our short-stroke switches ensure safe shutdown even for extremely short actuation travel.

Position switches with separate actuator/tumbler mechanism

A wide variety of enclosures and actuator versions is available to monitor protective doors.
Thanks to the multiple mechanically coded actuator, it is not possible to simply bypass protective devices.
With positively opening contacts.
Tumbler mechanism:
Position switches with separate actuator and tumbler mechanism keep a protective door interlocked until the operating zone can be entered without incurring any danger. An electrical signal, e.g. from a standstill (zero speed) monitor controls the interlocking solenoids and there fore releases the protective door.

Interlocking with spring force (closed-circuit principle) as well as interlocking with solenoid force (open-circuit principle) versions with 4 contacts as standard are available.

Hinge-mounted switches

Versions with a standard enclosure acc. to EN 50047 to be mechanically connected to the hinge axis as well as hinge-mounted switches with already mounted hinge are available.
With positively opening contacts.
The NC contacts already open at protective door opening angles of 4 degrees and issue the command to shut down. For versions with snap-action contacts, the signaling command (NO contact) is simultaneously issued with the shutdown command (NC contact).

Magnetically-operated switches

These contactless magnetically-operated switches offer a high degree of protection against manipulation. They are available in 3 different designs.

The safety-related evaluation and monitoring to achieve Category 4 acc. to EN 954-1 is realized using the 3TK284, 3SE6 safety relays, ASIsafe and F-SIMATIC.

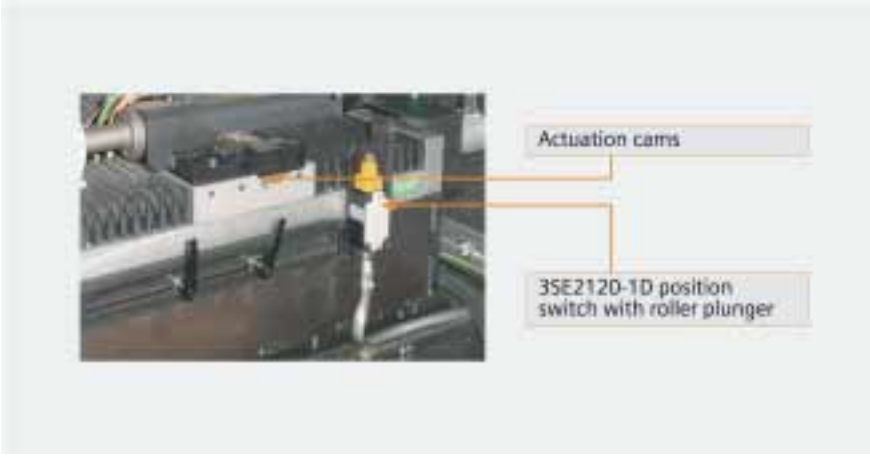
Design

- Standard switches:
  Modular design with replaceable elements (actuator head, enclosure, contact blocks).
- Separate actuator as well as switches with tumbler mechanisms:
  Fixed contact unit can be combined with various actuators (standard actuators, with lateral mounting and radius actuators).
- Hinge-mounted switches:
  Compact contact unit that is directly mounted on the hinged axis or with already pre-assembled hinge.
- Standard connections for mechanical position switches:
  Metric glands, preferably M20x1.5. Versions with M12 connector and multi-pole connectors are available.
- Magnetically-operated switches:
  Compact, device cast in resin where the connecting cables are already connected.

Examples

1. Standard switches:

Sensing end positions and endstops on tool slides in special-purpose machinery construction



2. Switches with separate actuator:

Protective door monitoring for automatic production equipment

3. Hinge-mounted switches:

Monitor access hatches for wood-working machines

4. Magnetically-operated switches:

Possible combination of monitoring unit - magnetically-operated switch system

Possible combination – monitoring unit – magnetically-operated switch

Monitoring unit	**Magnetically-operated switch** 1NC/1NO			**Magnetically-operated switch** 2NC
	contact 3SE6 605-1BA (M30)	**contact 3SE6 605-2BA** (25 x 33 mm)	**contact 3SE6 605-3BA** (25 x 88 mm)	**contact 3SE6 604-2BA** (25 x 88 mm)
	Switching relay 3SE6 704-1BA	**Switching relay 3SE6 704-2BA**	**Switching relay 3SE6 704-3BA**	**Switching relay 3SE6 704-2BA**
Relay output SIRIUS safety relay, 6-fach [1] 3SE6 806-2CD00	•	•	•	–
Electronics output SIRIUS safety relay, electronic [2] 3TK284.	–	–	–	•
SIRIUS safety relay, with contactor relay, electronic [2] 3TK285.	–	–	–	•
SIRIUS safety load feeders electronic [2] 3RA7.	–	–	–	•
ASIsafe [2] 3RK1.	–	–	–	•
SIMATIC ET 200S [2] PROFIsafe [2] 4/8F-DI DC24V	•	•	•	•
SIMATIC ET 200M [2] SM326, DI DC24V SIMATIC S7 300F [2] SM326, DI 8 x Namur	•	•	•	•

[1] Category 3 acc. to EN 954 can be achieved

[2] Category 4 acc. to EN 954 can be achieved

Technical data

SIRIUS position switches	
Standard position switches	• **Positively opening contacts, acc. to IEC 947-5-1** • **High contact reliability even at 5V DC / 1mA** • **Suitable for ambient temperatures from -35° to +85°C** • **Extremely high mechanical endurance (30 million switching operations)** • **High IP67 degree of protection** • Various NC/NO contact versions - up to 4 contacts are possible • Enclosure in compliance with EN 50041, EN 50047 and special designs
Position switches with separate actuator/ tumbler mechanism	• **Moulded plastic or metal enclosure in IP66 and IP67** • **Enclosures acc. to EN 50047, EN 50041 and Special designs** • **Safety standard for protective door interlocking functions acc. to EN 1088** • **Can be approached from 4 or 5 directions** • **High IP65 or IP67 degree of protection** • **Mechanical endurance $1x10^6$ operating cycles** • **Ambient temperature from -30^o to $+85^oC$** • Various NC/NO contact versions, up to 4 contacts possible, as well as position monitoring of the actuator and the interlocking solenoids with up to 2 contacts.
Hinge-mounted switches	• Enclosure acc. to EN 50047 for hinge mounting 1NO/1NC snap-action, 5 degrees or 15 degrees switching point • Switch with integrated hinge for 40 mm profile, switching point 4 degrees, 5 or 15 degrees, 1NO/2NC slow-action contacts

5.2 SIRIUS Emergency Stop

Overview

The SIRIUS Emergency Stop command devices are used to manually shut down plants and systems when hazards occur and are initiated by operating personnel (acc. to ISO 13850 (EN 418)).

Features

SIRIUS Emergency Stop command devices distinguish themselves as a result of:

- Extensive product range with various Emergency Stop operator components
  - rotate to release
  - pull to release
  - key-operated release
- Can be simply and quickly mounted
- Plastic and metal versions
- Embedded - among other things in the AS-Interface bus system

The following advantages are obtained:

- Can be used up to Category 4 acc. to EN 954-1 thanks to the positively-opening NC contacts
- High degree of protection up to IP67
- Harmonized range of command and signaling devices
- Directly connected to ASIsafe, directly connected to the yellow profiled cable

Applications

In all types of plants and machines, Emergency Stop command devices allow plants and systems to be manually shut down when hazards arise and are used in the following industry sectors:

- General machine construction
- Automation technology
- Special-purpose machine building
- Woodworking industry
- Machine tool construction
- Food and beverage industry

Product family/product groups

The family of SIRIUS command devices includes, in addition to Emergency Stop actuators:

- Pushbuttons
- Indicator lights
- Selector switches
- Key-operated switches
- Emergency Stop command devices

These devices are available either in round or square moulded-plastic versions as well as in round metal versions.

The Emergency Stop command devices can be used up to Category 4 acc. to EN 954-1. They all have positively-opening contacts.

For safety-related evaluation and monitoring, 3TK28, ASIsafe and F-SIMATIC are used in order to achieve Category 4 using a safety-related module.

Design

The command devices have a modular design and comprise actuator elements such as Emergency Stop, pushbutton as well as a holder to retain the device in the front panel hole and the contact elements and lamp sockets that can be snapped-in.

The actuator elements are mounted in a standard 22.5 mm front panel hole and are retained from the rear using clips. Contact elements and lamp sockets are snapped onto the rear of the actuator element.

Contact elements and lamp sockets are available with either screw terminal, Cage Clamp terminal as well as solder pins that allow them to be soldered onto PC boards.

Example

Automated production line with Emergency Stop command devices located at exposed positions. These are used to manually shut down the line or module when a hazard occurs.

Technical data

SIRIUS Emergency Stop	
Degree of protection	IP66 (plastic versions) IP67 (metal versions)
Mounting hole	22.3 mm+0.4 mm (round designs, plastic and metal) 26 x 26 mm (square plastic versions)
Rated operating voltage	400 V, AC 12
Rated operating current	10 V, AC 12
Contact reliability (test voltage, current)	5 V, 1 mA

5.3 SIRIUS command and signaling devices

Overview

SIRIUS command devices are used to manually shut down plants when hazards occur and this is initiated by operator personnel. Classic Emergency Stop command devices (acc. to ISO 13850 (EN 418)) are available for this purpose.

SIRIUS signaling devices are used to visually and acoustically signal machine and plant states. Signaling devices are available for the modular range of "SIRIUS 3SB3 command and signaling devices" as well as the 8WD signaling columns with a comprehensive range of accessories.

Features

SIRIUS command devices include:

3SB3 Emergency Stop pushbuttons

- Extensive product range with various Emergency Stop operator components - release by turning, pulling and key-release
- Emergency Stop function acc. to ISO 13850 (EN 418)
- Fast and simple to install
- Moulded plastic and metal versions
- One-man installation without any special tools
- Actuator elements can be equipped in a modular fashion
- Extensive range of accessories
- Embedded, among other things, in the AS-Interface bus system

3SB3 two-hand operator consoles

- Solution in compliance with the Standards acc.to EN 574 and DIN 24980
- Emergency Stop function acc. to ISO 13850 (EN 418)
- Moulded plastic and metal versions
- Rugged metal versions for the toughest of application conditions
- AS-Interface solution that can be retrofitted

3SE7 cable-operated switches

- Emergency Stop function acc. to ISO 13850 (EN 418)
- Versions for cable lengths up to 100 m
- LED signal display with high intensity
- Monitoring function for cable breakage and cable tension
- Integrated ASIsafe

3SE29 foot switch

- Latching function acc. to ISO 13850 (EN 418)
- Rugged metal versions as well as favorably-priced plastic pedal button
- Available with and without protective cover

SIRIUS command devices offer:

3SB3 Emergency Stop pushbuttons

- Embedded in the installation-friendly range of "SIRIUS command and signaling devices 3SB3" products
- Various colors using incandescent lamps and LEDs
- Moulded-plastic and metal versions
- High IP67 degree of protection and NEMA4

Signaling columns 8WD4

- Modular design, up to 5 modules per column
- Simple to mount and change lamps without tools
- Connected to AS-Interface
- High IP65 degree of protection
- Extensive range of accessories

Applications

SIRIUS command and signaling devices allow, in all types of plants and machines, the hazard to be manually shut down and are mainly used in the following industry sectors.

- General machinery construction
- Automation technology
- Special-purpose machine construction
- Woodworking industry
- Machine tool construction industry
- Food and beverage industry

Cable-operated switches are used in plants extending over a wide area - for example, transport conveyor belts in open-cast mining or material feeder belts for printing machines.

Product family/product groups

3SB3 command and signaling devices

The complete 3SB3 spectrum includes a very extensive range of products for front panel mounting as well as many standardized and customer-specific enclosures.

Solutions are available for the complete range to connect to AS-Interface.

3SB3 two-hand operator consoles

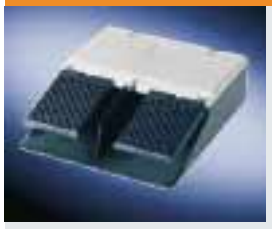
Various versions in moulded plastic and metal are available so that both hands are required to control presses and punches. These can be mounted directly at the machine as well as on a stand (accessory). The two-hand operator consoles are equipped, as standard with two push-buttons and one Emergency Stop mushroom pushbutton.

3SE7 cable-operated switches

System comprising cable-operated switch and cable.

Cable-operated switches are, depending on the length of cable required, available in various designs. Cable lengths of up to 100 m are possible. Different contacts are available for each design.
In order to visualize the state of the cable-operated switch, the switch can be equipped with an LED display.
Extensive range of accessories.

3SE29 foot switches



Foot switches in a 1 or 2-pedal version with momentary and latching contacts.
The foot switches are available with a rugged protective cover for additional protection.

8WD signaling columns

Available elements:
Steady-light, single-flash light, rotating beacon, repeated flash light and siren elements
Colors: Red, yellow, green, blue, clear (white)
Devices are connected using screw and Cage Clamp terminals.
Up to 5 elements can be mounted for each signaling column. They can be directly connected to the AS-Interface bus system using the integrated ASI module.
Various acoustic modules up to 105 dB are available.

Design

SIRIUS 3SB3 command devices have a modular design and comprise actuator elements such as Emergency Stop, pushbuttons as well as holders for mounting in front panel holes and contact blocks and lamp sockets that can be snapped in.

The actuator element is mounted in a standard 22.5 mm front panel hole and retained from the rear with the holder. Contact blocks and lamp sockets are snapped onto the rear of the actuator element.

Contact blocks and lamp sockets are available with screw terminals, Cage Clamp terminals (spring-loaded terminals) as well as with solder pins for soldering into printed circuit boards.

Technical data

SIRIUS position switches	
2SB3 commanding	• IP66 degree of protection (moulded-plastic versions), and signaling devices IP67 (metal version) • Mounting hole 22.3 mm+0.4 mm (round versions, moulded plastic and metal), 26 x 26 mm (square plastic versions) • Rated operating voltage 400 V, AC 12 • Rated operating current 10 V, AC 12 • Contact reliability (test voltage, current) 5 V, 1 mA
3SE7 cable-operated switch	• Metal enclosure in degree of protection IP65 • Electrical loading AC 15 400 V AC, 6 A • Short-circuit protection 6A (slow-acting) • High IP65 or IP67 degree of protection • Mechanical endurance >1x10^6 operating cycles • Ambient temperature from –25^O to +70^{O}C • Various NC/NO contact versions, up to 4 contacts are possible
3SE29 foot switch	• Metal enclosure in degree of protection IP65 , plastic • Electrical loading AC15 400 V AC, 6 A or 16 A • Short-circuit protection 6 A (slow-acting) or 16 A • High IP65 degree of protection • Mechanical endurance >1x10^6 operating cycles • Ambient temperature from –25^O to +80^{O}C • Various NC/NO contact versions
8WD signaling columns	• Connecting element: Rugged thermoplastic enclosure • Light elements: Thermoplastic • Operating voltages: 24 V AC/DC, 115 V AC and 230 V AC • High IP65 degree of protection • Ambient temperature from –30^O to +50^{O}C

5.4 SIRIUS safety relays

Overview

Safety relays are used to initiate, as a result of an actuated contact (e.g. by actuating Emergency Stop, entering a hazardous range), the appropriate response to safely and reliably protect man, machine and the environment.

Typical plants and systems, in which safety relays are used, distinguish themselves by a low number of sensors, a smaller footprint as well as the fact that they are independent of a bus system (island operation).

SIRIUS safety relays fulfill, on one hand, the requirements of the relevant safety standards, and on the other hand, the requirements of industry thanks to their compact design and their reliability. They are an essential component of the Siemens Safety Integrated safety concept.

They are subdivided into 2 groups:
a) 3TK28 safety relays
b) 3RA71 safety load feeders

Features

SIRIUS safety relays offer users a whole raft of technical advantages. They are harmonized with one another and can be cascaded. This permits a high degree of flexibility to be realized when expanding the safety functions in an existing plant or system. All of the devices that are required to implement safety circuits - from the sensor through the safe evaluation up to the actuator - are available in the SIRIUS product range. The compactness of the safety relays in the SIRIUS optical design allow electrical cabinets to be configured with the same harmonized look & feel. What is especially interesting for companies that export their machines is the fact that our SIRIUS safety relays are certified for worldwide use. Another significant advantage - especially for this group of customers - is also the fact that SIRIUS safety relays operate without any wear (electronic family of devices) or with alternating switching sequences (devices with mounted contactor relays and safety load feeders) achieve and extremely high lifetime. This significantly reduces the number of service calls.

The features at a glance:

SIRIUS safety relays:

- Monitor safety functions
- Are a necessary component of the safety circuit
- Protect man, machine and the environment

Applications

SIRIUS safety relays are used wherever sensor signals must be reliably evaluated and where it is necessary to shut down hazardous states in a safety-related fashion, e.g.

- Monitoring areas with hazardous motion, e.g. protective door, light grid, light barrier
- Monitoring the movement of vehicles used at the shop floor using laser scanners
- Safely stopping and shutting down after an Emergency Stop has been initiated

These applications are used

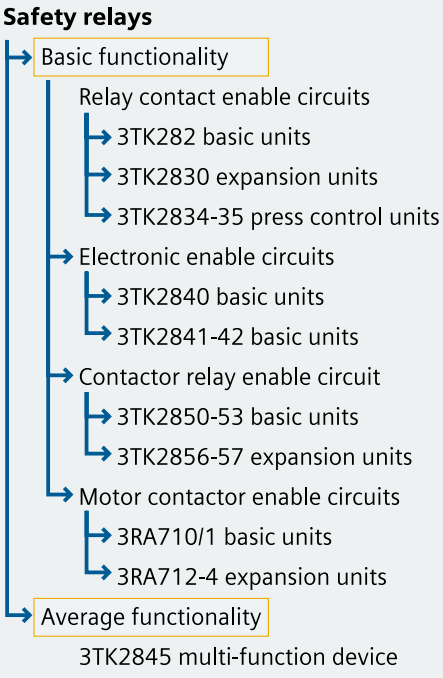
- In the automobile industry and the companies that supply the automobile industry
- In general machine construction
- In paper production and printing
- In conveyor technology
- In the food and beverage industry

Product family/product groups

The family of SIRIUS safety relays is subdivided into devices with basic and average functionality. Devices with a basic functionality have one input to connect a safety sensor. When the sensor is triggered, all of the safety-related enable circuits are shut down - either instantaneously or with a time delay. Devices with an average level of functionality have two or several sensor inputs. The safety-related enable circuits of these devices are assigned to sensor inputs via a safety logic.

The 3TK28 / 3RA71 safety relays fulfill, depending on their external circuitry, safety requirements up to Category 4 acc. to EN954-1 and SIL 3 acc. to IEC 61508 (detailed information about the individual devices is provided in Catalog LV10 Order No.: E86060-K1002-A101-A4).

SIRIUS safety relays can be parameterized without having to use software tools. As a result of the preset functionality, these devices are ready to operate after they have been installed.



Design

SIRIUS safety relays without integrated contactor relays are available in two compact enclosures in the SIRIUS design (22.5 and 45 mm wide). The electronic safety relays with integrated contactor relays as well as the safety load feeders are 90 mm wide.

All of these devices are designed to be snapped onto 35 mm mounting rails in compliance with EN 50022. 22.5 and 45 mm wide devices can also be screw-mounted using additional push-in lugs. Push-in lugs are available as accessory with Order No. 3RP1903.

The connecting cables are connected to the device at the top and bottom. The screw or Cage Clamp terminals are accessible from the front of the device. This feature allows the devices to be simply mounted in a transparent fashion. The terminal blocks can be removed from the devices. This means that when service is required, plant downtimes can be reduced to an absolute minimum.

Functions

SIRIUS safety relays are used to evaluate safety sensors and to monitor safety functions.

According to the requirements of the Standards, the devices must ensure that

a) Faults in the safety relay or in the sensor/actuator circuit must be identified early on in order to prevent loss of the safety function.

b) The safety function is always kept even if faults occur.

In order to fulfill the above requirements, there are some significant differences between safety relays and non-safety relays.

Basic devices

Monitoring the sensor circuit

Safety relays monitor sensors for cross-circuit faults (2-channel connection) and welded contacts. This is realized differently depending on whether it involves an electronic or a relay device.

Cross-circuit fault: For the relay device, as a result of the cross-circuit fault, the P potential at the relay is connected to ground bypassing the relay. This means that the relay drops-out and the hazard is shut down. For the electronic version, the electro-mechanical sensors are monitored using electronic pulses. If the received pulses do not match the sent pulses, then the device shuts down.

Welded sensor contact: Before the device can be switched-in, both sensor inputs, for a two-channel connection, must have been opened once, otherwise the device does not switch-in.

Monitoring the actuator circuit

External contactors that are used to switch the load circuit of the hazardous motion, are also monitored by the safety relay. This device has inputs to connect the feedback signal contacts of the contactor. If the contacts are not closed, the safety relay cannot be switched-in. The contactors, controlled from the device, have positively-driven contacts. The contactor has load and signaling contacts that cannot be simultaneously closed. This function ensures that the safety relay can no longer be switched-in when a load contact welds.

Monitoring its own function

As a result of the redundant inner circuitry of the switching relay, and the fact that the functions mutually monitor one another, a fault in a component results in the hazardous motion being shut down. Two safety relays are redundantly incorporated in the devices. These safety relays mutually monitor their functions.The electronic devices have two microcontrollers that mutually monitor their function. When a fault occurs in one of the microcontrollers, the device shuts down the potentially hazardous motion. This means that even if the device has a fault condition, the safety function is kept.

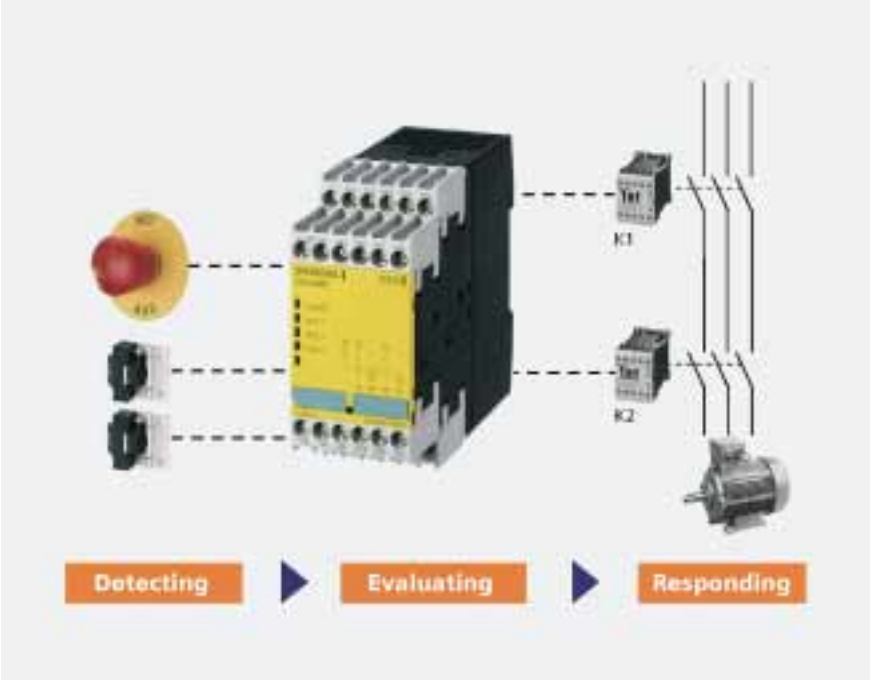
Device faults and operating states are signaled using an LED on the front panel.

Safety relays are mainly used to implement safety functions in plants and systems with a small footprint without being connected to a bus system (island operation). These devices are always used in a so-called safety circuit. A safety circuit comprises the functions - DETECTING, EVALUATING and RESPONDING.

Detecting: Detecting a safety request using a sensor - e.g. when an Emergency Stop pushbutton is actuated or a protective door opened.

Evaluating: Evaluating the signal from the sensor and monitoring the complete safety function using the safety relay.

Responding: Shutting down a hazardous motion



Expansion unit

If the number of safety-related enable circuits available at the basic unit, is not sufficient for the particular safety relevant application, then this number can be increased using an expansion unit (contact multiplier). An expansion unit only has this safety-related input that is controlled using a safety-related output of the basic unit. The basic unit monitors the function of the expansion unit via the feedback signal contact of the expansion unit. Expansion units may only be used in conjunction with basic units and achieve the same safety category as the basic unit.

Press control unit

Presses are one of the most hazardous machines. In order to protect the operator from e.g. irreversible injury, the two-hand operating console forces him to use both hands to operate the press ensuring that both hands are kept outside the hazardous zone.

The 3TK2834 press control unit is used to evaluate the two-hand operator console.

The unit detects the following faults:

- Short-circuit, e.g. between the pushbuttons
- Defective relay coils
- Broken conductors
- Welded contacts

The enable circuits cannot be switched-in, if

- The pushbuttons are not pressed at the same time (≤ 0.5 s)
- Only one pushbutton is pressed
- The feedback circuit is open

Integration

The 3TK28 / 3RA71 safety relays are part of the Safety Integrated system. These relays are preferably used in standalone operation. This means that a bus connection is not required. Depending on the type of unit being used, operating states as well as also diagnostics data can be signaled to a higher-level control via the signaling outputs.

In order to implement the safety-related functions for more complex plants and systems, or to expand existing plants or systems, the safety relays can be cascaded (AND logic). This means that the units can be connected to one another. This allows, for example, the number of safety-related outputs to be multiplied (with expansion blocks), or also shutdown groups formed (selective shutdown).

In order that the safety circuit described above can function, sensors and actuators for the SENSING and RESPONDING functions must be connected to the safety relay.

For sensors, a differentiation is made between sensors with contacts and electronic sensors.

Sensors with contacts include, e.g.

- Emergency Stop command devices
- Hinge-mounted switches
- Position switches
- Cable-operated switches
- Contact mats
- etc.

Electro-sensitive protective devices with semiconductor outputs include, e.g.

- Light barriers
- Light curtains/grids
- Laser scanners
- etc.

Contactors from the modular SIRIUS system are used, for example, as actuators. For the 3TK285 and 3RA71 safety relays, these contactor relays or load contactors are already integrated.

The use of these relays offers two decisive advantages:

1. Lower wiring costs thanks to the pre-configured wiring in the factory

2. Fewer possible fault sources when locally connecting-up and installing

SIRIUS safety relays can be seamlessly integrated in the Totally Integrated Automation (TIA) concept. The safety relays can be directly controlled from the higher-level plant control (e.g. PLC) using the cascading input or via the input for normal operational switching. This means that normal operating switching is possible - i.e. no additional controls are required to switch the load. The safety-related function always has a higher priority over operational switching.

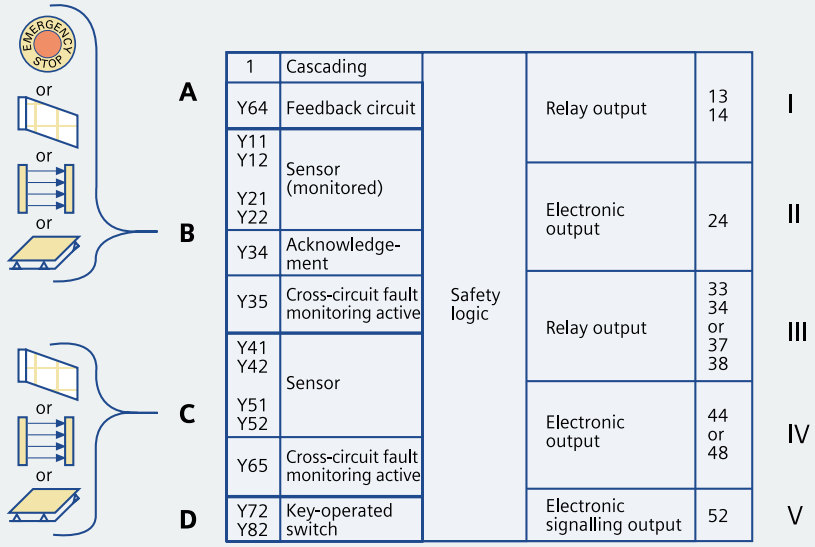
Examples

Application:

A processing machine has a protective door and an Emergency Stop function. The tool of the machine must be regularly replaced. To do this, the protective door must be opened. It is possible to toggle between maintenance operation and normal operation using a key-operated switch.

This function is implemented using a 3TK2845.

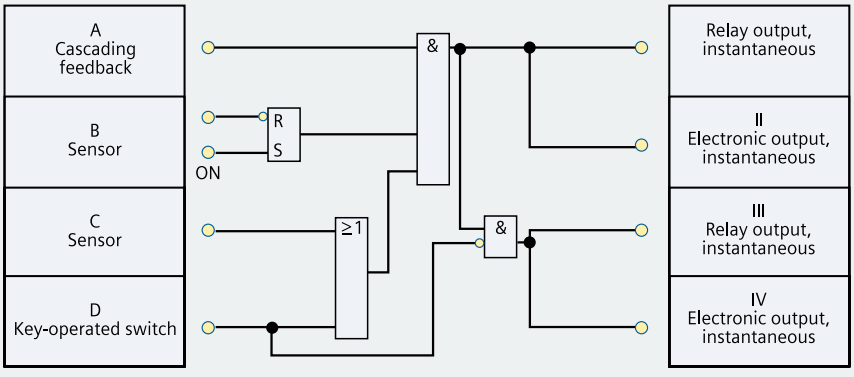
Fig. 5/1
3TK2845



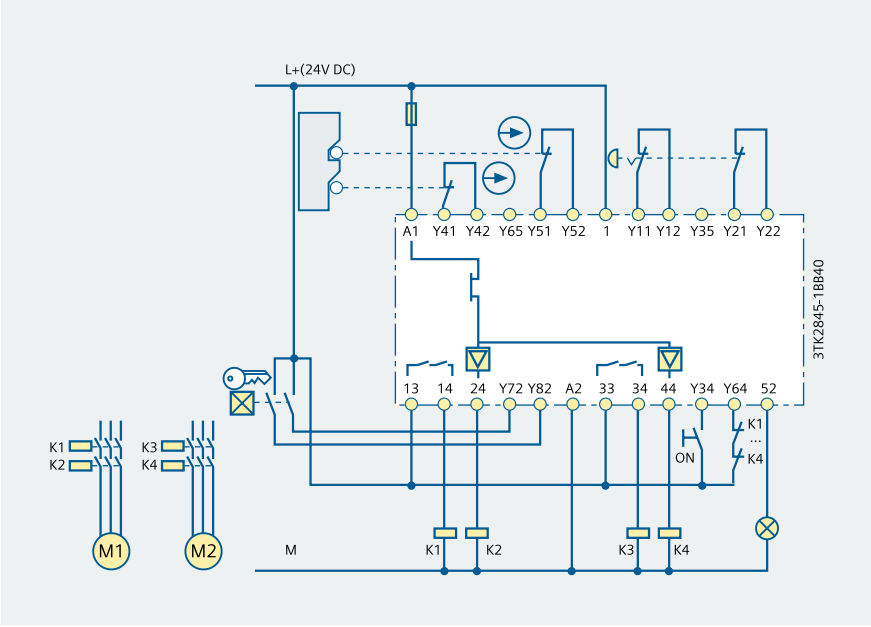
Normal operation: When the protective door is opened or the Emergency Stop is actuated all of the outputs of the evaluation unit are shut down.

Maintenance operation: Only the hazardous motion is shut down using the key-operated switch. The auxiliaries continue to run. When the protective door is opened, the outputs are no longer shut down. When the Emergency Stop is actuated, then, as before all of the outputs are shut down.

Safety logic



Circuit example



Normal operation:

When an Emergency Stop is issued or the protective door actuated, then outputs 14, 24 (M1), 34, 44 (M2) are switched-out. It is only possible to power-up the system again after the Emergency Stop command device has been released, the protective doors and the feedback circuit (RF) at Y64 are closed. After the Emergency Stop command device has been actuated, then in addition, the ON button at Y34 must be pressed. After the protective door has been closed, the outputs are automatically switched-in again.

When the key-operated switch is actuated (to activate service operation): Outputs 34, 44 (M2) shut down (suitable to reduce the speed or drive components are not operational).

Service operation:

The position switches of the protective doors are not evaluated. Outputs 34 and 44 (M2) are switched-out.

When the Emergency Stop command device is actuated, outputs 14 and 24 (M1) are switched-out.

The system can only be powered-up again after the Emergency Stop command device has been released, the feedback circuit at Y64 is closed and the ON pushbutton Y34 is pressed.

Comment:
For Category 4, it is not permissible to connect several position switches in series for the protective door monitoring (fault detection).

		Safety outputs					
	Max. Category	Contacts		Electronic		Signaling circuit	
	acc. to EN 954-1	Stop Cat. 0	Stop Cat. 1	Stop Cat. 0	Stop Cat. 1	Contact	Electronic
Basic functionality (1 safety-related sensor can be connected)							
Electronic enable circuits							
Instantaneous, safety outputs							
3TK2840-.BB40 Basis unit	3	--	--	2	--	--	--
3TK2841-.BB40 Standard unit	4	--	--	2	--	--	--
Delayed, safety outputs							
3TK2842-.BB4. Standard unit with time delay 3s - 300s	4	--	--	1	1	--	--
Relay contact - enable circuits							
Instantaneous, safety outputs							
3TK2821-.CB30 Basic unit, auto start	3	3	--	--	--	1	--
3TK2822-.CB30 Basic unit, auto start	4	2	--	--	--	--	--
3TK2824-..... Basic unit, auto start	4	2	--	--	--	--	--
3TK2825-..... Basic unit, auto start	4	3	--	--	--	2	--
3TK2823-.CB30 Basic unit, automatic start	4	2	--	--	--	--	--
3TK2830-..... Expansion unit	as for basic unit	4	--	--	--	--	--
3TK2834-..... Two-hand control unit	4	2NO + 2NC	--	--	--	--	--
3TK2835-..... Run-on test unit	--	3NO + 1NC	--	--	--	--	--
Delayed, safety outputs							
3TK2828-..... Basic unit, auto start with time delay 0.5 - 30s, 0.05 - 3s	4	2	2	--	--	1	--
3TK2827-..... Basic unit, monitored start with time delay 0.5 - 30s, 0.05 - 3s	4	2	2	--	--	1	--
Contactor relay enable circuits							
Instantaneous, safety outputs							
3TK2850-..... Basic unit	3	3	--	--	--	--	--
3TK2851-..... Basic unit	3	2	--	--	--	1	--
3TK2852-..... Basic unit	3	6	--	--	--	1	--
3TK2853-.BB40 Basic unit	3	3	--	--	--	--	--
3TK2856-.BB40 Expansion unit, instantaneous,	as for basic unit	6	--	1	--	1	--
Delayed, safety outputs							
3TK2857-.BB4. Expansion unit with time delay 3s - 300s	as for basic unit	--	3	1	--	--	--
Power contactor enable circuits							
Instantaneous, safety outputs							
3RA710 Basic unit up to Category 3	3	3	--	--	--	*	--
3RA711 Basic unit up to Category 4	4	3	--	--	--	*	--
3RA712 Expansion unit, instantaneous	as for basic unit	3	--	--	--	*	--
Delayed, safety outputs							
3RA713 Expansion unit with time delay 0.05 - 3 s	as for basic unit	--	3	--	--	*	--
3RA714 Expansion unit with time delay 0.5 - 30 s	as for basic unit	--	3	--	--	*	--
Average functionality (2 safety-relative sensors can be connected)							
Electronic and relay contact enable circuits							
Instantaneous, safety outputs							
3TK2845-.BB40 Multi-functional unit, instantaneous	4	2	--	2	--	--	1
Delayed, safety outputs							
3TK2845-.BB4. Multi-functional unit with time delay 0.05 - 300s	4	1	1	1	1	--	1

* possible using mounted auxiliary contacts

Additional technical details are provided in the Catalog as well as in the technical documentation in the Internet under:
http://www.siemens.de/automation/service

	Rated control supply voltage / V	Rated operating voltage / V	Switching capability				Electronic sensors	Enclosure width / mm
			AC-1	AC-3	AC-15	DC-13		
			at Ve=400V, 50Hz	at Ve=400V, 50Hz	at U=230 V	at U= 24 V		
	24 V	24 V	--	--	--	0.5 A	No	22,.
	24 V	24 V	--	--	--	1,5 A	Yes	22,5
	24 V	24 V	--	--	--	1,5 A	Yes	22,5
	AC/DC 24 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	22,5
	AC/DC 24 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	22.5
	AC/DC 24 V, DC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	22,5
	AC/DC 24 V, DC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	6 A	6 A	No	45
	AC/DC 24 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	22.5
	AC/DC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	6 A	6 A	No	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	No	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	No	90
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	No	90
	DC 24 V, AC 230 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	No	90
	DC 24 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	No	90
	DC 24 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	--	90
	DC 24 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	--	90
	AC 690 V	DC 24 V, AC 230 V			--	--	No	90
	AC 690 V	DC 24 V, AC 230 V			--	--	Yes	90
	AC 690 V	DC 24 V, AC 230 V			--	--	--	90
	AC 690 V	DC 24 V, AC 230 V			--	--	--	90
	AC 690 V	DC 24 V, AC 230 V			--	--	--	90
	24 V	24 V, 230 V	--	--	2 A	1,5 A	Yes	45
	24 V	24 V, 230 V	--	--	2 A	1.5 A	Yes	45

5.5 ASIsafe

Reference - link

Overview, features / customer benefits as well as function design and applications were explained in Chapter 4.2 (Safety-related communications using standard fieldbuses; Section ASIsafe). The product spectrum will be discussed in detail and a typical structure shown in the following.

Safety monitors

The safety monitor is the core element of ASIsafe. A safety-related application is configured using a PC. In this case, various application-specific operating modes can be selected. These include, e.g. Emergency Stop function, protective door tumbler mechanism as well as the selection of Stop Category 0 or 1. In order to be able to fully utilize ASI diagnostic possibilities, the monitor can be optionally operated with the AS interface address. There are two monitor versions:

- Basis safety monitor
- Enhanced safety monitor

Both expansion stages are available with enable circuits implemented with either one or two channels.

SIRIUS Emergency Stop

Emergency Stop command devices can be directly connected using the standard ASI-Interface with safety-related communications.
This applies to the SIRIUS 3SB3 Emergency Stop command device for front panel mounting and for mounting in an enclosure. An Emergency Stop command device mounted in a front panel can be directly connected to the AS-Interface via a safety module.

Emergency Stop in enclosures

Different enclosures with 3SB3 command devices with Emergency Stop can be directly connected to ASIsafe.
Customer-specific arrangements of the command and signaling devices inside the enclosure can also be ordered.

SIRIUS position switches

SIRIUS position switches can be directly connected using the standard AS-Interface with safety-related communications. There is a direct connection available for this purpose, that is mounted onto the position switch thread. This is the reason that the components for the safety-related functions no longer have to be conventionally connected-up.

SIGUARD light curtains and light grids

The light curtains and light grids, Category 4 acc. to EN 954-1 offer active optical protection for personnel at machines. They can be directly connected to AS-Interface in a safety-related fashion.

SIGUARD LS4 laser scanners

The laser scanner is an optical, electro-sensitive protective device to secure hazardous zones up to a radius of 4 m. The AS-Interface version allows a direct connection to be implemented in a safety-related fashion.

K45F safety module

The compact K45F safety module is equipped with 2 safety-related inputs for electro-mechanical transmitters and sensors.
In operation up to Category 2 according to EN 954-1, both inputs can be separately used. However, if Category 4 is required, the module has a 2-channel input.

K60F safety-related module

The compact K60F safety module is equipped with 2 safety-related inputs for electro-mechanical transmitters and sensors.
Both inputs can be separately used for operation up to Category 2 acc. to EN 954-1; if Category 4 is required the module has a 2-channel input. In addition, the module also has 2 non safety-related outputs. K60F is available in two versions:

- Power supply for the outputs via the yellow cable
- Auxiliary power supply for the outputs via the black cable ($V_{aux.}$)

S22.5F safety module

The SlimLine S22.5F safety module has 2 “safety” inputs for electro-mechanical transmitters and sensors. This allows safety-related signals to be connected to ASIsafe in distributed local electrical cabinets and boxes.
Both inputs can be separately used for operation up to Category 2. If Category 4 is required, the module also has a 2-channel input

All important standards and regulations are fulfilled, e.g.:

- IEC 61508 (up to SIL 3),
- EN 954 (up to Category 4)

Technical data

There are two safety monitor versions:

- Basis safety monitor
- Enhanced safety monitor

Both expansion stages are available with enable circuits utilizing either one or two channels.

Table: Comparison between the basis safety monitor - expanded safety monitor

	Basis safety monitor	Enhanced safety monitor
No. of monitoring blocks	32	48
No. of OR logic gates (inputs)	2	6
No. of AND logic gates (inputs)	-	6
Space retainer for monitoring blocks	Yes	Yes
De-activating monitoring blocks	Yes	Yes
Fault release	Yes	Yes
Hold diagnostics	Yes	Yes
A/B slaves for acknowledgment	Yes	Yes
Safety time function	No	Yes
Function “Key”	No	Yes
Contact de-bounce	No	Yes

	Safety Monitor
	3RK1 105
Rated operating current	
• I_e/AC-12	to 250 V, 3 A
• I_e/AC-15	115 V, 3 A
	230 V, 3 A
• I_e/DC-12	to 24 V, 3 A
• I_e/DC-13	24 V, 1 A
	115 V, 0.1 A
	230 V, 0.05 A
• Response time (worst case) in ms	≤40
• Ambient temperature in degrees in °C	0 ... +60
• Storage temperature in °C	-40 ... +85

Example - packaging machine

A typical ASIsafe application is shown in the following diagram:

Description of the sequence:

Empty boxes are transported along conveyor belt 1 for filling. The products to be placed in the boxes are moved to the robot using conveyor belt 3.
This fills the empty boxes. The filled boxes are then transported away on conveyor belt 2.

Protective devices and equipment:

The robot has a protective fence around it to protect personnel against injury.
The light grid ensures that the application is shut down within the protective fence.
The cable-operated switch allows conveyor belt 1 to be shut down.
The Emergency Stop powers-down the complete plant or system in a safety-related fashion.
A door is provided in the safety fence for maintenance purposes. This door is monitored using a protective door tumbler mechanism. When the robot system is entered through the door, the application inside the protective fence is shut down.

Implementation with ASIsafe:

The circuit for an AS-Interface solution is shown in the adjacent diagram.
Safety monitor 1 switches the power for motor 1.
Safety monitor 2 switches the power for motors 2 and 3.

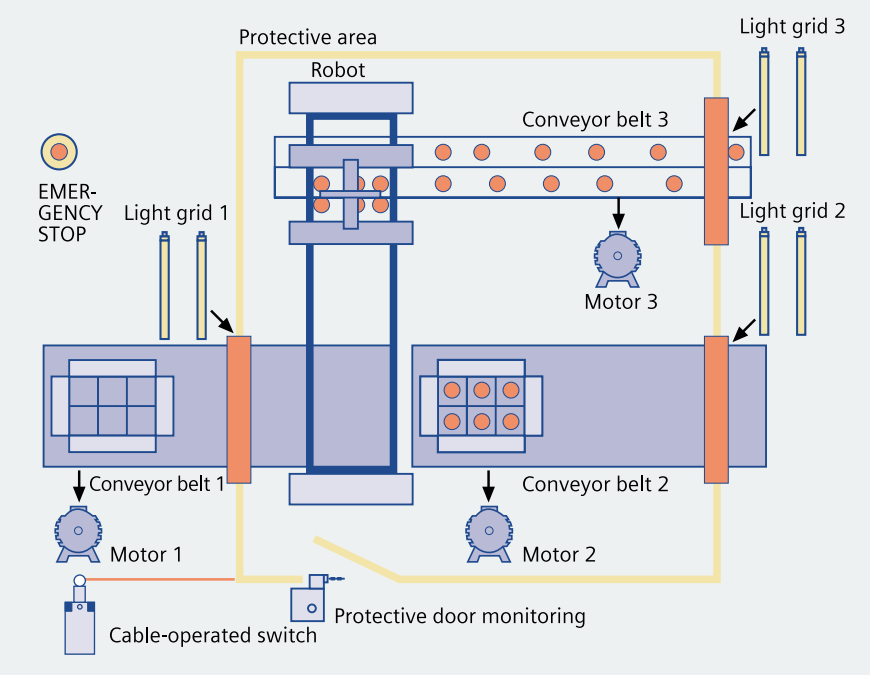


Fig. 5/2
Combination of safety slaves using as an example a packaging machine. This indicates the specific, safety-related shutdown of sub-areas.

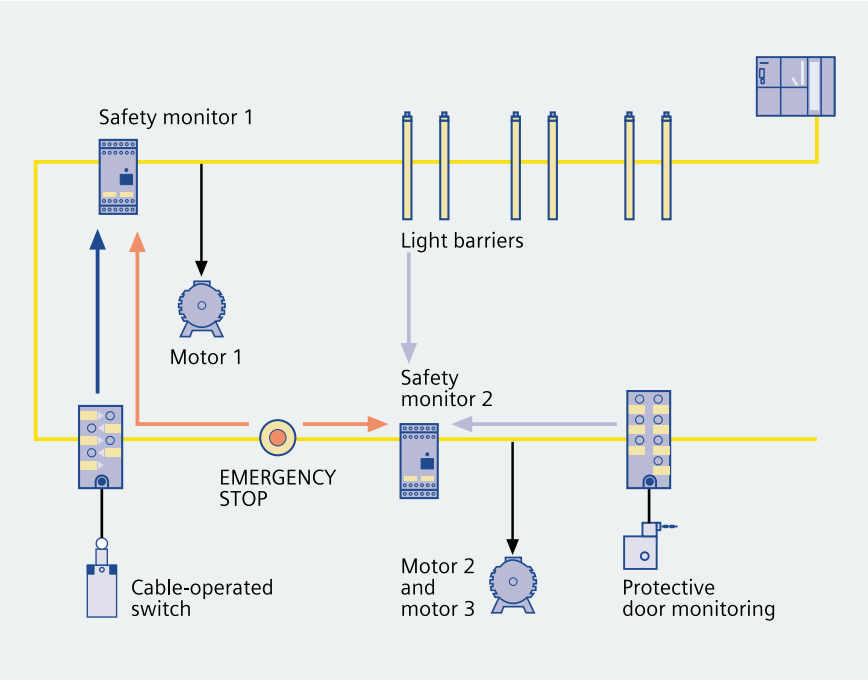


Fig. 5/3
Forming groups with ASIsafe

ASIsafe allows safety-related signals to be appropriately grouped.
This means that the safety slaves can be assigned to the safety monitors.
The protective door monitoring and the light barriers are assigned to safety monitor 2 (bright blue arrow).
The cable-operated command device is assigned safety monitor 1 (blue arrow). The Emergency Stop command device is assigned both safety monitors (red arrow).

This means that the cable-operated switch shuts down safety monitor 1 via a safety module.
The light barriers and the protective door shut down the application within the protective fence via safety monitor 2.

The complete system can be shut down via the Emergency Stop command device - that is assigned to both safety monitors.

5.6 ET 200S Safety Motor Starter Solution

Overview

The ET 200S Safety Motor Starter Solutions comprise the following:

- Safety modules
- ET 200S Motor Starters, Standard
- ET 200S Motor Starters, High Feature
- ET 200S Failsafe Motor Starters

The devices have been designed for use in the distributed ET 200S I/O system. The motor starters are equipped with electrically isolating contacts.

These Safety Motor Starter Solutions can protect and switch any three-phase load without any fuses being required. All of the inputs and outputs necessary to connect the motor starter and safety system to the higher-level control are already integrated. They are also optimally suited for use in distributed electrical cabinets (degree of protection IP20) as a result of the communications interface and the extensive diagnostic functionality.

With ET 200S Safety Motor Starter Solutions, the complex and therefore cost-intensive engineering and wiring costs when compared to conventional safety systems are eliminated. ET 200S Safety Motor Starter Solutions are designed for Category 4 acc. to EN 954-1 and SIL 3 (IEC 61508).

Applications

ET 200S Motor Starter Solutions are preferably used in all sectors of production and process automation where the reduction of production times or the increase of plant availability plays a significant role.

1. ET 200S Motor Starter Solutions Local, from the perspective of the safety system, should be limited to one station.

2. On the other hand, ET 200S Motor Starter Solutions PROFIsafe are frequently used in more complex safety system applications that are networked with one another.

Technical requirements

- PROFIBUS or PROFINET
  If the ET 200S Safety Motor Starter Solution PROFIsafe is required, then in addition, a safety-related SIMATIC control and PROFIBUS or PROFINET with the PROFIsafe profile as communications medium are required.

Customer requirements

- Safety direct or reversing starters up to 7.5 kW / at 500 V acc. to DIN VDE 0106, Part 1014 – IEC 60947-1, EN 60947-1 and for 600 V acc. to UL, CSA must be able to be simply integrated into standard automation environments.
- Seamless, integrated total system and complete safety technology from a single source.
- Simplified engineering thanks to seamless and integrated tools.

- Safety-related components must be able to be simply connected - e.g. Emergency Stop command devices, protective door monitoring devices or light curtains via safety modules.
- For complex requirements placed on the safety system, a favorably-priced solution in comparison to conventional systems with load feeders and discrete safety technology.
- Reduced costs for testing and documentation.
- Fast configuration and commissioning
- A system can be easily expanded with lower engineering and wiring costs.
- High degree of availability thanks to extensive diagnostics (fast trouble-shooting) and service-friendliness (plug-in modules / hot swapping) * .

Features

Our ET 200S Safety Motor Starter Solutions allow safety-related direct or reversing starters to be used in the distributed SIMATIC ET 200S I/O system. Applications involving machines and plants can be optimally emulated thanks to the finely modular system architecture.

The motor starters are suitable for switching and protecting three-phase loads.
Motor Starters, Standard: Max. 5.5 kW (AC 500 V) with self-establishing power bus up to 40 A

Motor Starters, High Feature: Max. 7.5 kW (500 V AC) with self-establishing power bus up to 50 A
Failsafe Motor Starters: Max. 7.5 kW (500 V AC) with self-establishing power bus up to 50 A
All of the motor starters can be optionally expanded using modules to control brakes integrated in the motor.

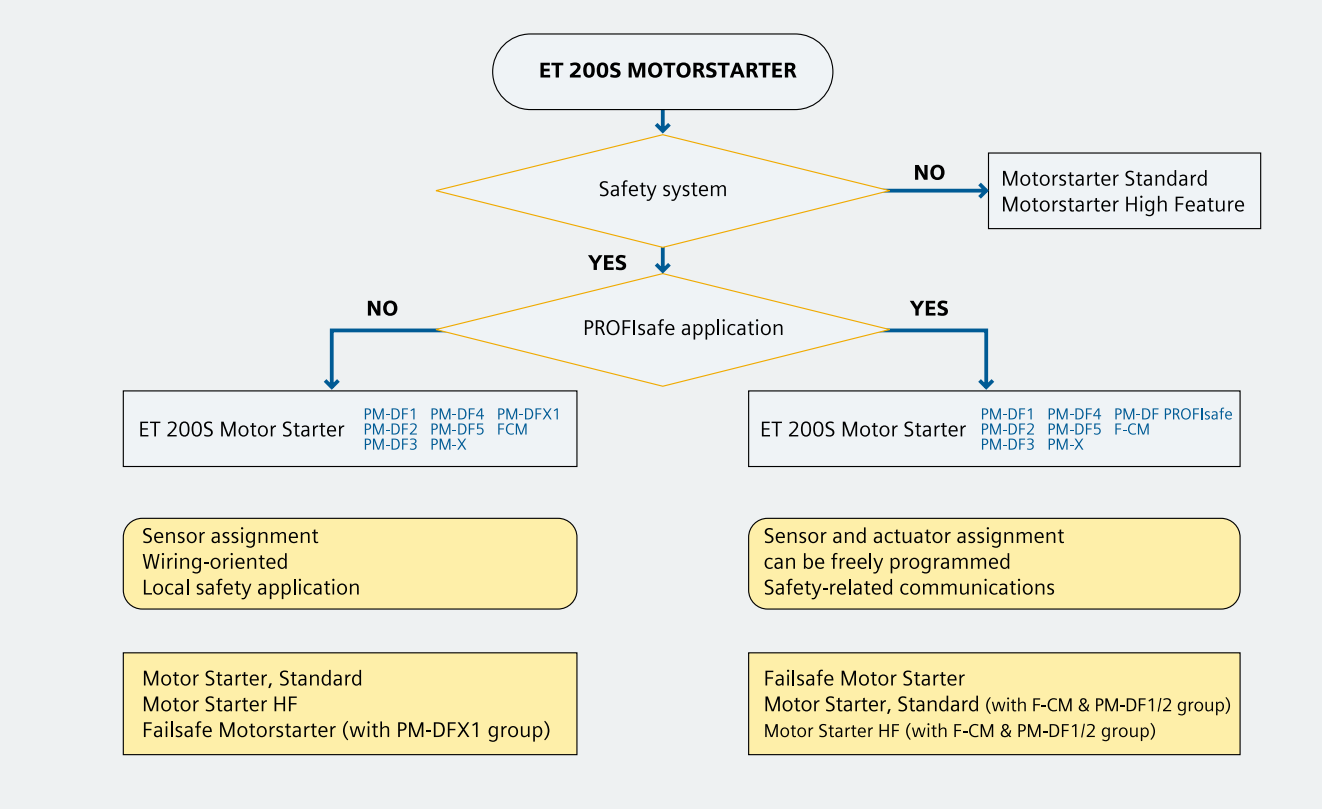


Fig. 5/4
ET 200S Motor Starter

* Hot swapping: Devices are replaced in operation without having any effect on the operational CPU or motor starter.

ET 200S Safety Motor Starter Solutions can also be combined, within an ET 200S station - with SIMATIC ET 200S FC frequency converters (refer to Chapter 9.3). Also in this case, safety-related components can be combined with non safety-related components.

The complete SIMATIC ET 200S system is UL/CSA certified.
TÜV (German Technical Inspectorate) has certified our ET 200S Failsafe Motor Starters.

ET 200S Safety Motor Starter Solutions Local
Wiring-oriented sensor assignment: The logic of the safety-related functions is implemented using the wiring

Several safety circuits can be easily configured using ET 200S Safety Motor Starter Solutions Local. The safety sensor systems are directly connected to the safety modules. These safety modules handle the task of the otherwise obligatory safety relays and depending on the selected function safely shut down the downstream motor starters. The cross connections that are required are already integrated in the system and no additional wiring is required. It goes without saying that ET 200S Motor Starters can also be used in conjunction with external safety relays or with ASIsafe.

When compared to conventional safety systems, the ET 200S Safety Motor Starter Solution Local saves a considerable about of wiring when it comes to local safety applications.

There are three versions:

Local safety applications - ET 200S Motor Starters, Standard: Group shutdown

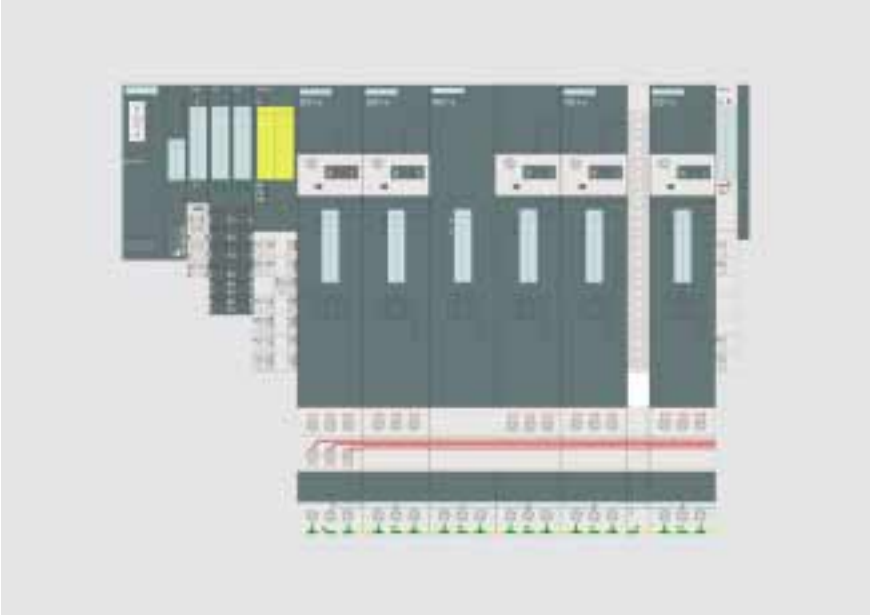


Fig. 5/5
ET 200S Safety Motor Starter Solution Local (with Motor Starters, Standard) F-Kits 1 or 2 are required. From Category 3 EN 954-1: Redundantly switching, external supply contactor is required

Fig. 5/6
Distributed electrical enclosure with ET 200S Safety Motor Starter Solution Local

- Several monitored motor starters up to 5.5 kW can be quickly and simultaneously combined in a distributed I/O system to form one or several safety-related groups. This is the reason that even more complex safety-relevant applications can be handled using the ET 200S Safety Motor Starter Solutions Local (up to 42 standard motor starters can be combined in just one station).

ET 200S Safety Motor Starter Solution is optimized for applications up to Category 4 acc. to EN 954-1.
This means that the system identifies defects and after a safety-related shutdown, prevents a restart. The PM-DF1 / PM-DF2 / PM-DF3 / PM-X safety modules handle these tasks.

Various functions are possible:

- Emergency Stop Shutdown (PM-D F1 safety module / monitored start) protective door monitoring (PM-D F2 safety module / automatic start) safety-related circuits can be expanded using other motor starters, e.g. in another tier (PM-D F4) time-delayed shutdown (STOP 1 using PM-D F3) safety contact multiplication (PM-D F5)
- Can be used in conjunction with external safety circuits.
  Can be integrated into existing safety concepts.
- Simple diagnostics capability:
  Faults in the plant/system are automatically signaled via bus without any programming required.
- Self-establishing 40 A power bus
- Recommended for applications where few changes will be required or flexibility when assigning safety-related segments.

Local safety-related applications with ET 200S Motor Starters, High Feature: Group shutdown

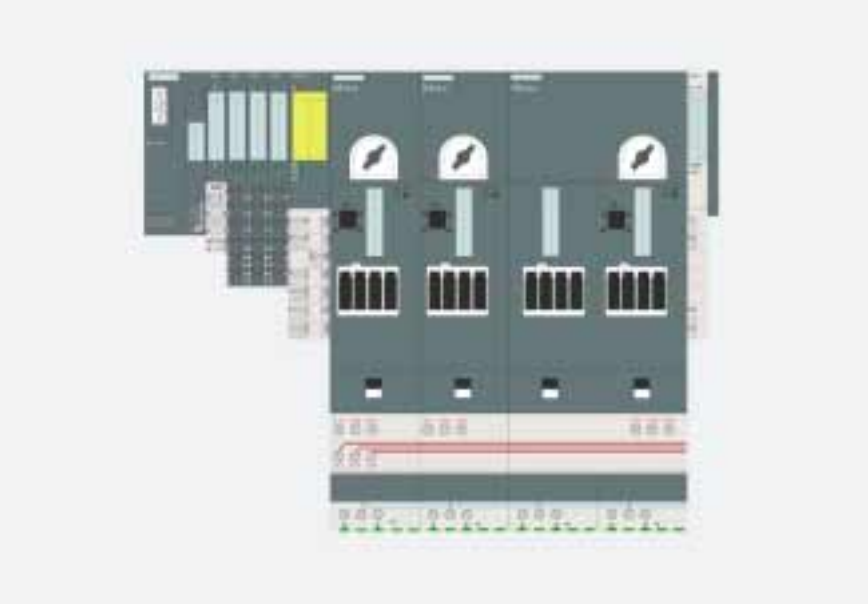


Fig. 5/7
ET 200S Safety Motor Starter Solution Local (with Motor Starters, High Feature)
HF motor starters and their terminal modules have the function of the F-Kits already integrated as standard. From Category 3 EN 954-1 onwards: A redundantly switching external supply contactor is required.

Standard Motor Starters and High Feature Motor Starters can also be combined with one another as required - e.g. to form a single shutdown group.

When compared to the Standard Motor Starter the High Feature Motor Starter has additional advantages:

- Motor starters up to 7.5 kW with only two versions (wide setting range)
- Coordination type 2
- if the High Feature Motor Starter is used, then the selective protective concept can differentiate between an overload and short-circuit. This means that an overload trip can be remotely acknowledged via the bus.
- Parameterization via PROFIBUS.
- When replacing (this is permissible under voltage!) all parameter data is automatically downloaded from the higher-level PLC.
- Up to 29 High Feature Motor Starters can be installed in a station (max. 2 m wide).
- Self-establishing 50 A power bus
- The motor starters have extensive diagnostics, e.g. current limit value
- Statistical data, e.g. current of the last overload trip or the number of switching cycles can be read-out using the software Switch ES Motor Starter for service and commissioning purposes.

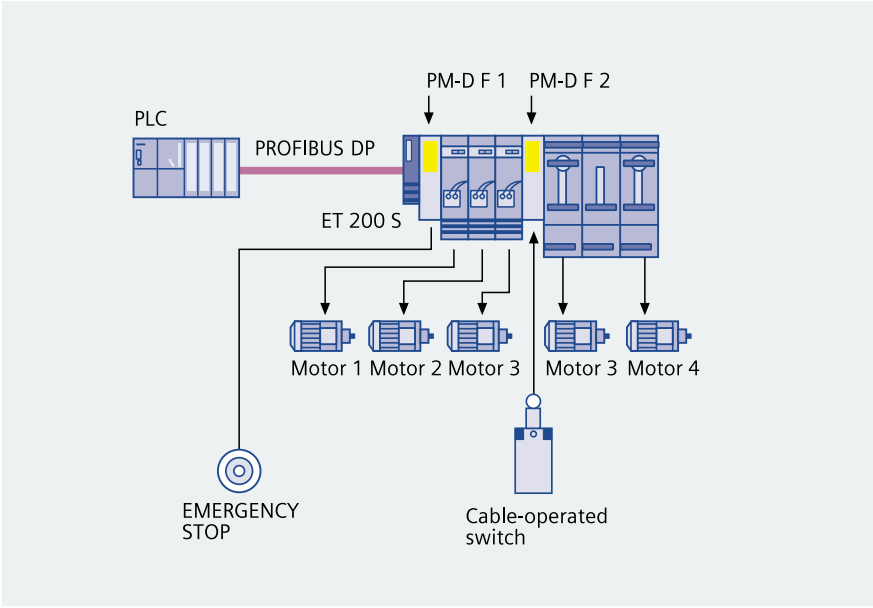


Fig. 5/8
ET 200S Safety Motor Starter Solution Local with Failsafe Motor Starters (PM-D F1, PM-D F2 application)

Local safety applications with Failsafe Motor Starters: Selective shutdown.

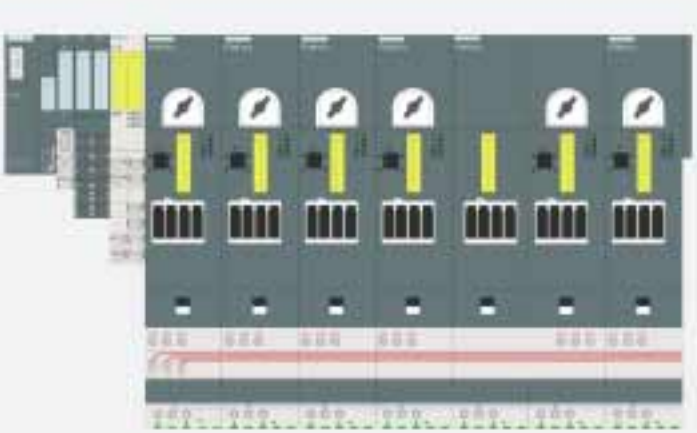


Fig. 5/9
ET 200S Safety Motor Starter Solution Local (with Failsafe Motor Starter and PM-D FX1) An external supply contactor is not required as redundant second shutdown element, as the motor circuit-breaker is used.

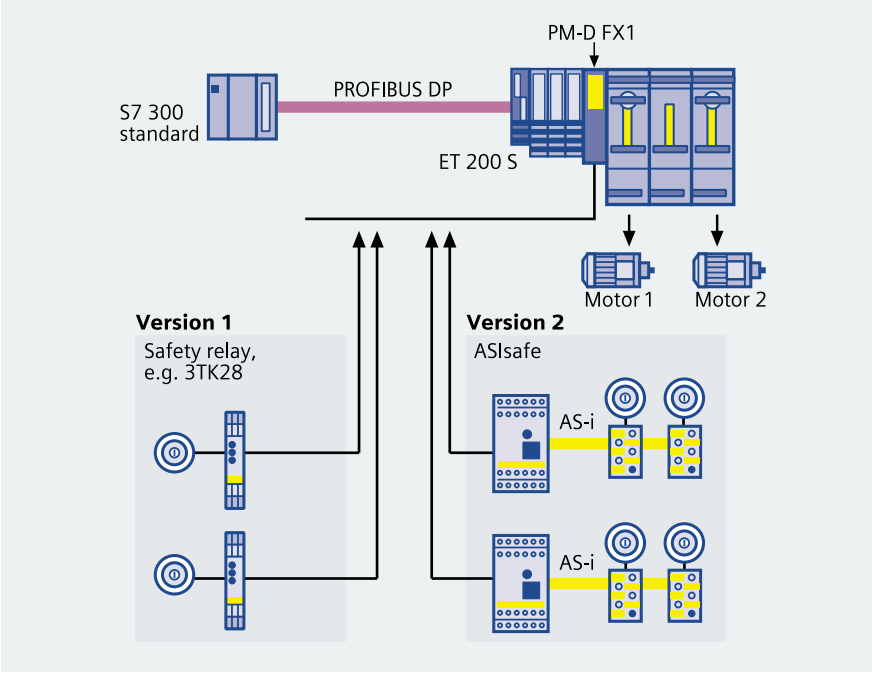


Fig. 5/10
ET 200S Safety Motor Starter Solution Local with Motor Starters, Standard and High Feature

As part of the ET 200S Safety Motor Starter Solutions Local (without F-CPU and without PROFIsafe Communication) a combination with Failsafe Motor Starters offers the following additional customer benefits:

- the Failsafe Motorstarter can be used in conjunction with either safety relays or with ASIsafe. By enabling an ASIsafe safety monitor or a safety relay, safety-related signals can be fed into the ET 200S station via the PM-D FX1 supply module and therefore can be used to control the Failsafe Motor Starters; these then safely shut down motors.

- The external safety relays can be supplied from the safety- relevant voltage U1 from PM-D FX1.

- Fully-selective safety shutdown: A PM-D FX1 safety module can handle a total of 6 safety shutdown groups by accessing the 6 buses SG1 to SG6 (safety groups). It transfers the safety-related control voltage of the shut - down groups SG1 to 6 onto the voltage buses of the terminal modules up to the sub-sequent Failsafe Motor Starters. Terminal modules of the Failsafe Motor Starter have an additional coding block that allows the motor starter to be assigned to one of six shut-down groups. The shutdown is realized by an external ASIsafe safety monitor or a safety relay switching one of the 6 SGx buses into a no-voltage condition.

- The Failsafe Motor Starter is shut down in a safety-related fashion using its contactor. As a result of the integrated evaluation electronics used for fault detection, when the contactor fails, the circuit-breaker is additionally tripped. A specific diagnostics signal automatically signals such a fault to the higher-level control. The redundant shutdown is only carried-out when a fault occurs in a Failsafe Motor Starter.

- Significantly less hardware is required: Contactors, auxiliary switches, supplementary modules are no longer required. This results in significantly less wiring.

- Up to 29 Failsafe Motor Starters can be installed in a station (2 m max.).

- Failsafe Motor Starters up to 7.5 kW with more diagnostics: Single-switch identification, cross-fault detection, contactor failure. Status display for each safety-related shutdown group

- The PM-D FX1 safety module represents a transfer node. The safety-related potential (voltage) group can be coupled to one or several ET 200S stations.

- The ET 200S Safety Motor Starter Solutions Local with PM-D FX1 can be expanded using the F-CM safety module. The F-CM safety module provides 4 safety, electrically isolated relay contacts which can be used to safely shut down additional actuators or devices.

- An important benefit of the F-CM contact multiplier is the safety-related control of a separate, large contactor if motors exceed the maximum power of the ET 200S Motor Starter (> 7.5 kW). The F-CM is controlled using a PM-D FX1 safety module.

ET 200S Safety Motor Starter Solutions PROFIsafe
As part of the distributed safety concept, the assignment of sensors and actuators can be programmed: This means that every safety function can be implemented.

If a safety-related SIMATIC CPU is used, then the ET 200S can be used as safety-related I/O. However, conventional technology can be mixed with modules with safety-related functions in such a station with motor starter and input/output modules.

The safety-related functions are available in the complete network. This means that the ET 200S Safety Motor Starter Solutions PROFIsafe permits the selective shutdown of a group of Standard, High Feature or Failsafe Motor Starters. It does not matter to which I/O station the safety-related command devices are connected. This is why this solution offers a degree of flexibility that has been unknown up until now and far less wiring for applications with a large, extensive footprint or those that only sporadically have to be modified or changed when assigning the safety segments. ET 200S Motor Starter Solutions PROFIsafe is optimally suited for safety concepts with Cat. 2 to 4 acc. to EN 954-1, SIL 2 and 3 acc. to IEC 61508.

There are three versions:

Safety Applications with safety-related communications and Motor Starters, Standard: Group shutdown

The F-CM safety module (contact multiplier) is an important supplement to the fail-safe ET 200S I/O modules. For example, to provide an interface between an ET 200S station and plants or systems utilizing conventional safety systems - for instance, robots.

An F-CM safety module can be assigned to a safety shutdown group SG1 to SG6 of a PM-D F PROFIsafe safety module and comprises four separate, electrically isolated enable circuits as NO contact. At each ON – OFF cycle of the contact multiplier, the contacts of the F-CM are checked to ensure that they open and close correctly. If welded contacts are identified in any enable circuit of the F-CM, then the device is prevented from restarting as a result of the positively-driven contacts. In this case, an appropriate diagnostics signal is transferred to the higher-level control.

The F-CM safety module forms an interface between a PROFIsafe application and a wiring-oriented motor starter group.
This means that standard motors starters can be used and safely shut down via PROFIsafe.

- Favorably-priced implementation of a shutdown group
- A redundant switching, external supply contactor is used via the PM-X safety module (only required for Cat. 3 or 4 EN 954-1)
- The feedback circuit is monitored via PM-D F2
- Motor protection up to 5.5 kW using a circuit-breaker
- Behavior for CPU STOP can be set
- Group diagnostics

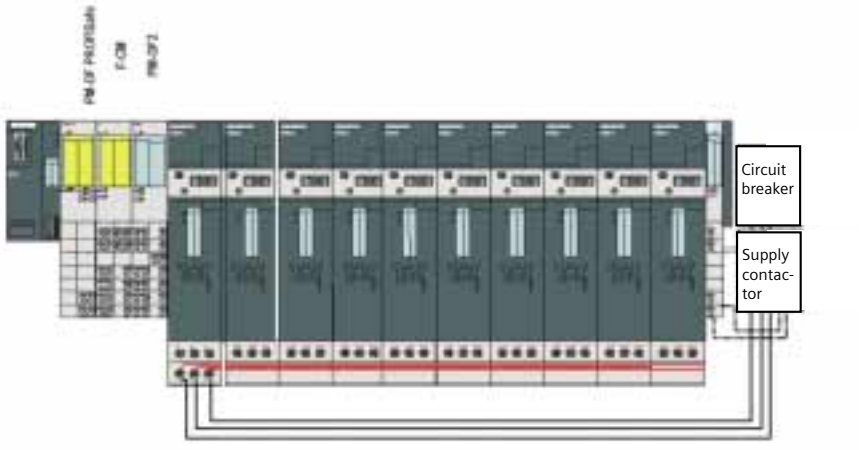


Fig. 5/11
ET 200S Safety Motor Starter Solution PROFIsafe (with Motor Starters, Standard) Additional F-Kits 1 or 2 required. From Category 3 EN 954-1: Redundant switching, external supply contactor is required

Safety applications with safety-related communications and Motor Starters, High Feature: Group shutdown

When compared to Standard Motor Starters, High Feature Motor Starters have the following advantages:

- The feedback circuit is already integrated (an F-Kit is not required)
- Electronic motor protection up to 7.5 kW
  Behavior under overload conditions thermal motor model
  Behavior when the current limit value is violated
  Behavior when detecting a zero current
  Behavior when imbalance occurs
  Behavior for a CPU STOP
- Remote reset after overload trip is possible
- Group diagnostics
- Extended individual diagnostics

Fig. 5/12
ET 200S Safety Motor Starter Solution PROFISAFE (with Motor Starters, High Feature)
F-Kits 1 and 2 are not required: High Feature Motor Starters and their terminal modules have the function of the F-Kits integrated as standard. From Category 3 EN 954-1 onwards: A redundant switching external supply contactor is required

Safety applications with safety-related communication and with Failsafe Motor Starters: Completely selective shutdown

The motor starters are assigned to one of six safety-related segments within an ET 200S station.
For plants and systems with a distributed architecture, the shutdown signals of these safety segments are preferably from a higher-level safety-related control via PROFIsafe. This signifies the highest possible degree of flexibility when assigning motor starters to different safety circuits. As an alternative, an ET 200S interface module with safety-related CPU can be controlled. This is especially recommended for local, limited applications and more basic safety interlocks. It is also possible to control external safety systems such as e.g. the AS-Interface.
If a station is expanded by additional shutdown groups, then the PROFIsafe structure with the failsafe motor starters is more favorably priced than a PM-D F1/2-based solution.

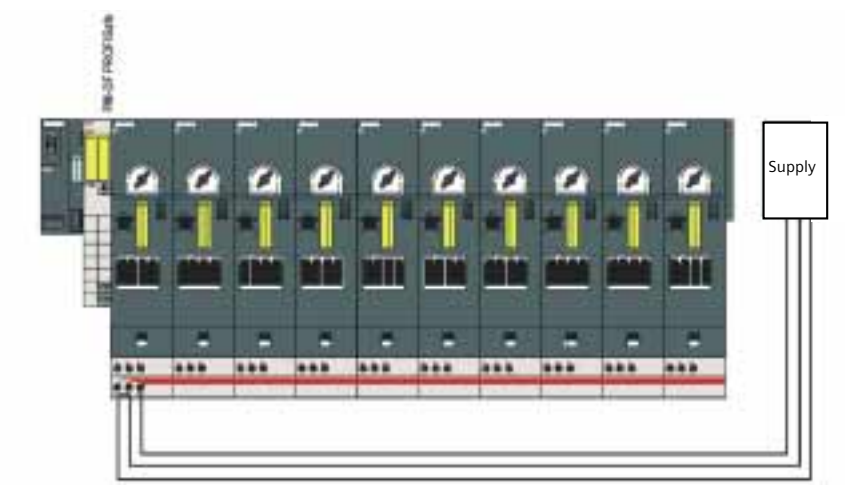


Fig. 5/13
ET 200S Safety Motor Starter Solution PROFISAFE (with Motor Starters, High Feature)
F-Kits 1 and 2 are not required: The redundant, second shutdown element is no longer a main contactor, but a circuit-breaker with auxiliary release integrated into the motor starters.

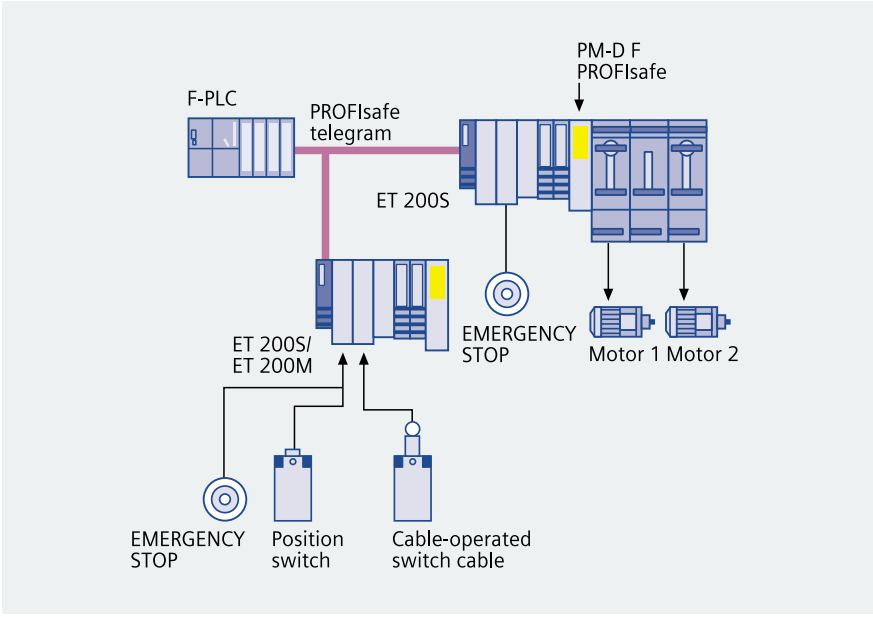


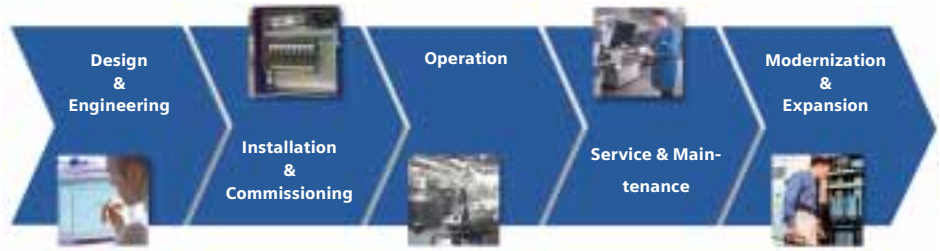
Fig. 5/14
ET 200S Safety Motor Starter Solution PROFIsafe with motor starters Failsafe (PM-D F PROFIsafe application)

The highlights include: Absolute fail safety

In addition to a circuit-breaker - contactor combination, the new fail-safe motor starters have a safety-related electronic evaluation circuit for fault detection. If the contactor to be switched fails in an Emergency Stop situation, then the integrated double processor monitoring detects a fault, e.g. if the contactor contacts are welded and then opens the circuit-breaker in the motor starter in a safety-related fashion. This means that every individual motor starter - without any additional supply contactors (redundant contactor) and feedback - circuit can reach Category 4 acc. to EN 954-1 or SIL 3 acc. to IEC 61508.

For safety relevant applications, the ET 200S Safety Motor Starter Solution offers many advantages for plant and machinery construction companies as well as for those companies operating the plants. The reason for this is that they can be optimally integrated but at the same time retaining a high degree of flexibility - and that in each phase of the plant lifecycle:

"Life cycle of industrial equipment"



Requirements that are fulfilled	Plant builders and machine OEMs	Plant operating companies	Feature
Phase 1: DESIGN and ENGINEERING			
Lower costs for engineering and documentation	✓		• Motor starters are-parameterized and documented using the standard STEP7 tool • All motor starter control functions can be configured/engineered using the PLC • Pre-configured programming examples for the safety-related functions • Fewer components: e.g. only 2 versions of Motor Starters, High Feature or Failsafe up to 7.5 kW with wide setting ranges
Faster reproduc-ibility	✓		Software solution can, contrary to a hardware solution, be simply multiplied
Higher degree of flexibility	✓	✓	• Fully-selective safety shutdown. • The logic of the safety function is implemented in the software – not in the wiring
Phase 2: INSTALLATION and COMMISSIONING			
Significantly faster mounting and installa-tion	✓		• Optimum cabinet design and layout by horizontally mounting motor starters "side-by-side" without de-rating up to 60° C • Up to 90% less control/safety wiring thanks to the safety system already integrated in the ET 200S and the data coupling with S7-300F via PROFIsafe • Thanks to the fast installation system of the ET 200S with self-establishing power bus, cable ducts are eliminated, terminals are replaced • All supply voltages are only connected once and are then automatically connected to the next modules. • All motor starters are completely connected-up only the motor has to be connected.
Lower space require-ment (fewer/smaller electrical cabinets)	✓	✓	• More compact solution • Separate components that were previously used are eliminated) due to the integrated redundancy and the integrated safety monitoring
Significantly faster commissioning	✓		• Simple testing thanks to standardization and a modular plant concept • Significantly fewer wiring errors are possible • Interface for ES Motor Starter Software Switch
More favorably priced and simpler acceptance pro-cedure (Machinery Directive)	✓	✓	Motor starters, safety modules and programming examples (F library) have been certified by the TÜV (German Technical Inspectorate)
Lower purchasing costs	✓		Often, the plug-on motor starters are only required weeks later. This reduces the amount of capital that is tied-up.

Requirements that are fulfilled	Plant builders and machine OEMs	Plant operating companies	Feature
Phase 3: OPERATION			
Increased availability and productivity		✓	• Faults are detected earlier thanks to the improved diagnostic functions • If motor starters are to remain available in plant or machine sections when the bus is interrupted, then the appropriate station can be engineered with local intelligence (IM151 CPU). • Overload of motor starters can be simply acknowledged using a remote reset via PROFIBUS • When an overload occurs or the current limit is violated, the motor starter can be parameterized for alarm and shutdown. • Emergency Start function • Coordination type "2" for 50 kA
Phase 4: SERVICE & MAINTENANCE			
Extensive motor diagnostics		✓	• Overload and short-circuit are separately detected using the diagnostics block in STEP 7 • The clear diagnostics (identifying the faulted component) must neither be programmed-in (F-PLC) nor connected-up (electro-mechanical solution)
Shorter downtimes		✓	• Hot swapping (motor starters are replaced in just a few seconds without requiring any tools) "pre-configured wiring" and self-coding motor starters (an incorrect motor starter is mechanically prevented from being inserted). • Automatic remote parameterization using the PROFIBUS master when hot swapping. • Complete motor protection as a result of overload protection, short-circuit protection, imbalance and stall protection (motor starting classes 10, 10A, 20) • Long motor starter lifetime with up to 10 million operating cycles
Lower spare part stocking costs		✓	Fewer components for the safety-related functions (instead of many electro-mechanical components proportional to the complexity of the F functions, there are only a few components independent of the complexity of the F functions) and only max. 2 versions of motor starters with wide setting ranges for the rated motor current.
Simple preventive service &maintenance that can be scheduled		✓	• Rated motor currents are monitored • Diagnostics for current limit value violation and statistics
Phase 5: MODERNIZATION AND EXPANSION			
Changes can be simply engineered	✓	✓	Software solution with standard STEP7 tool and parameterization instead of re-wiring
Simple to integrate in previous safety-concepts	✓	✓	Can be used in conjunction with external / conventional safety circuits.
Non communications-capable systems can be simply connected	✓	✓	Safety electrically-isolated relay outputs are available with the FCM safety module.

Applications

ET 200S Safety Motor Starter Solutions Local is used in all plants and systems where:

- Three-phase loads up to 7.5 kW are to be protected and operated.
- A peripheral (I/O system) in conjunction with a non safety-related PLC with degree of protection IP20 with PROFIBUS DP or PROFInet interface is practical.
- Local safety-related systems are required in plants and parts of plants with a limited footprint for safety-relatedload shutdown.
- No F-CPU is to be used.

ET 200S Safety Motor Starter Solution PROFIsafe is used in all plants, in which:

- Three-phase loads up to 7.5 kW are to be protected and operated.
- A peripheral (I/O) system in conjunction with safety-related PLC with PROFIBUS DP interface is practical.
- Safety-related communications. capable load shutdown is required.
- Optimum for use in plants and systems with an extensive footprint

This solution is predestined for the distributed safety concept.

Configuration example

comprising a control with peripherals (I/O), operator panel, laser scanner and light curtain.

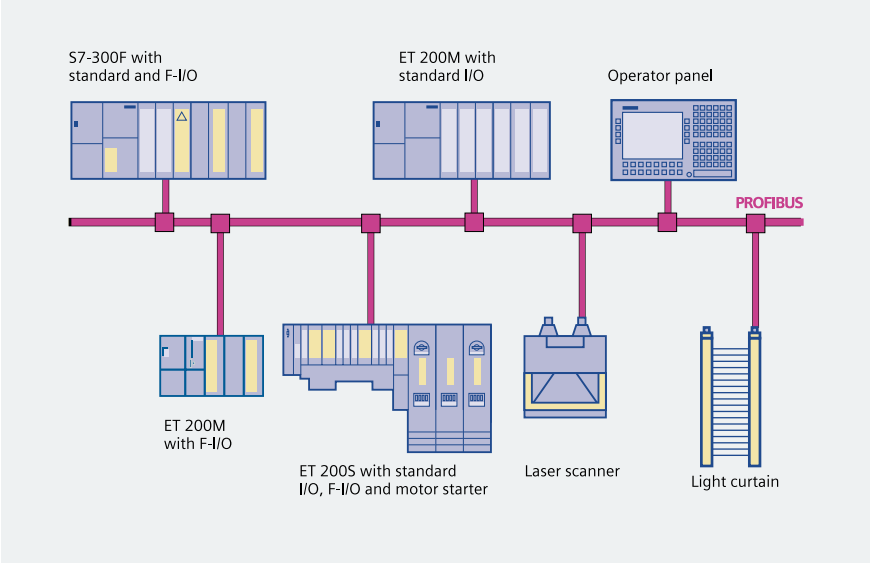


Fig. 5/15

ET 200S Safety Motor Starter (either with or without PROFIsafe) Solutions are mainly used in the production industry, but also in the process industry.

Here is an example for a machine tool in the production industry:

- SINUMERIK/SIMODRIVE as PROFIsafe master
- 1 ET 200S reversing starter for the revolver head
- 1 direct starter for the tool lubricating pump
- Emergency Stop and hazardous zone monitoring

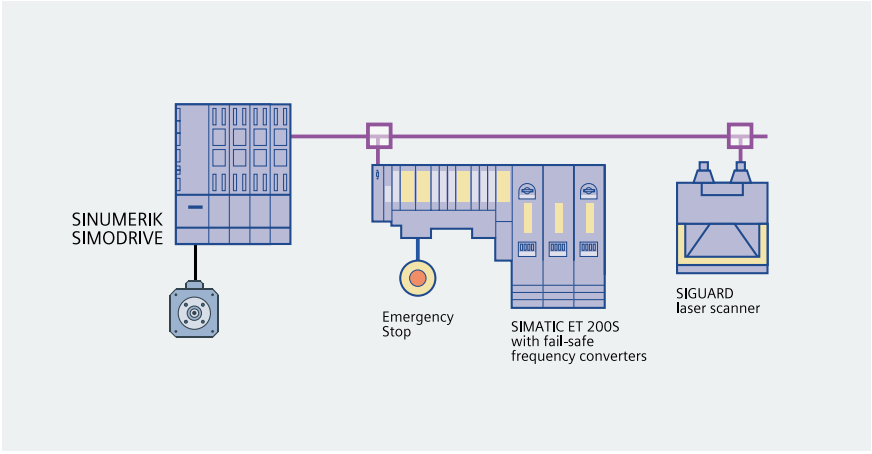


Fig. 5/16
Application example in the production industry

The following modules are available:

PM-D F PROFIsafe

Safety-related PROFIsafe power module with 6 integrated, safety-related shutdown buses (SIL 3), 24 V and 2 A to safely shut down downstream failsafe motor starters or contact multipliers when internally controlled via PROFIsafe.

PM-D F X1

Safety-related power module (feeder terminal module) with 6 integrated safety shutdown buses (SIL 3), 24 V and 2 A to safely shut down downstream failsafe motor starters or contact multipliers, when shutting down via external safety relays with electrically isolated contacts (e.g. 3TK28, ASIsafe safety monitor, relay outputs of safety-related PLCs etc.).

F-CM

Safety-related contact multiplier with 4 (SIL 3) outputs for 24 V and 2 A

Motorstarter Failsafe

Safety-related direct and reversing starter with a switching capability up to 7.5 kW, with redundant electrical isolation

An ET 200S configurator allows the distributed ET 200S I/O system to be quickly, simply and correctly configured.

Advantages:

- Parts lists and ordering data are automatically generated.
- Fast preliminary calculation.
- Transparent, graphic representation.
- Automatic configuration and structure test.

The ET 200S configurator is available free-of-charge on the Catalog CD-ROM CA01 and also through the Internet.

Structure

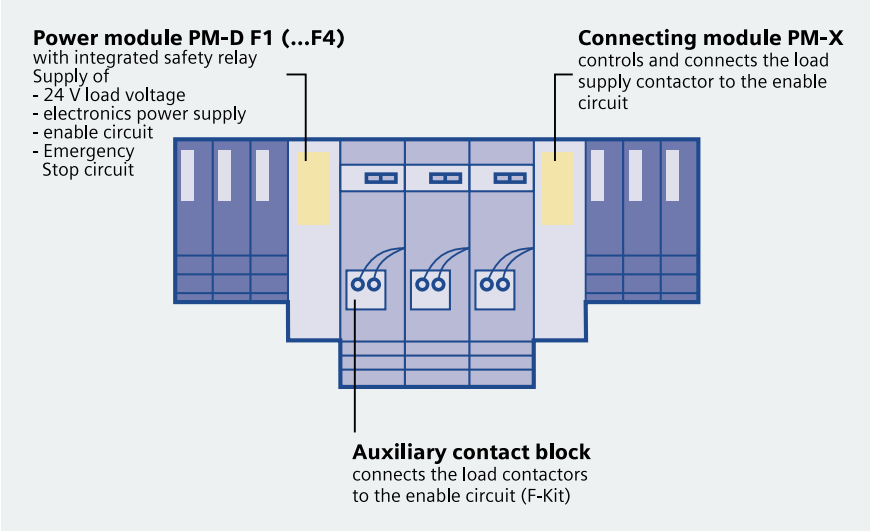


Fig. 5/17
Structure of an ET 200S Safety Motor Starter Solution Local with Standard Motor Starters and mounted F-Kits station

Examples

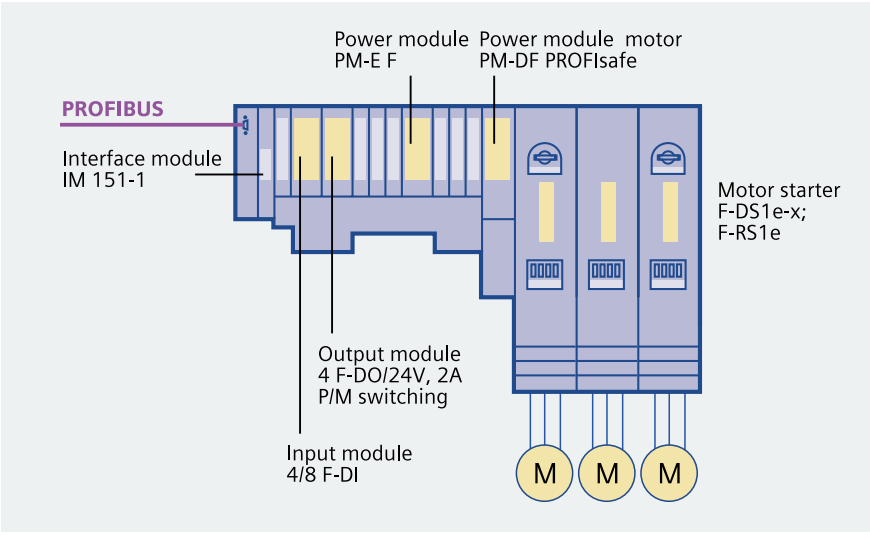


Fig. 5/18
Configuration of an ET 200S Safety Motor Starter Solution PROFIsafe with Failsafe Motor Starters

Fig. 5/19
Distributed electrical cabinet with ET 200S Failsafe Motor Starters

Technical data

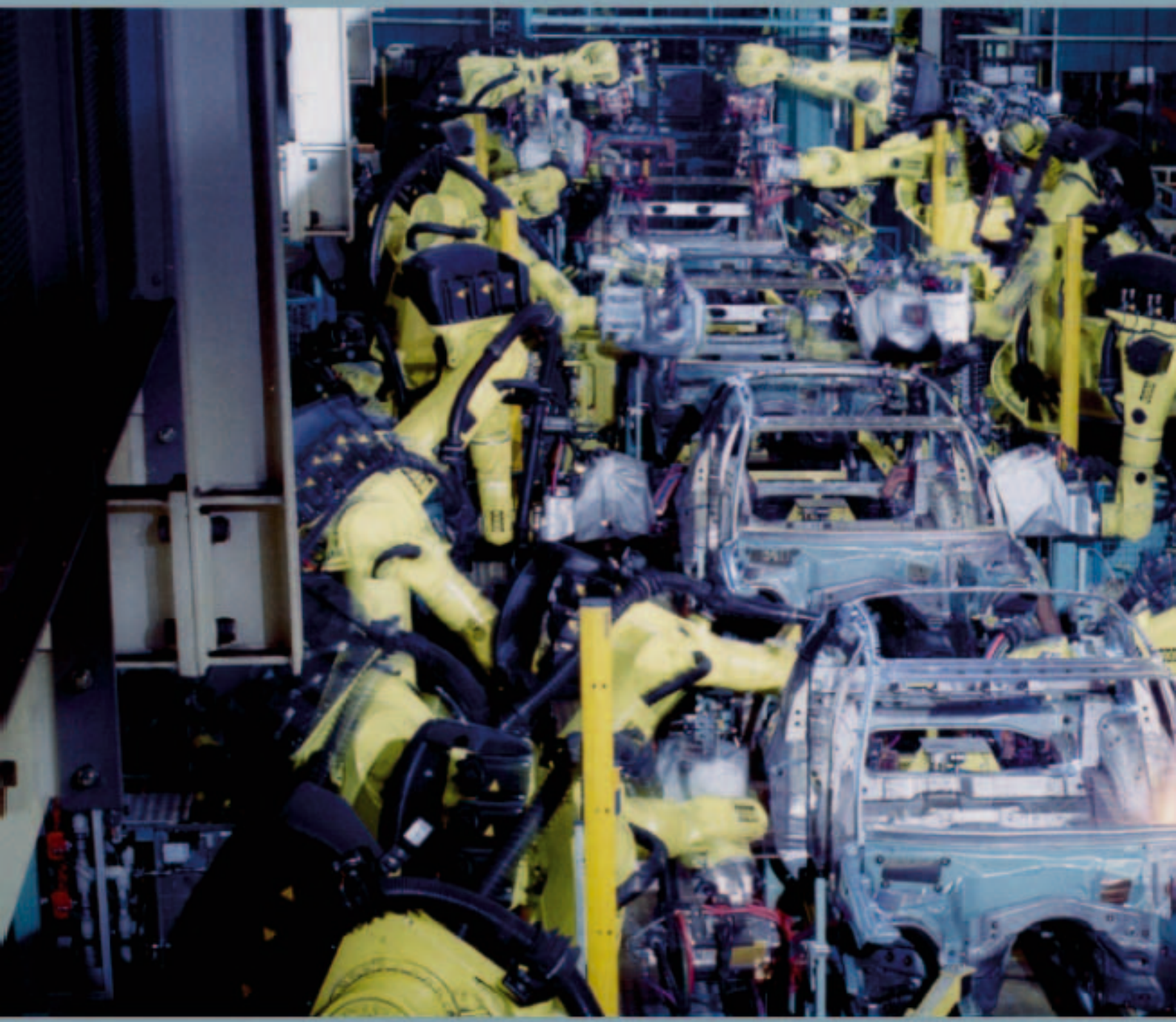
	ET 200S Standard Motor Starter	ET 200S High Feature / Failsafe
Current setting Ie	Manually, local at the m.c.b.	Wide range 0.3–3 A, 2.4–8 A, 2.4-16 A in 10 mA steps
Behavior when a current limit is violated	Shutdown	**Shutdown** with/**without** restart Alarm
Shutdown	CLASS 10	**CLASS** 10/20 (10A/10 for DSS1e-x)
No-load time	-	1-255 s/**de-activated** The overload model can be cleared
Zero current detection	-	Behavior/response, alarm/**shutdown**
Dissymmetry	Via thermal release	Alarm/**shutdown**
Lower, upper current limit value	-	18.75% to 100% Ie 50% to 150% Ie
Motor current measured value	-	Can be transferred via bus

Response times

With high internal data transfer rates and the 12 Mbaud connection of the ET 200S interface module connected to PROFIBUS DP, ET 200S Safety Motor Starter Solutions can be used in applications that are extremely critical from a time perspective.

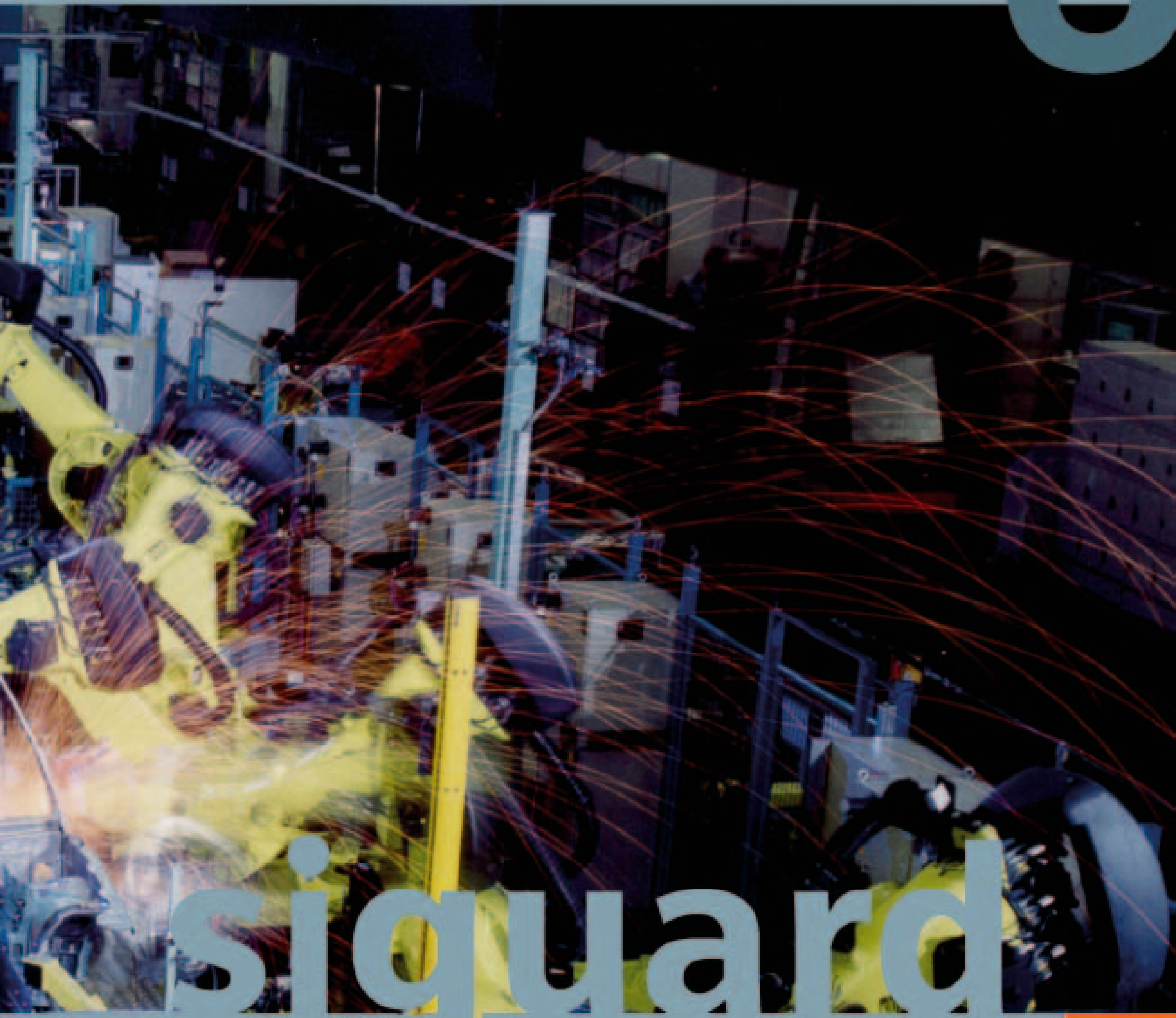
Further, ET 200S Motor Starters with expansion modules can be expanded in a modular fashion. For instance, the braking module - with or without independently effective fast stop inputs, reduces the response time of drives that must be especially quickly switched or braked. This means that assembly belts can be more precisely positioned, or a valve control can be very simply implemented.

• Minimum command duration PM-D F1, F2	200 ms
• Switch-in delay PM-D F3 to 5	< 150 ms
• Recovery time	
for PM-D F1, F2	< 1 s
for PM-D F3 to 5	< 50 ms
• Drop-out delay	
for PM-D F1, F2, F4	30 ms
for PM-D F3	0.5 to 30 s (can be continually set)
• Auxiliary circuit U2 PM-D F1, F2, F4 and F5	
Rated operating current	4 A
Continuous thermal current	5 A
• PM-D F PROFIsafe	
Summed current of the outputs	5 A (continuous current) / 10 A
Internal data processing time	3 ms < T < 9 ms
Rated operating current of an SGs	2 A
• Failsafe Motor Starter current drain from SG1...6	
Pulling-in	250 mA (for 200 ms)
Holding	max. 55 mA
• Failsafe Motor Starter current drain from U1 (electronics supply)	
Direct starter	40 mA
Reversing starter	100 mA



6

Fail-safe optical sensors



siguard

6 Fail-safe optical sensors

6.1 SIGUARD LS4 laser scanners

Overview

SIGUARD laser scanners are electro-sensitive protective systems to secure and protect hazardous zones at stationary machines and plants as well as at mobile systems.

The scanner is an optical distance sensor that transmits periodic light pulses within an operating field of 190°.
If these pulses strike an obstruction or a person, the light is reflected, is received by the laser scanner and evaluated. The scanner calculates the precise coordinates of the "detected" object from the light propagation time. A stop function is executed if the object or the person is located within a defined area. In this case, the semiconductor switching outputs are switched-off within the system response time. Depending on the mode and when the protective field is free, the stop function is either automatically reset or after acknowledgment.

Fig. 6/1
SIGUARD LS4 laser scanners

SIGUARD laser scanners can reliably detect persons up to a range of 4.0 m, even if these persons are wearing very dark clothing. By using this so-called safety-related protective field, the SIGUARD laser scanner is designed for personnel protection. Non-safety-related objects can be detected up to 15 m away. Four programmable protective field pairs allow the protective area to be optimally adapted to the application. A field pair is the combination of a pre-warning field (object protective field) and a protective field (personnel protective field). The scanner can be used on vehicles (driverless transport systems, shunting vehicles) and can be permanently mounted (to secure hazardous areas of machines). The contactless measuring principle means that SIGUARD laser scanners really are protective devices that can be universally used.

- Electro-sensitive, reliable protection of hazardous zones for universal applications: At machines, production robots, conveyor belts and systems, vehicles etc.
- Standard version with fail-safe semiconductor outputs
- User-friendly version with PROFIBUS-connection, PROFIsafe profile
- Automatic parameter transfer via PROFIBUS when the devices are replaced
- Category 3 acc. to EN 954-1
- Up to 4 personnel protective and warning field pairs can be freely set
- Protective field with a 4 meter maximum radius for personnel security
- Extremely compact design
- Low current drain

Protecting stationary hazardous areas

In modern production plants and systems, personnel must frequently enter potentially dangerous zones and areas. While personnel are in such dangerous areas, it must be absolutely guaranteed that the machine or plant does not represent any danger. However, the safety measures required should, as far as possible, not have a negative impact on production operations.

SIGUARD laser scanners allow dangerous areas and zones to be secured - flexibly and contactlessly.

Fig. 6/2
Stationary danger zone protection

Protecting horizontal dangerous areas

- Safely detecting persons and objects in dangerous areas of machines and plants
- Flexible programming, essentially any protective and warning fields can be set-up

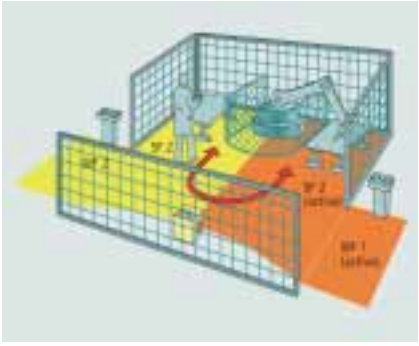


Fig. 6/3
Horizontal danger zone protection

Protecting horizontal dangerous areas with several protective fields

- Safely detecting persons in different dangerous areas by toggling between protective fields
- Increased availability by specifically securing only those areas that are presently active

Securing driverless transport vehicles - mobile applications

Our SIGUARD LS4-4 laser scanner can be used on driverless transport vehicles to monitor the route. Persons and objects are detected and the vehicle is automatically brought to a standstill when necessary. Previous protective systems such as bumpers, protective bars etc. only permit a low vehicle velocity. A significantly higher safety area is obtained with the SIGUARD LS4-4 laser scanner as contactless "leading bumper". This means that vehicles can operate faster and stopping times are reduced to the necessary minimum.

Fig. 6/4

Monitoring routes of driverless transport systems

- Persons and objects that approach the vehicle aresafely protected
- When compared to bumpers or protective bars, laser scanners offer a wider safety area therefore permitting higher speeds

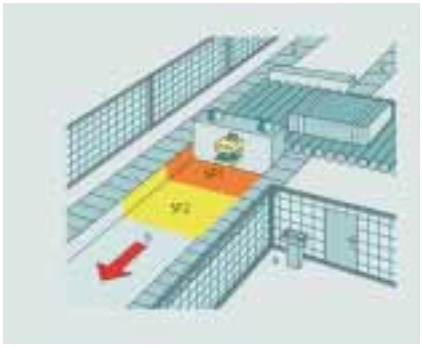


Fig. 6/5

Collision protection for vehicles

- Persons along the route are reliably protected
- Objects along the route are detected in plenty of time therefore avoiding damage to the vehicle and the material it is carrying

Product families/product groups

SIGUARD LS4-4 laser scanners, standard version

Fail-safe semiconductor outputs incl. LS4soft software — **3RG7834-6DD00**

SIGUARD LS4-4 laser scanner, ASIsafe

Fail-safe direct connection to ASIsafe incl. LS4soft software — **3SF7834-6DD00**

SIGUARD LS4-4 laser scanner, PROFIsafe

Fail-safe direct connection to PROFIBUS Incl. LS4soft software — **3SF7834-6PB00**

Fig. 6/6

SIGUARD LS4 laser scanners are available in three different versions. The appropriate version can be selected depending on whether the scanner is to be electrically integrated in the safety circuit. There is no difference in the various units as far as their function is concerned as laser scanner to secure dangerous areas.

In the standard version, the scanner has two fail-safe self-monitoring semiconductor outputs that allow it to be integrated into conventional circuits.

The bus versions for ASIsafe allow the fail-safe direct connection to ASIsafe.

The safety-related shutdown is realized, in this case via the AS-Interface safety monitor.

The second bus-capable version connects the laser scanner to PROFIBUS. The non-proprietary PROFIsafe profile is used to exchange data in both directions in a fail-safe way. Both the safety-related shutdown signal as well as also the protective field changeover can be transferred via the bus, controlled from the fail-safe PLC.

There is a range of accessories for the SIGUARD laser scanners. These include mounting brackets, software as well as connecting and programming cables.

Individual details regarding the accessories as well as additional SIGUARD laser scanner documents are provided in the Internet under:
http://www.siemens.de/fas

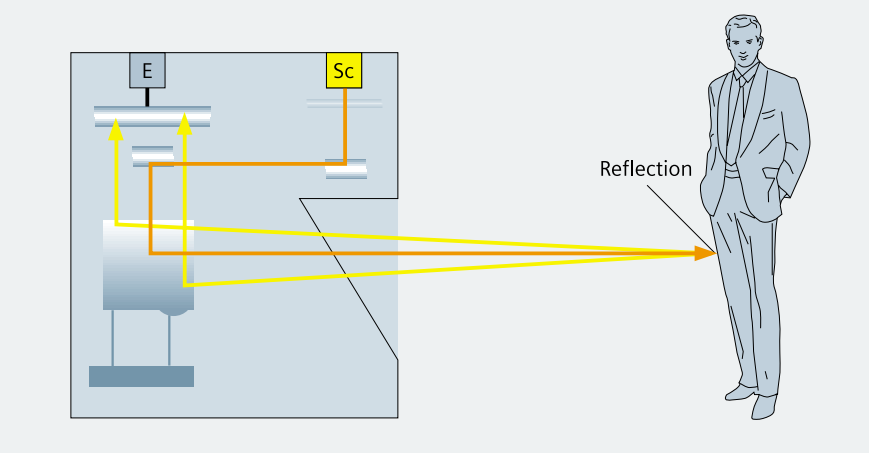


Fig. 6/7
Mode of operation

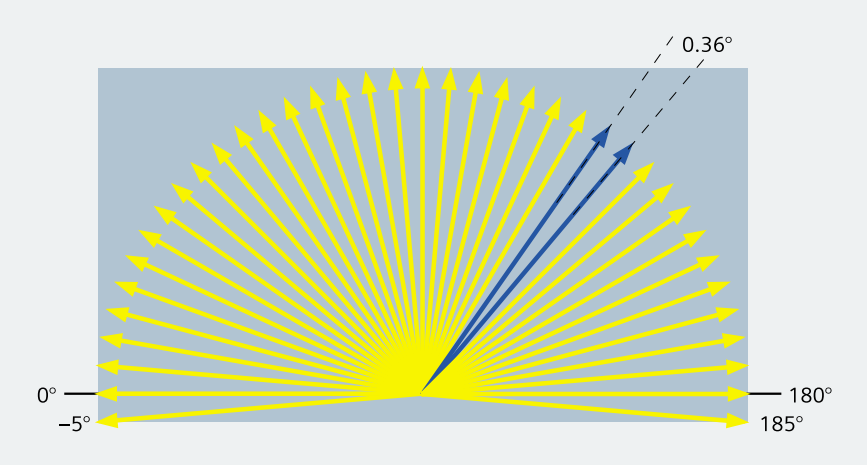


Fig. 6/8
Angular resolution

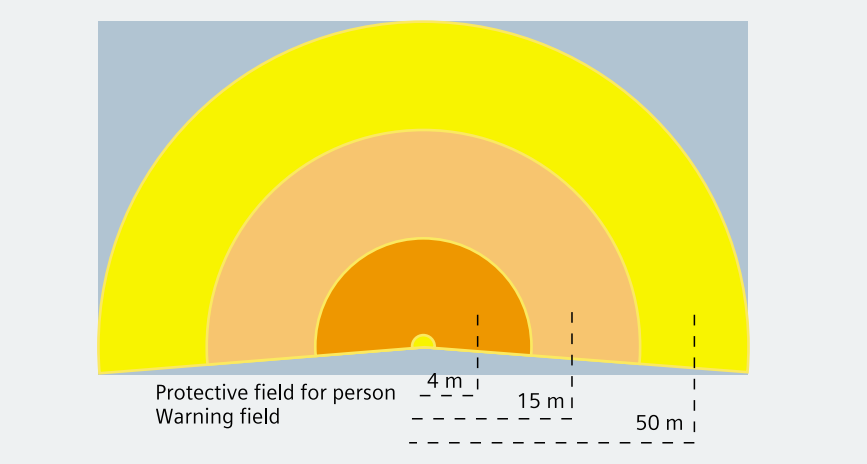


Fig. 6/9
Protective warning fields

Design

SIGUARD LS4 laser scanners are optical, electro-sensitive area scanners that have been mainly designed for the protection of personnel. The laser scanner continuously generates periodic light pulses, generated using a laser diode with the appropriate optical system. These light pulses are distributed over the complete operating area using an integrated rotating mirror. If persons or objects enter the field, then the scanner evaluates the reflected light pulses, and using the propagation time of the light pulses, precisely and continually calculates the precise position coordinates. If the defined personnel protective field is violated, it outputs a shutdown signal to immediately shut down the machine itself.

The operating range of the SIGUARD LS4 laser scanner is 190° and is subdivided into angular segments of 0.36° degrees. The scan rate is 25 scans per second. This means a light pulse in every segment every 40 ms. A special algorithm ensures that objects from a size of 70 mm onwards – this corresponds to the scanner resolution – are reliably detected. However, it is ensured that ambient effects – such as dust – do not have a negative impact on the availability of the plant or system.

SIGUARD LS4 laser scanners reliably detect persons – even if they are wearing dark clothing – safety-related up to 4 meters away. Persons and objects can be detected up to a distance of 15 meters away and an alarm message can be output (at this distance, it is not safety-related).

Functions

Protective field changeover

SIGUARD laser scanners can be flexibly adapted to any requirement thanks to four, variable protective field pairs for personnel protective field and warning field. These can be set at a PC. It can be used on stationary machines and plants, but also for mobile applications involving vehicles, driverless transport systems and trolleys. For example, for robots, various operating areas can be secured. The laser scanner scans one area after the other - both in time and space. For driverless transport systems, fast movement, slow movement, left-hand curves and righthand curves can be secured using four protective fields.

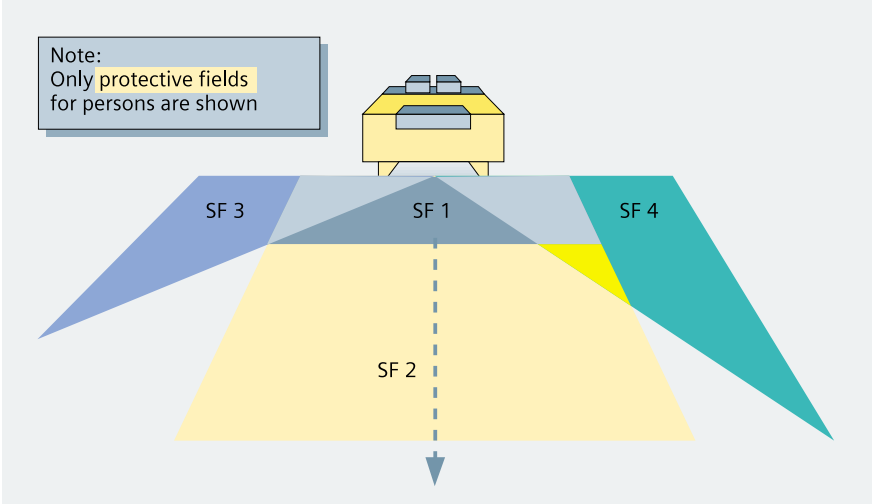


Fig. 6/10
Protective fields

Restart inhibit

The LS4 laser scanner has a restart inhibit function. This function can be selected and de-selected and is used to couple the machine restart to a manual agreement. This affects all protective fields and is independent of any protective field changeover operations.

The appropriate pushbutton must be located so that

- From the operator control position, the complete dangerous area and the protective field weakening are visible;
- From the operator control position it is not possible to directly enter/ access the dangerous area or the hazardous location.

Restart

Depending on the operating state, the restart input has several functions:

- Enables the restart inhibit after a protective field has been violated
- Enables the start inhibit after a system start
- Restart after a device fault has been resolved
- Detects a defined enable signal
  - after a device fault
  - after a protective field violation

  to initiate the restart inhibit

User-friendly LS4soft parameterizing software

The LS4soft operator control and parameterizing software allows parameter data to be set and the protective and warning fields.

- Protective fields can be configured in a user-friendly fashion using a PC or laptop
- Additional functions can be configured - such as protective field changeover, restart inhibit etc. using a software Wizard
- Extensive set of displays – e.g. defined protective fields, actual scan contour, system settings etc.
- Safety-related access protection using passwords with various authorization stages
- Can run under Microsoft Windows 95/98/2000/NT/XP

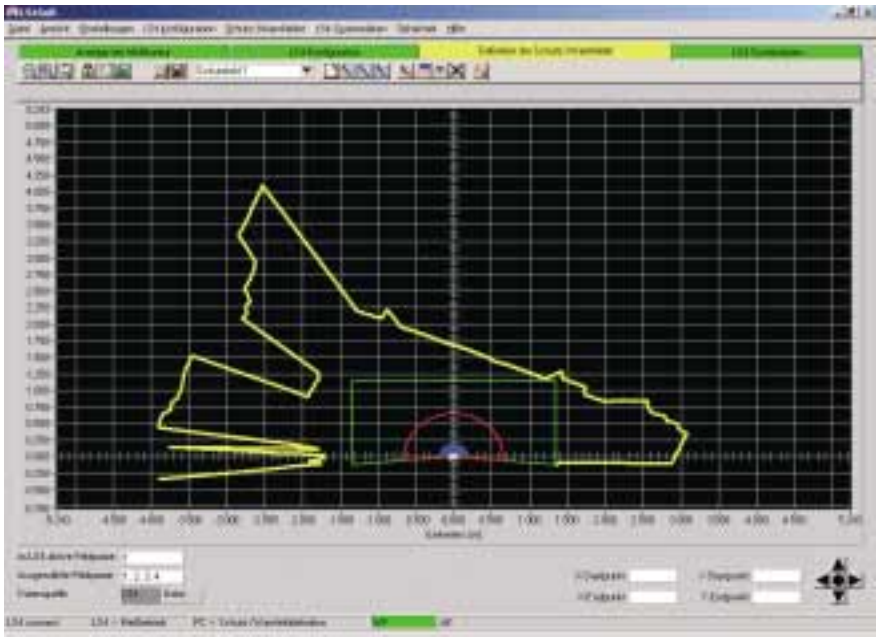


Fig. 6/11
LS4Soft software

Integration into the system

Depending on the requirements and type of safety system that the user has selected, safety sensors can be connected in various ways to the safety circuit of the particular machine or plant.

The basic ways of connecting various sensors is described in Chapter 3. Here, SIGUARD laser scanners offer every possibility. In addition to favorably-priced, conventional connection through fail-safe semiconductor outputs, the bus-capable versions allow laser scanners to be incorporated into Siemens automation solutions in a safety-related fashion using standard bus systems AS-Interface and PROFIBUS.

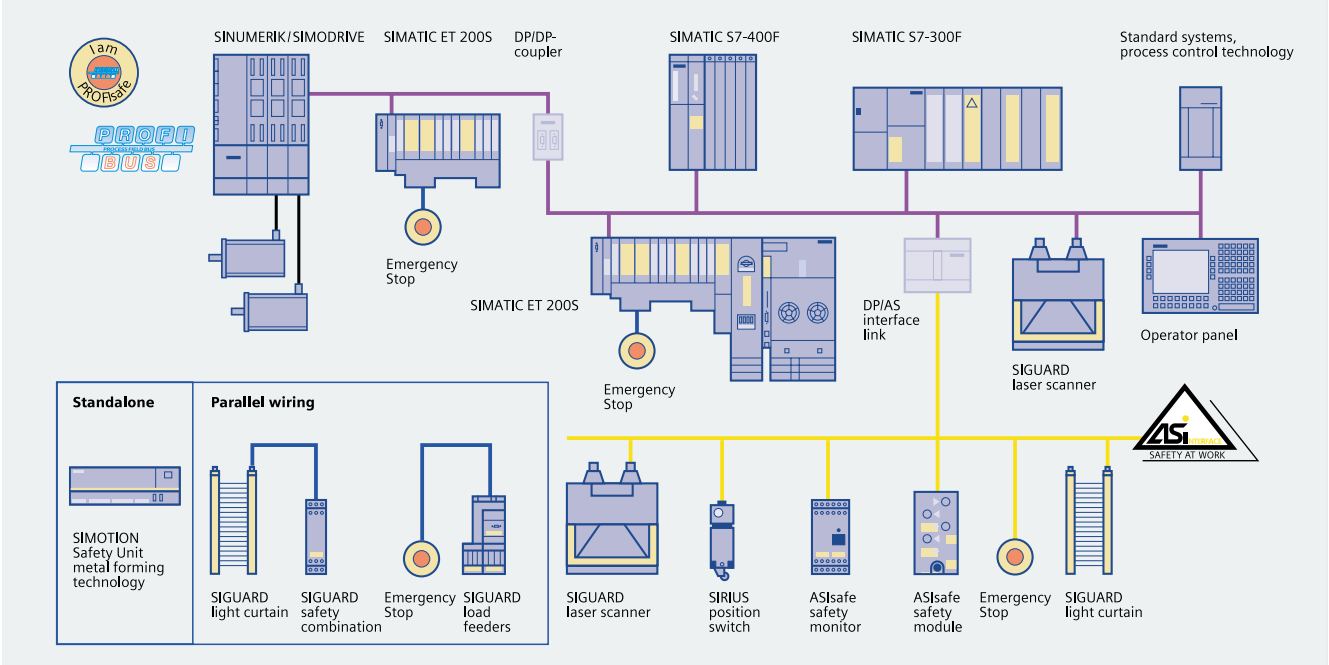


Fig. 6/12
Integration into the overall system

Application information

SIGUARD laser scanners are optical, electro-sensitive protective systems. Conditions relating to their correct use must be carefully observed when using these devices.

Some of the most essential issues are listed below:

General information:

- SIGUARD LS4-4 laser scanners should be mounted so that the-protective field completely covers the access to the dangerous area to be monitored.
- The scanner mounting position must be protected against moisture, dirt, as well as temperatures below 0°C or above 50°C.
- The mounting location should be selected so that the danger of mechanical damage is minimized. Additional protective covers or bars must be provided at exposed locations.
- Protective covers, panels, mounting niches and other machine-related elements may not have a negative impact on the scanner field.
- If areas are located in the scanner field of operation that cannot be scanned - as a result of permanent obstructions, that were defined as protective field limit, then these should be secured (e.g. using protective gates), so that persons in these areas that cannot be detected, cannot suddenly enter the protective field. When carrying-out a hazardous analysis of the machine or plant, this point must be carefully taken into account.
- Retro-reflectors or very bright surfaces, such as certain metals or ceramics, close to the protective field and at the scanner level height should be avoided as these can cause measuring faults and errors.
- In order to secure a consistent detection height at every point in the-protective field, the scanner – and therefore the beam level should be mounted parallel to the reference plane.
- If the “restart inhibit” function is activated, the restart button must be located outside the protective field at a location where the complete hazardous area is clearly visible and can be seen.

Information regarding protective field changeover:

In order to achieve optimum machine utilization, often, alternating loading/ machining cycles are implemented that results in changing hazardous areas. Also driverless transport vehicles, from their very nature, include various hazardous zones. If it can be expected that persons enter these areas, then it is absolutely necessary to provide an appropriate safety system. Our SIGUARD LS4 laser scanner fulfills many requirements regarding securing the widest range of applications thanks to its four freely-configurable protective and alarm fields that can be changed over (field pairs).

The user-friendly “LS4soft” operator program can be used to define the necessary field pair contours.

The field pairs are activated by connecting 24 V at the appropriate inputs.

If the SIGUARD LS4-4 laser scanner is to be restarted or it is necessary to toggle between various field pairs, then the following points must be carefully observed:

- The field pair intended for the start, must be defined, taking into special account the dangerous areas valid at this time.
- The second field pair should first be switched-in, and then the first field pair switched-out.
- The changeover must take place within 1 s.
- At no time, may the changeover sequence include de-activating all field pairs.
- With the exception of the changeover operation, only one field pair may be active at any one time.
- The sequence of the monitoring fields to be activated must ensure that at no time the application-related minimum protective field size is fallen below.
- Changeover signals may never change simultaneously due to a systematic fault. This is achieved by using independent circuits (e.g. separately actuated binary switches), taking into account the switching behavior described above.

Calculating the protective field

When using electro-sensitive optical protective systems such as laser scanners, it must always be ensured that any potentially hazardous machine motion is stopped before people are injured. This is the reason, for example, that the laser scanner must monitor a protective field that is large enough that after a dangerous area is entered, then there is enough time to initiate a machine stop.

Securing stationary dangerous areas

The following calculations must be used as basis when using a laser scanner to secure static dangerous areas.

Fig. 6/13
Securing stationary dangerous areas

In order to calculate the safety clearance and the minimum protective field depth, the following relationships apply in compliance with IEC 61496-3 and DIN EN 999 when approaching parallel to the protective field:

Safety clearance

$S = (K \times T) + C$

$C = 1200\ mm - 0.4\ H$

$C_{MIN} = 850\ mm$
$H_{MIN} = 15\ (d - 50\ mm)$
$H_{MAX} = 1000\ mm$

S = Safety clearance, minimum clearance from the dangerous area to the detection point, to the detection plane or to the protective field in mm

K = Approach velocity of a person or his body parts in mm/s (1600 mm/s)

T = Run-on time of the total system (response and braking times down to standstill) in s

C = Safety-related constant in mm to take into account intervention/penetration into the dangerous area before the protective device responds

C_{MIN} = Minimum value of the safety-related constant in mm (850 mm)

H = Height of the measured value detection plane from the reference point in mm

H_{MIN} = Minimum height of the measured value detection plane from the reference plane in mm

H_{MAX} = Maximum height of the measured value detection plane from the reference plane in mm

d = Scanner resolution in mm (70 mm, protective field width)

Tolerances

The sum of the system-specific and application-related protective field tolerances are calculated using the formula below:

$Z_{GES} = Z_{SM} + Z_{REFL}$

Z_{GES} = Sum of the system-specific and application-related protective field tolerances in mm

Z_{SM} = Measuring error of the scanner in mm

Z_{REFL} = Tolerance for reflectors that have to be taken into account in mm

Protective field depth

The protective field depth is the quantity, which is relevant for the protective field to be programmed into the scanner, is calculated according to the following formula:

$S_T = (K \times (T_{SCAN} + T_{MACH} + (T_{RUN\text{-}ON} \times L_{RUN\text{-}ON}))) + C + Z_{TOT}$

S_T = Protective field depth, clearance from the hazardous area to the detection point/line, including the system and application-related tolerances in mm

K = Approach velocity of a person or his body parts in mm/s (1600 mm/s)

T_{SCAN} = Response time of the scanner in s

T_{MACH} = Response time of the machine or plant in s

$T_{RUN\text{-}ON}$ = Run-on time of the complete system in s

$L_{RUN\text{-}ON}$= Factor for the run-on-increase (1.1 if no other values are known)

C = Safety-related constant in mm

Mounting height

Acc. to DIN EN 999, the lowest permissible height of the scan plane from the base plane for persons is calculated using the following formula:

$H_{MIN} = 15 * (d - 50\ mm)$

H_{MIN} = lowest permissible scan level from the base plane

d = Resolution of the scanner in mm (70 mm, protective field width)

The permissible height range of the scan plane lies between 300 and 1000 mm above the base plane.

If the application requires a higher scan plan than 300 mm, or if there is a possibility that children may attempt to access the dangerous area, then in the dangerous area analysis, the potential danger of crawling below the scan plane must be taken into account.

Protecting driverless transport vehicles - mobile applications

The following essential conditions must be carefully observed when using the SIGUARD laser scanner to protect driverless transport systems - i.e. mobile applications.

Fig. 6/14

Safety clearance

When calculating the safety clearance, the following relationships apply according to IEC 61496-3:

$S = (V_{MAXFTS} \times T) + S_{ANHALT}$

V_{MAXFTS} = Maximum velocity of the driverless vehicle in mm/s

T = Response time of the scanner and the driverless vehicle in s

S_{ANHALT} = Stopping distance of the driverless vehicle down to standstill in mm

Protective field depth

The depth of the protective field in the direction of travel, referred to the distance between the limit of the vehicle and the protective field limiting line is calculated according to the following formula:

$S_T = V_{MAXFTS} \times (T_{SCAN} + T_{FTS}) + (S_{ANHALT} \times L_{ANHALT}) + Z_{GES}$

S_T = Protective field depth in the direction of travel in mm

V_{MAXFTS} = Maximum velocity of the driverless vehicle in mm/s

T_{SCAN} = Response time of the scanner in s

T_{FTS} = Response time of the driverless vehicle in s

L_{ANHALT} = Factor for brake wear (1.1 if no other values are known)

Z_{GES} = Sum of the system-specific and application related tolerances in mm

Tolerances

$Z_{GES} = Z_{SM} + Z_{REFL} + Z_{AFUSS} + Z_{AU}$

Z_{SM} = Scanner measuring error in mm

Z_{REFL} = Tolerance in mm for the reflectors to be taken into account

Z_{AFUSS} = Tolerance in mm for the driverless vehicle and the floor

Z_{AU} = Application-relevant tolerance in mm (e.g. under-cuts)

Mounting height

The mounting height should always be kept as low as possible in order to prevent somebody crawling below the protective field. This parameter is restricted by e.g. unevenness in the floor surface and the spring travel of the driverless vehicle.

The maximum mounting height should be selected so that an object (horizontal cylinder with a 200 mm diameter) is reliably detected (refer to DIN EN 1525). This should be checked at the maximum protective field depth. Regarding adequate detection resolution, for a driverless vehicle application, an object (upright cylinder) with a diameter of 70 mm, protective field width, is sufficient.

The examples described here provide the basic principles when it comes to calculating protective fields. More detailed information and calculation example are provided in the Technical Instructions of the SIGUARD laser scanners in the Internet under: http://www.siemens.de/fas

Technical data

Protective data	
Protective field for persons	
Detection range	0-4 m (no dead zones when correctly mounted)
Remission capacity	Min. 1.8% (matt-black)
Measuring error	Max. 83 mm (for a protective radius < 3.5 m) Max. 100 mm (for a protective radius > 3.5 m)
Object size	70 mm (cylindrical test body)
Response time	Min. 80 ms (for the standard version)
Number of protective fields	4 (can be switched-over using switching inputs)
Output	Two fail-safe PNP transistor outputs 24 V/250 mA or safe bus connection
Category	Category 3 acc. to EN 954-1, type 3 acc. to DIN EN IEC 61496-1, IEC 61496-3 Requirement Class 4 acc. to DIN V 19250, single-fault proof
Starting	The start test routine and the start inhibit can be separately parameterized
Warning field	
Detection range	0-15 m
Remission capacity	Min. 20%
Object size	150 x 150 mm
Response time	Min. 80 ms (corresponds to 2 scans)
Number of protective fields	4 (can be switched-over using switching inputs)
Output	PNP transistor output, max. 100 mA and connection to the bus
Optical properties	
Angular range	190°
Angular resolution	0,36°
Scan rate	25 scans/s or 40 ms/scan
Laser protection class	Class 1 (safe to the eyes), DIN EN 60825-1, wavelength = 905 nm, Beam divergence = 2 mrad, time base = 100 s

General data

	Standard	AS-Interface	PROFIBUS
Electrical supply			
Power supply	+24 V DC +20 % / -30 %, power supply according to IEC 742 with safety transformer or		
	comparable for DC/DC converters		
Overcurrent protection	Using a fuse 1.25 A medium slow-acting in the cabinet		
Current drain	Approx. 300 mA	Approx. 350 mA	Approx. 350 mA
(use a power supply unit with 2.5 A)			
Power drain	Approx. 8 W at 24 V	Approx. 9 W at 24 V	Approx. 9 W at 24 V
	plus the output load		
Inputs			
Restart/reset	A command device is connected for the mode “with restart inhibit”		
	and/or equipment set, dynamically monitored		
Field pair changeover	4 field pairs are selected using 4 control lines with internal monitoring (field pair = 1 protective field and 1 warning field), 24 V DC opto de-coupled	4 field pairs are selected using 4 control lines with internal monitoring (field pair = 1 protective field and 1 warning field), 24 V DC opto de-coupled	Field pair changeover via PROFIBUS (PROFIsafe profile)
Outputs			
Protective field	2 x safety semiconductor outputs, PNP max. 250 mA monitored for short-circuits, overcurrent protected	AS-Interface, safety slave (ASIsafe)	PROFIBUS, safety slave (PROFIsafe profile)
Warning field/ dirt/fault	PNP transistor output max. 100 mA	AS-Interface	PROFIBUS
Software			
Operator software	Communications and parameterizing software LS4soft under Windows 95/98/2000/NT/XP		
	with secure protocol for programming		
Interfaces			
RS 232, RS 422	To parameterize the units and define fields using LS4soft		
	(RS 422 only for standard versions)		
Environment and material			
Degree of protection	IP 65 acc. to IEC 60529		
Shock hazard protection	Protective Class 2		
Operating temperature	0 ... + 50°C		
Storage temperature	- 20°C ... + 60°C		
Humidity	DIN 40040 Table 10, code letter E (relatively dry)		
Dimensions (W x H x D) in mm	140 x 155 x 135	140 x 168 x 165	140 x 168 x 165

6.2 SIGUARD light curtains and light grids

Relevant Standards

- EN 61 496-1, -2, IEC 61 496-1, -2 (requirements for contactless protective systems)
- EN 999 (e.g. calculating safety clearances)
- EN 954-1 (safety of machinery safety related parts of controls)

Fig. 6/15
SIGUARD light curtains, light grids and evaluation units

SIGUARD light curtains and light grids

- Are active opto-electronic protective devices (AOPD)
- Correspond to type 2 (3RG78 41) or type 4 (3RG78 42/4) acc. to EN 61496-1, -2
- Are EC-prototype tested
- Protect operating personnel at or close to hazardous machines
- Operate contactlessly
- Are wear-free when compared to mech. systems (e.g. contact mats)

The prerequisites are as follows:

- Correctly mounted and installed
- Correctly connected to the machine control

Information is provided in this section and in the Instruction Manuals provided with the particular devices.

Tests/Service

The devices are EC type tested (TÜV [German Technical Inspectorate] Product Service in conjunction with the Institute for Health and Safety at Work - BGIA).

Configuration

- Using teach-in with opto-magnetic key
- Configuration data is transferred using a plug-in configuration card

Features

SIGUARD light curtains, grids and transceivers 3RG7844/ 3SF7844 with integrated evaluation for category 4 acc. to EN 954-1

- Resolution 14, 30 and 50 mm
  Protective field heights of 150 to 3 000 mm
  ranges 0.3 to 6 m or 0.8 to 18 m.
- 2, 3 or 4-beam light grids
  beam clearance 500, 400 and 300 mm
  ranges 0.8 to 18 m or 6 to 70 m
- 2-beam transceiver
  beam clearance 500 mm
  range 0.8 to 6 m
- Host and guest devices can be cascaded for higher protective field heights and lengths or for angled arrangements

Integrated functions:

Standard function package
- Start/restart inhibit
- Contact monitoring
- Multi-scan

Blanking function package
- Functions of the standard function package and additionally
- Fixed blanking
- Floating blanking
- Reduced resolution

Muting function package
- Functions of the standard function package and additionally
- 4-sensor, sequential muting
- 2-sensor, parallel muting
- 3-sensor, direction muting
- 4-sensor, parallel muting

Cycle control function package
- Functions of the standard function package and additionally
- Cycle control using 1-clock and 2-clock cycle operation

Configuration:

- Using teach-in with opto-magnetic key
- Configuration data is transferred using a plug-in configuration card
- 2 data transfer channels
- Host and guest devices can be cascaded
- Extended display (2x7 segments)

Outputs/connections available for every function package

- Local interface to connect additional safety sensors
- Transistor outputs with cable gland or Brad-Harrison-connectors
- Relay outputs with Hirschmann connectors
- Connection to ASIsafe

SIGUARD 3RG7842/3SF7842 light curtains, grids for Category 4 acc. to EN 954-1

- Resolution 14, 30, 50 and 90 mm
  Protective field heights from 150 to 3 000 mm
  Ranges 0.3 to 6 m or 0.8 to 18 m

- 2, 3 or 4-beam light grids, beam clearance 500, 400 and 300 mm
  Ranges 0.8 to 18 m or 6 to 70 m

- Host and guest devices can be cascaded for higher protective field heights or lengths and for angled arrangements

SIGUARD 3RG7841 light curtains for Category 2 acc. EN 954-1

- Resolution 30, 55 and 80 mm
  protective field heights of 150 to 1 800 mm
  Ranges 0.3 to 6 m

- Host and guest devices can be cascaded for higher protective field heights or lengths and for angled arrangements

SIGUARD 3RG7825/47 evaluation units for Category 2 and 4 acc. to EN 954-1

- These are used to connect the safety-related signals of light curtains, light grids, light barriers and transceivers in the machine control.

- Start/restart inhibit

- Contactor monitoring

- Muting

- Cycle control

- Predictive failure alarm for the relay contacts

- Diagnostic function using PC

- Numerous signaling outputs to a higher-level control

Applications

Light curtains for finger and hand protection at dangerous locations

These devices provide protection against fingers and hands entering dangerous zones when the light curtains are mounted close to the potentially hazardous machine component (finger and hand protection)

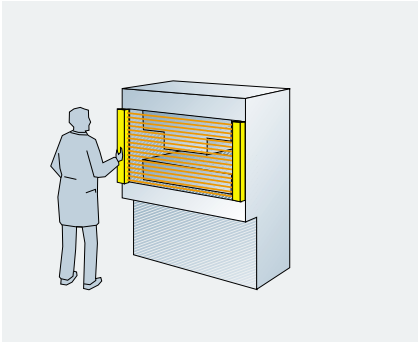


Fig. 6/16
Finger/hand protection

Device selection

Light curtains for Category 2 or 4 with 14 and 30 mm resolution

Applications

e.g. presses, punches, filter presses, cutting machines

Light curtains to horizontally protect dangerous areas

These devices safely detect personnel in dangerous areas when the light curtain is mounted close the floor (it is not possible to crawl below)

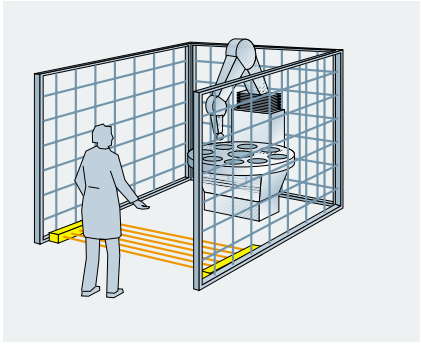


Fig. 6/17
50 mm dangerous area protection

Device selection

Light curtains for Category 2 or 4 with 50 or 55 mm resolution

Applications

e.g. welding and assembly lines as well as robots in automobile construction

Light curtains to horizontally protect dangerous areas

Safely detect personnel in dangerous areas when the light curtains are mounted in heights of 0.6 to 1 m

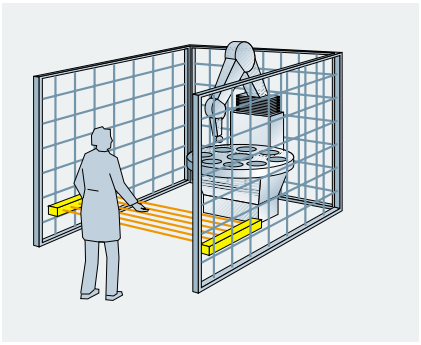


Fig. 6/18
90 mm dangerous area protection

Device selection

Light curtains for Category 2 or 4 with 80 or 90 mm resolution

Applications

e.g. welding and assembly lines as well as robots in automobile construction

Light grids for securing access

These devices safely detect personnel when they attempt to enter dangerous areas.

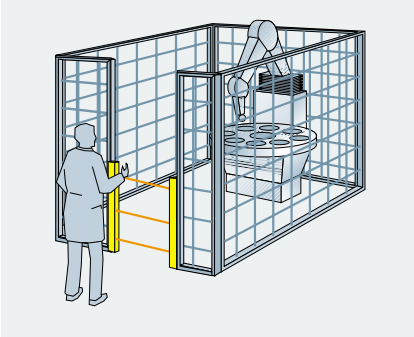


Fig. 6/19
18 m access protection

Device selection

2, 3 or 4-beam light grids for Category 4 with 18 m range

Applications

Securing access, e.g. to robots or automatic handling machines

Light grid to secure access to large areas

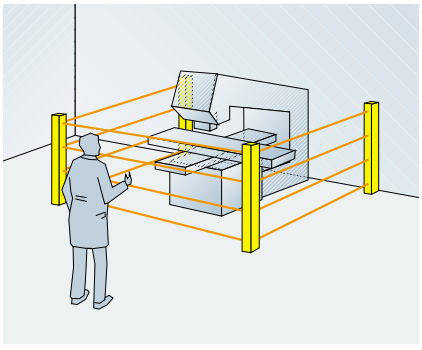


Fig. 6/20
60 m access protection

Safely detect personnel when entering dangerous areas.

Secures larger dangerous areas as a result of the high 70 m range.

Device selection

2, 3 or 4-beam light grids for Category 4 up to a range of 70 m.

Applications

Secures access, e.g. to automatic machining centers or palletizing equipment.

The following factors must be complied with when using light systems:

- It may not be possible to reach over reach under or go behind the protective field - it may be necessary to locate additional protective devices and guards.
- The control of the machine must be able to be electrically influenced and it must permitted to immediately terminate the potentially hazardous state - and that in every operating phase.
- Danger of injury due to heat, radiation or the ejection of materials and components from the machine must be prevented using other suitable measures.
- Ambient/environmental conditions may not have a negative impact on the light protection system.

Safety clearance

Machine movement or motion which can be potentially hazardous must be safely stopped before personnel are injured. In this case, the safety clearance between the light curtain and hazardous location must be maintained.

If a C Standard with other requirements is not applicable then the minimum clearance to the dangerous area is calculated using the following formula according to EN 999:

$S = (K * T) + C$

Where:

S the minimum clearance in millimeters, measured from the dangerous area to the protective field (or detection point, to the detection line, to the detection plane)

K a parameter in millimeters per millisecond, derived from data regarding the approach velocity of the body or parts of the body

T the run-on of the complete system in milliseconds
t1: response time of the protective device
t2: run-on time of the machine

C an additional clearance in millimeters, is used as basis for entering in the dangerous zone before the protective device trips

The values for K and C depend on the protective function (e.g. hand or finger protection, access security), resolution and the approach direction.

Light curtain in a vertical arrangement in (max. 40 mm)

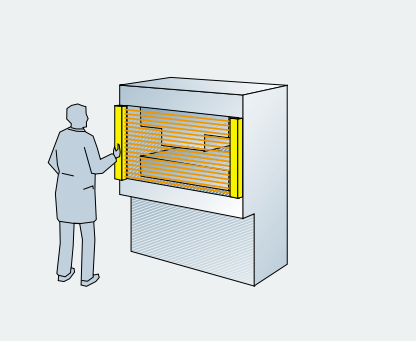


Fig. 6/21

It may not be possible to reach around, reach over or reach under the protective field. This can be implemented using additional mechanical meshes/ gates or by cascading the host and guest light curtains.

The minimum safety clearance S is calculated according to

S = (K * T) + C

With

K = 2 mm/ms
C = 8 (d-14 mm),
however, not less than 0.

Whereby

d = resolution of the light curtain in mm.

If the calculation results in a value less than 100 mm, then under all circumstances, a minimum clearance of 100 mm must be maintained.

If the calculation results in a value greater than 500 mm, then this can be repeated with K=1.6 mm/ms. Under all circumstances, a minimum clearance of 500 mm must be maintained.

If the clearance between the light curtain and the machine is greater than 75 mm, then protection must be provided against reaching around (e.g. using a horizontally arranged light curtain).

Light curtain in a vertical arrangement (resolution 40 mm ≤ 70 mm)

The minimum safety clearance S is calculated as follows

S = (K * T) + C

With

K = 1.6 mm/ms

C = 850 mm

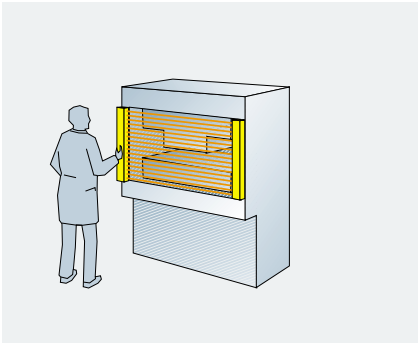


Fig. 6/22

Multi-beam light grids in a vertical arrangement for access security

It may not be possible to reach around, reach over or reach under the protective field. This can be implemented using additional mechanical gates or by cascading the host and guest light curtains.

The number and distance between the light beams depends on the risk evaluation and on the machine-specific regulations.

The minimum safety clearance is calculated as follows according to EN 999:

S = (K * T) + C

With

K = 1.6 mm/ms

C = 850 mm

Number of beams and height above the reference plane in mm	
4	300, 600, 900, 1200
3	300, 700, 1100
2	400, 900

Light curtains in a horizontal arrangement to secure dangerous areas

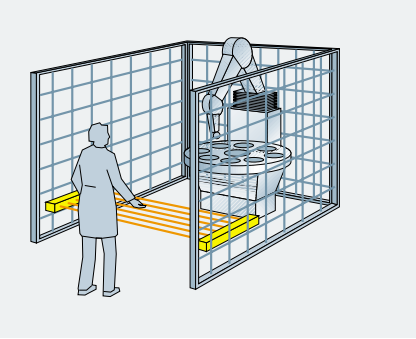


Fig. 6/23

When securing dangerous areas using horizontally mounted light curtains, the height H of the protective field may be a maximum of 1000 mm. If H is greater than 300 mm (200 mm if children are present), then it is possible to crawl below the protective field. This must be taken into account when accessing the risk.

The lowest permissible mounting height depends on the resolution of the light curtain in order to ensure that the human leg or joint in the foot can be safety detected.

$S = (K * T) + C$

$K = 1.6$ mm/ms

$C = (1200 \text{ mm} - 0.4 \times H)$

Where:

H = Height of the protective field above the reference plane

$H_{max} = 1000$ mm

$H_{min} = 15\ (d - 50 \text{ mm})$

d = Resolution of the light curtain

If the calculation for C results in a lower value than 850 mm, then a minimum value of C = 850 mm should be assumed.

General description

A SIGUARD light curtain or light grid comprises a sender and a receiver that are mounted opposite to one another. Depending on the resolution and length, a specific number of transmitting and receiving diodes are located one above the other. The infrared LEDs of the transmitter send short light pulses that are received by the associated receiver diodes.

The transmitter and receiver are synchronized with one another optically without requiring a direct electrical connection.

Depending on the application, light curtains are required with various resolutions.

The resolution (detection capability) of a safety light curtain is that size of obstruction that will be safely detected at every position in the protective field and thus result in a shutdown command.

The transceiver comprises a sender (transmitter) and a receiver in one device (transceiver). The infrared light from the transmitter diode is reflected twice through 90° using a mirror and therefore returns to the receiver diode of the transceiver. This therefore creates a two-beam light grid - that is more favorable than a conventional light grid with separate sender and receiver. The device has five-pin M12 sockets at the front panel. Muting sensors can be directly connected to this.

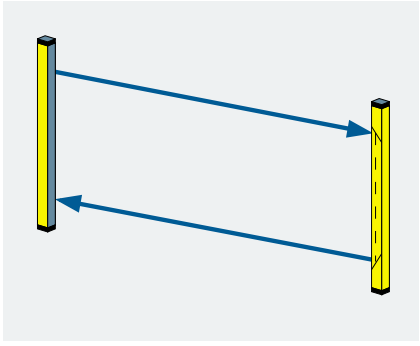


Fig. 6/24
Transceiver principle

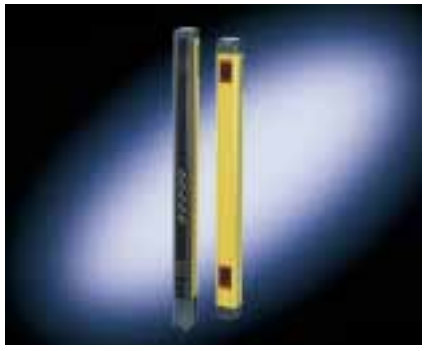


Fig. 6/25
Transceiver

If all of the light axes are free, the OSSDs of the receiver/transceiver switch to 24 V. However, if at least one light axis is interrupted, the outputs safely shut down - e.g. when intervening in the hazardous area/location.

If the outputs of the light curtains are shut down, with an additional circuit, this can be used to safely stop the potentially hazardous motion of the machine. This circuit can be a SIGUARD 3RG78 25/47 evaluation unit or a safety-related control (e.g. S7-400F/FH, S7-315F, SINUMERIK).

SIGUARD light curtains and light grids are available for applications, safety Category 2 and for the highest safety requirements for safety Category 4 acc. to EN 954-1.

Testing and monitoring light curtains

For 3RG78 42/44 and 3SF78 42/44 light curtains (safety Category 4), the outputs are redundant and self-monitoring. This means that they detect a possible incorrect function as well as when a fault occurs in the external circuit (e.g. cross-circuit fault or short-circuit).

SIGUARD 3RG78 25 and 3RG78 47 evaluation units (with the exception of 3RG78 47-4BB) automatically carry-out a test without interrupting the process. A failure (e.g. loss of detection capability), which could have a negative impact on correct operation is then detected at the next test cycle.

The test signal of the evaluation units can also be used for 3RG7841 light curtains, safety Category 2.

Host/guest combinations

By cascading devices, the optical axis can be extended and in turn the protective field height; whereby, using a flexibly connecting cable between the host and guest devices, protection in the horizontal and vertical planes can be simultaneously implemented. The safety outputs and the processor tasks run on the host device so that guest devices can be connected, independently. The standard cable that can be used to connect the host and guest devices is 300 mm long. The maximum total length of a host/guest combination is restricted to 240 light beams.

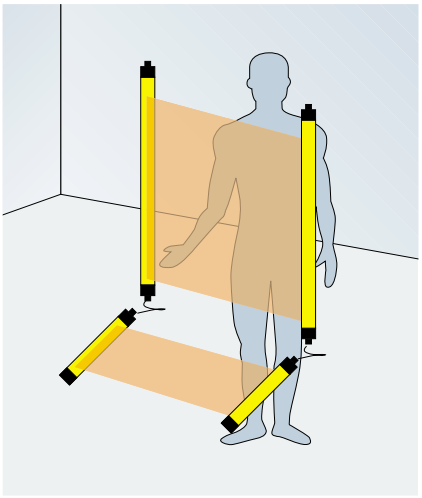


Fig. 6/26
Host Guest

Software

Both SIGUARD light curtains, types 2 and 4 as well as evaluation units can be connected to a PC or laptop via the serial interface for visualization and diagnostics.

The diagnostics software for light curtains visualizes the statuses of the individual light beams, which means that devices can be simply aligned. Furthermore, the software allows this data to be acquired during operation so that, for example, sporadic faults and errors can be pinpointed.

Fig. 6/27
Screen of the diagnostics software for light curtains

The software for the evaluation units offers the above-mentioned possibility of visualizing and tracing signals for the SIGUARD evaluation units. The diagnostics cable is simply connected to the socket of the unit. This software automatically recognizes the device version and displays the statuses of all of the inputs and outputs.

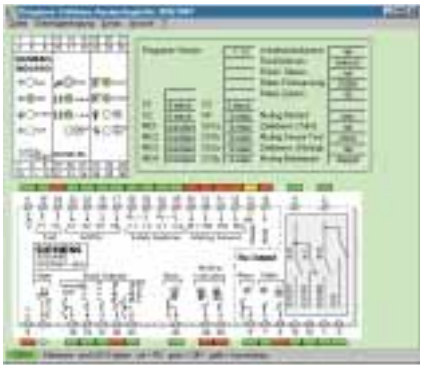


Fig. 6/28
Screen representation, diagnostics software for evaluation units

Accessories

There is a range of accessories, optimized for use in the field that simplify mounting, alignment/adjustment, commissioning and troubleshooting. These include retaining columns, deflection mirror columns, deflection mirrors, retaining brackets and laser alignment devices. The mounting columns and beam deflecting mirror columns allow the light curtains, light grids and transceivers to be simply mounted to the floor. After the columns have been bolted to the floor, a special mechanical design allows the light beams to be precisely aligned.

This operation can be easily carried-out using the laser alignment devices.

Connection versions

The light curtains, light grids and transceivers are available in the following connection versions:

- Transistor output with cable gland
  The user routes the power supply cable through a cable gland located in the end cap of the devices and connects this to the screw terminals in the connection cap. For senders (transmitters), only the power supply voltage is fed in; receivers and transceivers have in addition, the two safety switching outputs OSSD1 and OSSD2 as well as additional signal inputs and outputs.

- Relay outputs with Hirschmann connection
  The receiver/transceiver has 2 relay outputs and a connection for a Hirschmann connector in the end cap. The relay outputs with Hirschmann connection are suitable for switching protective extra low voltages up to 42 V AC/DC.

  For the transistor version, the sender doesn't have its own outputs, but has a Hirschmann connection to connect to the machine interface. The appropriate cable connection socket including the crimp contacts and the complete connecting cable - in various lengths - are available as accessories in both straight or angled versions.

- Machine interface with ASIsafe connection
  A 3-pin M12 connector is provided in the end cap and a 5-pole M12 connector for the receiver/transceiver. These connectors are used to connect to the AS-Interface. A suitable coupling module is available as accessory so that the device can be connected with a 1:1 connection using a standard M12 extension cable. In order to save using a bus address, it is possible to combine a sender with cable gland or Hirschmann connector with a receiver with ASIsafe connection.

Functions

Functions packages for integrated evaluation

For SIGUARD 3RG7842 light curtains and light grids, Category 4 as well as SIGUARD 3RG78 41 light curtains, Category 2, functions such as start/restart inhibit, contactor monitoring and muting are only possible in conjunction with an 3RG78 25 or 3RG7847 evaluation unit.

SIGUARD 3RG7844 light curtains and light grids, Category 4 represent a supplement to the existing product range, and are available in four function packages, in which, the following functions are integrated in the devices. This means that an evaluation unit is no longer required to implement these functions:

- Function package “Standard”:
  Start/restart inhibit, multi-scan, contactor monitoring, two data transfer channels as well as an optional 2-channel safety circuit with contacts.

- Function package “blanking”:
  This is just the same as the “standard” function package and in addition, the fixed blanking, floating blanking and reduced resolution functions

- Function package, “muting”: This is the same as the “standard” function package and in addition the muting function in order to bypass the protective device/equipment for a limited time as part of the correct functionality.

- Function package, cycle control:
  This is the same as the “Standard” function package and in addition, the cycle control function.
  This is intended not only to provide protection using the protective device, but also control it in a safety-related fashion.

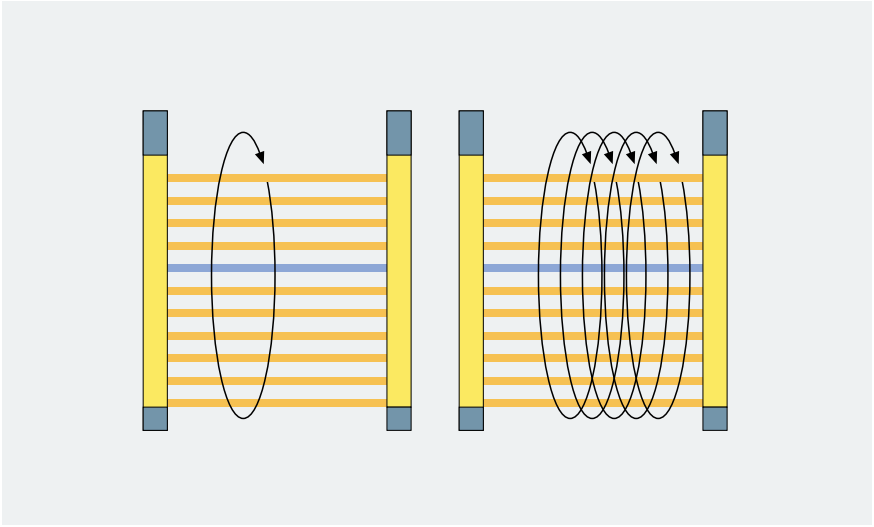


Fig. 6/29
Multi-scan

Increasing the noise immunity with respect to strong external light (multi-scan)

If disturbances are expected as a result of strong external light under “noisy” ambient conditions - for instance - from stroboscope lamps or welding robots, it is often more favorable, when a beam is interrupted, to first wait as to whether the interruption continues, before the outputs are shut down.

If the beam is no longer interrupted, then this could have been triggered by ambient conditions which would mean that it is not necessary to shut down the plant or system.

If the beam remains interrupted, then it must be assumed that there is a potential hazard and the plant or system is shut down. This increases the plant availability. However, the response time and therefore the safety clearance is increased.

If the multi-scan mode is used, the receiver and/or transceiver go into the OFF state for a defined number of consecutive scans as soon as the light beams are interrupted.

Data transfer channels

SIGUARD 3RG784 and 3SF784 light curtains, light grids and transceivers are equipped with two different data transfer channels. In order to differentiate between the transmitted infrared light and the ambient light, and to avoid influence, e.g. from warning lights of passing forklift trucks or welding sparks, data is transferred in pulse packets.

If two protective fields of a machine are located directly next to one another and there is a danger that, for example, beams from sender 1 are received by receiver 2, two different data transfer channels can be selected. The transfer channels must be changed over both in the sender as well as in the receiver so that the two appropriate devices recognize one another.

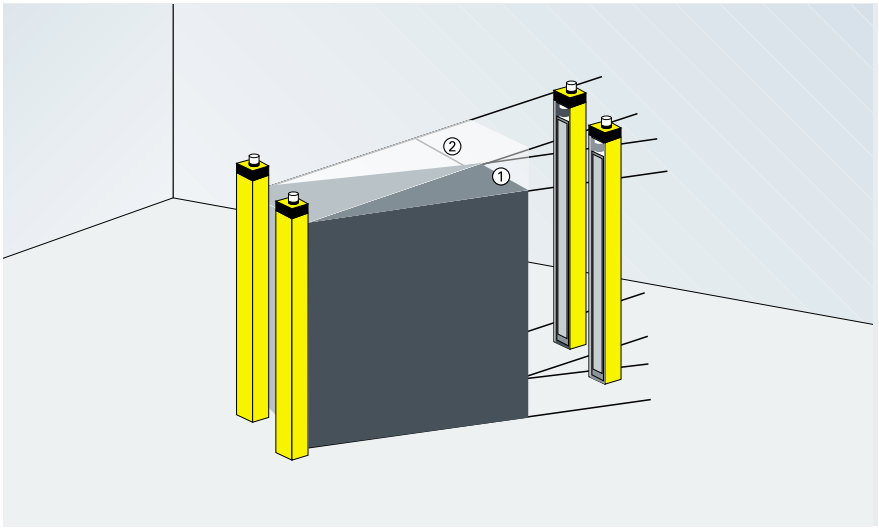


Fig. 6/30
Data transfer channels

Start/restart inhibit

In order to prevent that the plant or system immediately starts to run again after a protective field was interrupted and then becomes free again, the start/restart inhibit function can be activated. The receiver or the transceiver only go into the ON state if a start button is pressed and is then released again. The start button must be pressed and released within a time window of between 0.1 and 4 seconds.

The start/restart inhibit is mandatory for access security, as only the entry to the dangerous area is monitored, but not the area between the protective field and the potentially hazardous motion.

The command device to enable the start/restart inhibit must be mounted so that the

- dangerous area can be easily seen from the command device and this
- command device cannot be actuated from the dangerous area

Contactor monitoring

The contactor monitoring function is used to monitor the contactors, relays or valves downstream from the light curtain. In this case, switching elements with positively-driven feedback contacts are mandatory.

For the dynamic contactor monitoring function, a check is made whether, after the enable, the feedback circuit has opened within 300 ms, and after the OSSD has shut down, re-closes again within 300 ms. If this is not the case, then the enable circuit returns to the OFF state.

Blanking functions

There are three different blanking functions that can be selected depending on the application:

- Fixed blanking to suppress fixed objects that do not move
- Floating blanking for moving objects that are always in the protective field
- Reduced resolution for moving objects in the protective field that can temporarily exit the protective field

Depending on the blanking type, the system is configured using teach-in and the safety keys or using the DIP switch in the connection cap. It is neither necessary to have a PC nor connect a PC to the programming interface.

Fixed blanking

The “fixed blanking” function can be used if stationary objects are permanently in the protective field of the light curtain. If this function is not used, the light curtain would shut down as not all of the beams transmitted by the sender would be received by the receiver.

Fixed blanking is possible at any location of the light curtain, whereby the number of blanked beams is unrestricted. The first beam after the display field cannot be blanked as this involves the synchronizing beam between the sender and receiver.

The light curtain permanently monitors the blanked object: The light curtain checks whether the object is located precisely at the position which was taught-in. If the object is removed, the light curtain shuts down the plant - otherwise a safety risk would be created as a result of the blanked light beam.

Floating blanking

The floating blanking function can be used if moving objects are continually in the light curtain area. For floating blanking, several objects can be simultaneously blanked. The number of floating beams that can be blanked is unlimited.

The object that is blanked, floating, is permanently monitored: The light curtain checks as to whether the object is permanently in the light curtain area.

Reduced resolution

If moving objects are not permanently in the protective field of the light curtain, the reduced resolution function can be used. Contrary to floating blanking, the object is not permanently monitored. This means that no beam has to be interrupted, but, depending on the beam reduction selected, several beams can be interrupted.

The effective light curtain resolution is changed when using the "reduced resolution" function. The safety clearance must be re-calculated using the effective resolution.

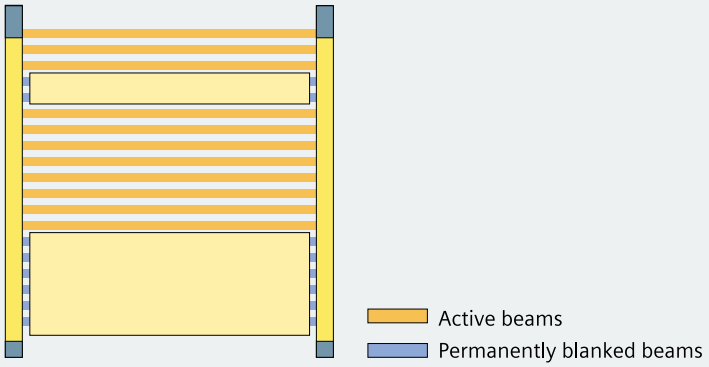


Fig. 6/31
Fixed blanking

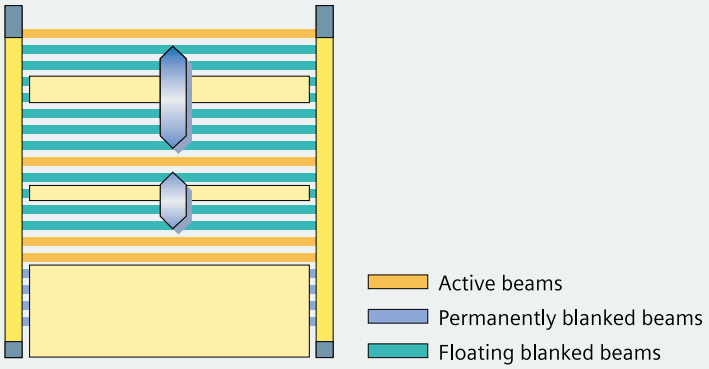


Fig. 6/32
Floating blanking

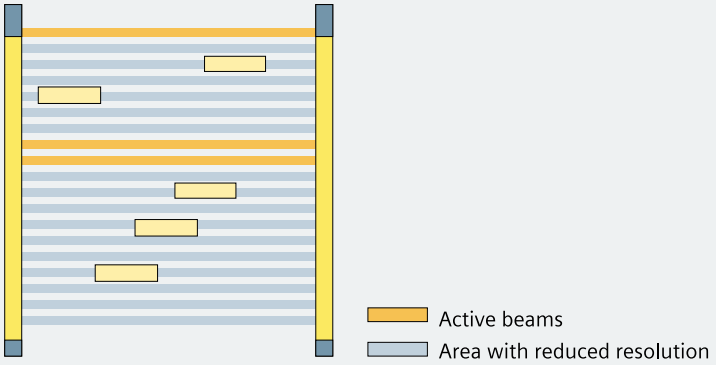


Fig. 6/33
Reduced resolution

Muting functions

When vertically arranged, light curtains, light grids and transceivers are often used to secure access points. The protective effect can be blanked (suppressed) using additional sensor signals in order to for example, transport material in and out of the hazardous zone.The protective field is temporarily blanked, and after the material has been transported, is re-activated again. During the muting operation, it must be guaranteed that nobody can enter the hazardous zone.

From the number of connected sensors and the sequence of the muting signals the devices automatically detect the muting mode “sequential muting” if inputs M1 to M4 are assigned, and 2-sensor parallel muting, if signals M2 and M3 are assigned (refer to Fig. 6/34 and Fig. 6/35). In addition, the SIGUARD 3RG78 44 and 3SF 78 44 light curtains, light grids and transceivers have the muting functions “3-sensor direction muting” and “4-sensor parallel muting”.

4-sensor sequential muting

If the material that is to be transported into the dangerous area always has the same dimensions and there are no space restrictions, then sequential muting is the preferred solution. For sequential muting, four muting sensors are connected. These must then be activated in a specified sequence in order to initiate the muting operation. They can be activated in the sequence M1, M2, M3, M4 or also in the sequence M4, M3, M2, M1. The material being transported must be long enough, as all four sensors must be briefly and simultaneously activated. The sequential muting is correctly terminated if the third activated muting sensor is no longer activated.

Using the SafetyLab software, a muting version can be selected where the second muting sequence can already be initiated even if the first sequence has still not been completed (sequential muting with two objects). This version saves time and therefore also costs in the user's production environment.

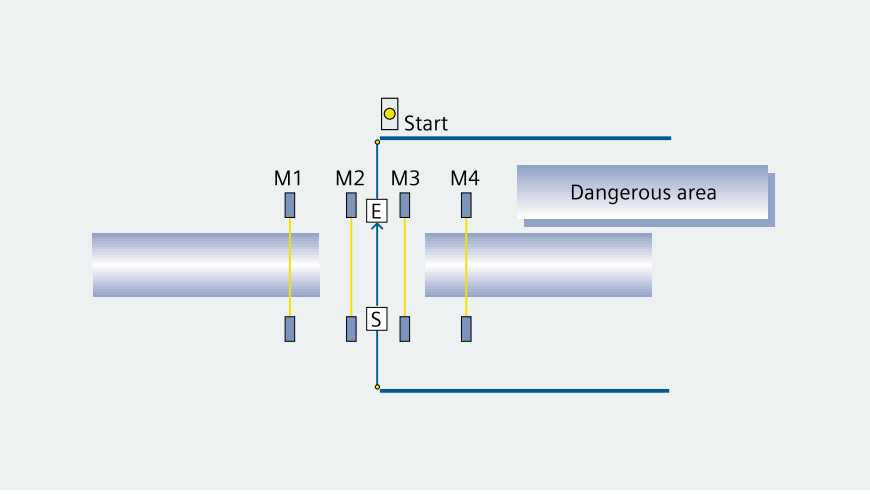


Fig. 6/34
4-sensor sequential muting

2-sensor parallel muting

Parallel muting is preferably used in those plants and systems where the dimensions of the material to be transported are not constant, or where space is somewhat restricted.
Two muting sensors can be used, whose beams cross behind the protective field in the hazardous area.

Parallel muting is initiated if the two M2 and M3 signals switch simultaneously without M1 and M4 either being activated or connected either beforehand or at the same time.
2-sensor parallel muting can be implemented at a low cost as only two muting sensors are required - and it is possible to move backwards and forwards within the muting distance.

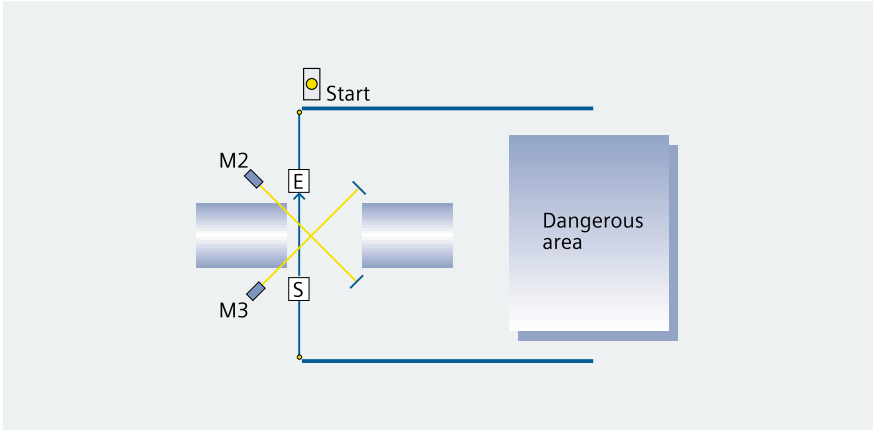


Fig. 6/35
2-sensor parallel muting

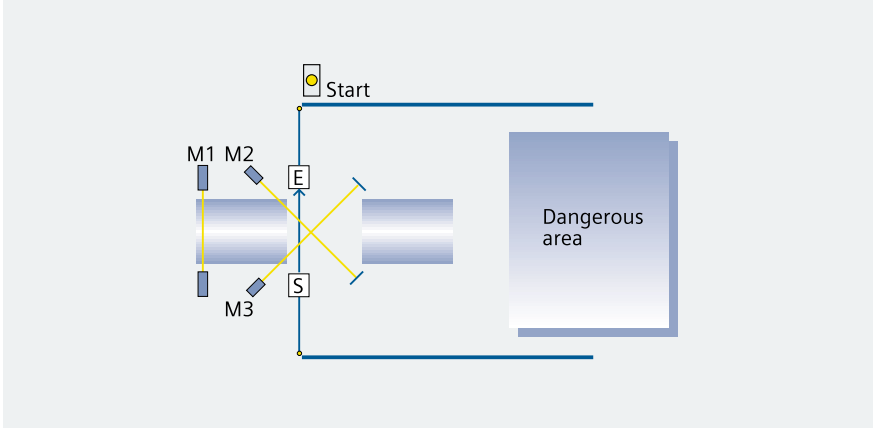


Fig. 6/36
3-sensor direction muting

3-sensor direction muting

3-sensor direction muting has a similar design to the 2-sensor parallel muting. Material can only be transported through the light curtain in one direction.
In order to initiate the muting function, to start, muting sensor M1 must be activated, followed by the two muting sensors M2 and M3. If the paths of muting sensors M2 and M3 are interrupted, it is no longer necessary to activate sensor M1.

4-sensor parallel muting

If the material to be transported is too small to be simultaneously protected by 4 sequentially arranged sensors, and if the space is extremely restricted to implement the light barrier crossover of the 2-sensor parallel muting, the 4-sensor parallel muting is the obvious choice, e.g. by using diffuse light sensors.

The 4-sensor parallel-muting corresponds, from the functional perspective, to two-sensor parallel muting. However, the activation signal is retrieved from two sensor pairs. Muting is initiated if sensors M2 with M3 or M1 with M4 are activated.

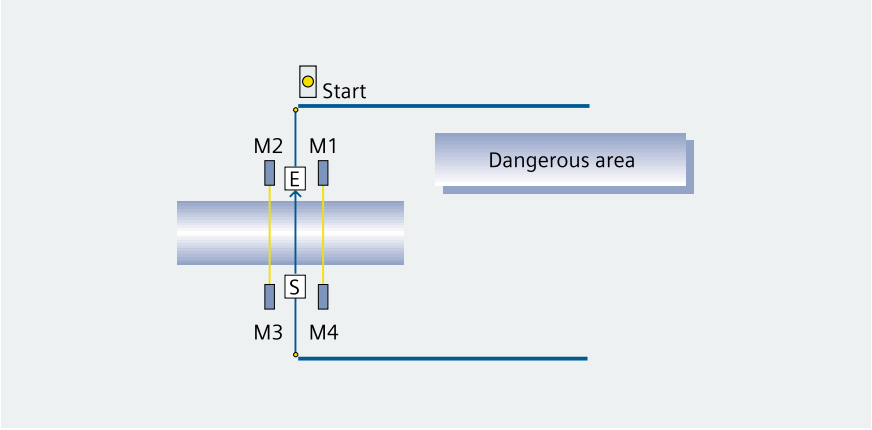


Fig. 6/37
4-sensor parallel muting

Muting restart

If, for example, the power supply fails while the material being transported is passing the muting sensors, the valid muting sequence is interrupted. If the power supply voltage returns, muting is not automatically continued, as the expected muting sequence is not available.

In order to remove the material being transported from the muting sensor area, the integrated removal mode can be implemented using the start button. The light curtain attempts to find a valid muting sequence from the muting sensors. If this is successful, the muting indicator lights stop flashing and go over to a steady light. If this is not successful, the start button must be held long enough until the muting distance is completely emptied.

Initiating machine motion using the light curtain (cycle control)

If it is necessary to intervene once or twice in the protective field of the light curtain (e.g. to insert or remove workpieces), the optional cycle control function should be selected. The SIGUARD 3RG78 44 light curtains, light grids and transceivers, cycle control function package and the appropriate SIGUARD 3RG78 47 evaluation units have this integrated functionality therefore permitting a faster and more productive machine operation.

6.3 SIGUARD light barriers

Relevant Standards

- EN 61 496-1, -2, IEC 61 496-1, -2 (requirements for contactless protective systems AOPDs)
- EN 999 (including calculating safety clearances)
- EN 954-1 (safety of machinery, safety-related parts of controls)

Fig. 6/38
SIGUARD 3RG78 2 light curtains

SIGUARD light barriers

- Are active opto-electronic protective devices (AOPD) and correspond to Category 2 (3RG78 23) or 4 (3RG78 24) acc. to Standard EN 61496-1, -2.
- Are EC-type tested
- Protect operating personnel at or close to hazardous machines
- Operate contactlessly (electro-sensitive)
- When compared to mechanical systems (e.g. contact mats), they are wear-free

Prerequisites - they must be:

- Correctly mounted and installed
- Correctly connected to the machine control

Information is provided in this section and is in the Instruction Manuals provided with the particular devices.

The devices are EC type tested (TÜV [German Technical Inspectorate] Product Service in conjunction with the Institute for Health and Safety at Work - BGIA).

Features

3RG78 23 light barriers for Category 2:

Ranges, 0 to 150 m
IP65 degree of protection
Connected through an M12 connector
Integrated heating for the optical system

3RG78 24 light barriers for Category 4:

Range, 0 to 60 m
IP65 degree of protection
Frequency modulated infrared light
Integrated pollution monitoring using an LED
Integrated heating for the optical system
High resistance to mechanical and chemical effects thanks to glass optics

3RG78 25 evaluation unit for Category 2:

Start and restart inhibit
Contactor checking
Electrically isolated safety outputs
Separate signaling outputs as pnp transistor outputs
Permanent cyclic testing
Operating function is not interrupted when testing
6 light barriers pairs can be connected in this series

Muting functions for light barriers, Categories 2 and 4 when using the 3RG78 47 evaluation units

Application examples

Light barriers in
safety category 2:

- Power-driven doors and gates
- Palletizers
- High-bay racking aisles
- Padernosters
- Elevating platforms
- Conveyor systems in dangerous areas

Light barriers in
Safety Category 4:

- Setting machines
- Packaging machines
- Warehouse equipment
- Plastic and rubber industries
- Woodworking machines

Protective/protective field heights

The protective heights and the number of light beams are defined by the requirements of the particular driven machine and the applicable accident prevention regulations, EN 999 or as a result of a risk analysis in accordance with EN 954-1. Usual protective heights according to EN 999 are listed in the Table in Fig. 6/39.

Application conditions

The protective function of the protective equipment is provided if the following prerequisites are fulfilled:

- It must be possible to electrically influence the control of the machine or plant.
- A switching command must immediately result in the machine or plant being shut down.
- The connected light barriers must be arranged so that it is only possible to enter the hazardous zone by completely covering at least one light bundle.
- When using and configuring safety-related equipment, the relevant legislation and regulatory specifications of the associated regulatory bodies and/or EU Directives for safety-related requirements on machines and plants apply.
- The light barriers must be arranged so that when at least one light bundle is interrupted, dangerous zone can only be accessed if the power equipment is no longer in a hazardous state. In this case, the prerequisite is that the required safety clearances acc. to EN 999 are maintained.
- All data in the Technical Description and Operating Instructions - especially the Sections Safety information" and "Commissioning" must always be carefully observed.
- Only qualified and trained personnel may mount, install, commission and service the devices.
- Only trained electrical technicians may carry-out electrical work.
- Only an authorized person responsible for safety issues may set and make changes to safety equipment (e.g. arranging the light beams, safety clearance etc.)
- Only the manufacturer or a person authorized by the manufacturer may carry-out repairs - especially opening the enclosure.
- If, as a result of their mounting location, light barriers alone do not offer adequate protection, then additional mechanical protective devices and equipment must be used.
- It may only be possible to access the hazardous zone through the protective field (it is not permissible that it is bypassed).
- The plant/system may not start as long personnel are in the hazardous zone.
- It is not permissible that the start button can be actuated from the dangerous area.

Safety clearance

There is a delay between the light barrier being interrupted and the machine coming to a standstill. Thus, the light barriers must be mounted so that when the dangerous area is entered, the dangerous location is not reached before the hazardous motion has been stopped.

According to EN 999, the safety clearance S between the protective device (light barrier) and the dangerous area is defined according to the following formula:

S = K x T + C

S Minimum safety clearance between the light barrier and dangerous area in mm

K Gripping or approach velocity in mm/s (constant)

T Delay time between the light being interrupted and the machine coming to a standstill in s, comprising:
t1: response time of the protective device in s
t2: overtravel time of the machine in s

C Safety constant (additional clearance in mm)

Caution:

Standards EN 294 and EN 999 are always decisive.

Number of light beams and their height above the reference plane acc. to EN 999

Number of light beams	No. of light beams above the reference plane in mm	Beam clearance S in mm
4	300, 600, 900, 1200	300
3	300, 700, 1100	400
2	400, 900	500
1	750	

Fig. 6/39
Height and safety clearances of the beams (EN 999 must be observed for all applications)

Clearance to reflective surfaces

Reflective surfaces, which are located within the transmitting and receiving cone of the light barriers, can cause reflections, which means it is possible that an obstruction is not identified. Thus, there must be a minimum clearance between reflective objects and the optical axis. This clearance is dependent on the angular aperture of the light sensor and the distance between the transmitter and receiver.

System design

SIGUARD light barriers are electro-sensitive protective devices, Category 2 or 4 acc. to EN 954-1. They are intended to secure dangerous areas at machines that could represent a risk of injury. When correctly used, they cause the machines to go into a non-hazardous condition, before personnel can be injured.

The complete safety system for safety Category 2 comprises an evaluation unit and the associated light barriers.

Up to 6 light barrier pairs can be connected in series to the 3RG78 25 evaluation unit.
The system for safety Category 4 comprises two light barriers.

Both of these systems operate together with the 3RG78 47, evaluation units in order to implement functions such as e.g. muting.

The evaluation units, in conjunction with the associated safety light barriers are implemented as self-monitoring components corresponding to EN 954-1, Category 2 or 4. They form the transition element between the light barriers and the machine control, and provide the required interfaces, including the power supply to operate the light barriers.

The safe functioning of the complete system is tested after powering-up (start test after “power-on”) and after a test request (when pressing a START button). In addition, a cyclic check is carried-out during operation to test the internal functions.

Fig. 6/40
SIGUARD 3RG78 25 evaluation unit

Start/restart inhibit

The start/restart inhibit function can be activated to prevent the plant or system immediately restarting after the trip when the protective field becoming free again. The receiver or the transceiver only go into the ON state after a start button has been pressed and released again. This start button must be pressed and received in a time window of between 0.1 and 4 seconds.

The use of the start/restart inhibit function is mandatory for securing access to dangerous areas. This is because only the access to the dangerous area is monitored - but not the area between the protective field and the potentially hazardous motion.

The command device to release the start/restart inhibit must be mounted so that

- the dangerous area is completely visible from the command device, and
- the command device cannot be actuated from the dangerous area

Contactor monitoring

The contactor monitoring is used to monitor downstream contactors, relays and valves. Switching elements with positively-driven feedback contacts are a prerequisite.

For dynamic contactor monitoring, a check is made as to whether, after the release, the feedback circuit has opened within 300 ms, and after shutdown, the OSSD re-closed again within 300 ms. If this is not the case, the enable circuit returns to the OFF state.

Muting functions

The protective effect can be blanked (suppressed) using additional sensor signals. For example, two transport materials in and out of the dangerous area. The protective field is temporarily blanked (suppressed), and after the material has been transported through the dangerous area, it is restored. During muting, it must be absolutely guaranteed that nobody can enter the dangerous area.

As a result of the number of connected sensors and the sequence of the muting signals, the devices automatically identify the "sequential muting" muting mode if inputs M1 to M4 are assigned and 2-sensor parallel muting, if signals M2 and M3 are assigned (refer to Fig. 6/41 and 6/42).

4-sensor sequential muting

If the material that is to be transported into the dangerous area always has the same dimensions, and there are no space restrictions, then sequential muting is preferably used. For sequential muting, four muting sensors are

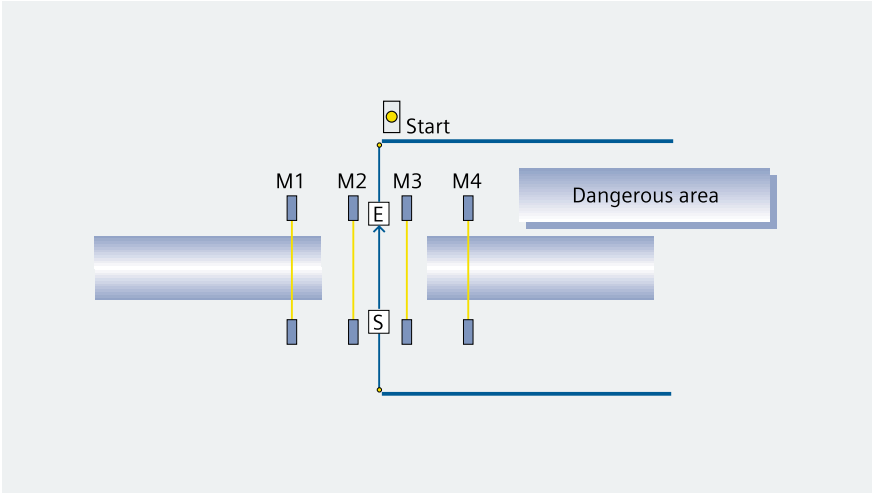


Fig. 6/41
Sensor sequential muting

connected that must be activated in a specified sequence in order to initiate the muting operation. They can be activated in the sequence M1, M2, M3, M4 as well as in the sequence M4, M3, M2, M1. The material being transported must be long enough, as all four sensors must be briefly and simultaneously activated. The sequential muting is correctly terminated if the third activated muting sensor is no longer activated.

2-sensor parallel muting

Parallel muting is preferably used in those plants and systems where the dimensions of the material being transported are not constant, or where space is restricted.
Two muting sensors can be used, whose beams cross behind the protective field in the hazardous zone.

Parallel muting is initiated if the two M2 and M3 signals simultaneously switch without M1 and M4 having been activated or connected - either beforehand or simultaneously.
2-sensor parallel muting can be implemented at a low cost as only two muting sensors are required - and it is possible to move backwards and forwards within the muting distance.

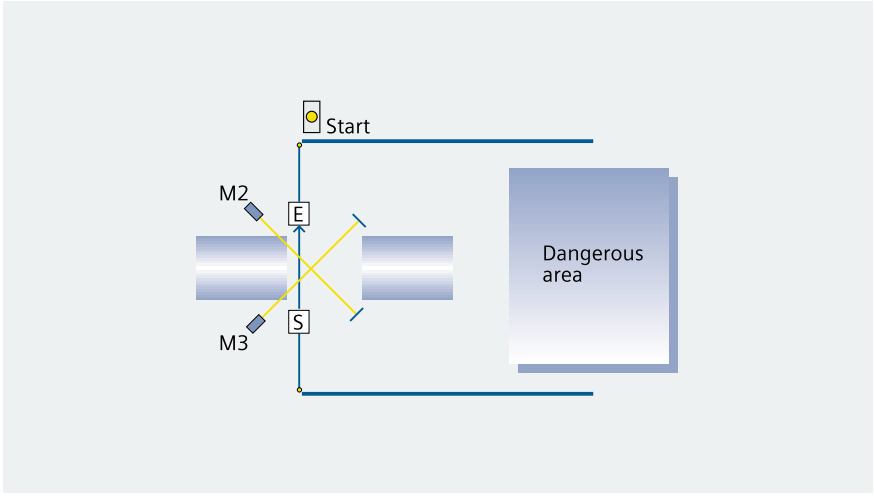


Fig. 6/42
Sensor parallel muting

6.4 SIGUARD switching strips

Overview

A switching strip is a mechanically actuated protective device that safely detects when contact is made to a person or a part of the body

Sender and receiver are optically and electrically coupled

An interruption of the light beam, influence of external light sources or failure of electronic components are safely detected

The sender power is automatically adapted to the length of the switching strip

Increased availability by compensating for the effects of aging, humidity and accumulated dirt

Shutdown and run-on travel are independent of the length of the profile

Features

- Neither gluing nor pre-assembling - required
- Neither technical know-how nor special tools required
- The system can be easily installed and mounted on-site
- Flexible planning up to shortly before actual installation and mounting
- Favorably-priced inventory
- Downtimes are minimized

Applications

Machines and plant construction
- Protective covers of machines
- Driverless transport systems
- Elevating tables
- Washing gantries
- Elevating platforms
- Automatic handling equipment

Doors and gates
- The forces occurring are limited when hitting an obstruction
- A suitable profile is selected
- The actuation angle for folding doors/gates is taken into account

Vehicle construction
- The forces occurring are limited when hitting an obstruction
- A suitable profile is selected
- Reliable, even at high speeds/ velocities
- Automatically closing doors
- Automatically closing windows

Product family/product groups

The German Trade Association [BG] has certified 3RG78 5 SIGUARD safety switch strips for Category 4 acc. to EN 954-1. The fail-safe functionality is achieved using the associated evaluation unit.

The system comprises
- An evaluation unit,
- A mounting strip,
- A sensor strip that is used to implement the shutdown function,
- An optical sender and receiver that monitors the switching strip

Design

Transmitter and receiver units are inserted into the hollow space in the rubber profile at each end. The rubber profile can be cut to the required length on-site and is resistant to, for example, ozone, oils, solvents, acids and fuels.

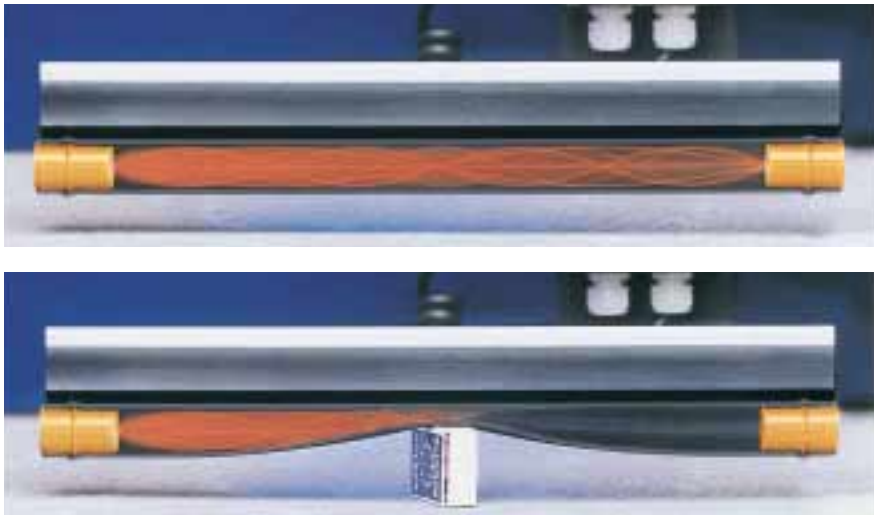


Fig. 6/43
Principle of operation of SIGUARD switching strips

Fail-safe controllers

SIMATIC Safety Integrated

7 Fail-safe controllers SIMATIC Safety Integrated

7.1 Overview

Increasing significance of safety systems in controllers

Accidents and damage resulting from faults and mistakes in plants or machines must, as far as possible, be avoided. This is the reason that legislation associated with safety at work and to protecting the environment is becoming increasingly more stringent. Today, different products and systems are often being used for safety-related functions (electro-mechanical) and standard tasks (classic PLC). When using conventional wiring and special safety-related buses, as the complexity of the automation task increases then the following also increase

- on one hand the wiring costs and
- on the other hand, the engineering costs.

Troubleshooting can take longer and the availability of the complete plant or system decreases.

This is the reason that machinery construction companies and plant operating companies are increasingly deciding to have the safety-related tasks handled by the automation components. This means that the protection of man, machines and the environment depends on automation systems functioning fault and error-free. This is the reason that the same high requirements are placed on safety-related electronic systems as safety-related electro-mechanical components. Both systematic as well as randomly occurring faults and errors must be controlled.

Standard automation and safety-related systems in a complete system

Up until now, generally, safety-related and standard tasks were implemented using different systems. The result - transitions between systems and twice the costs. With SIMATIC Safety Integrated, the standard automation and safety system are integrated to become one innovative total system. Existing SIMATIC know-how and knowledge about safety systems are sufficient to implement safety-related tasks with SIMATIC.

Well-proven safety technology using SIMATIC

Siemens has been established in the area of safety systems for more than 20 years now and since this time has created many innovative products and systems for fail-safe controllers. With its SIMATIC Safety Integrated, Siemens has done some pioneering work in many areas, e.g.

- The first fail-safe programmable logic controller – 1980
- The first fail-safe PROFIBUS-Master with PROFIsafe – 1999

Siemens is still actively working in domestic and international Associations in drawing-up Standards and Directives, such as e.g. ISO, NAM, DKE, IEC etc.

What does SIMATIC Safety Integrated mean for users?

By changing to intelligent controllers and distributed architectures, standard automation has become significantly more flexible and open. This therefore significantly increases the productivity of your machines and plants. Your automation will become even more efficient if safety technology consequentially follows this trend and allows itself to be seamlessly integrated into the standard automation environment. This means the following:

- Existing STEP7 know-how can be used - from engineering up to service & maintenance.
- PROFIBUS network structures can be used, also for safety-relevant communications.
- Existing components and infrastructure are used, as far as possible, also for safety systems.

7.2 Features

Complete integrated system

By integrating safety-related functions in the automation environment of Totally Integrated Automation, standard and safety automation grow together to form a complete seamless system.

SIMATIC Safety Integrated encompasses the fail-safe SIMATIC controllers as well as the I/O and engineering within the product range of Safety Integrated. When a fault or error occurs, the control or a sub-process can be brought into a safety-related state where it is also kept. These fail-safe controllers are based on well-proven standard SIMATIC PLCs.

PROFIBUS was extended for safety-related communications by the non-proprietary PROFIsafe profile. This means that safety-related and standard communications only require just one standard PROFIBUS cable.

The same engineering and programming tools (STEP® 7) are used to engineer the standard and safety functions of fail-safe SIMATIC controllers.

This means that in a SIMATIC controllers the safety system is seamlessly integrated in the standard automation.This also makes it easier for operating personnel to handle the complete plant or system. Not only this - engineering and training costs are also reduced. Another advantage is that extensive diagnostics of safety-related signals can be directly read-out using standard panels and HMI devices.

Thanks to the fine resolution of the fail-safe I/O design, safety technology only has to be used where it is actually required. Safety components can be simply combined with standard components; Safety-related and non-safety-related programs coexist in more than one controller as well on a common bus system.

Fail-safe fieldbus devices from other manufacturers can be simply connected-up using PROFIBUS and the non-proprietary PROFIsafe profile.

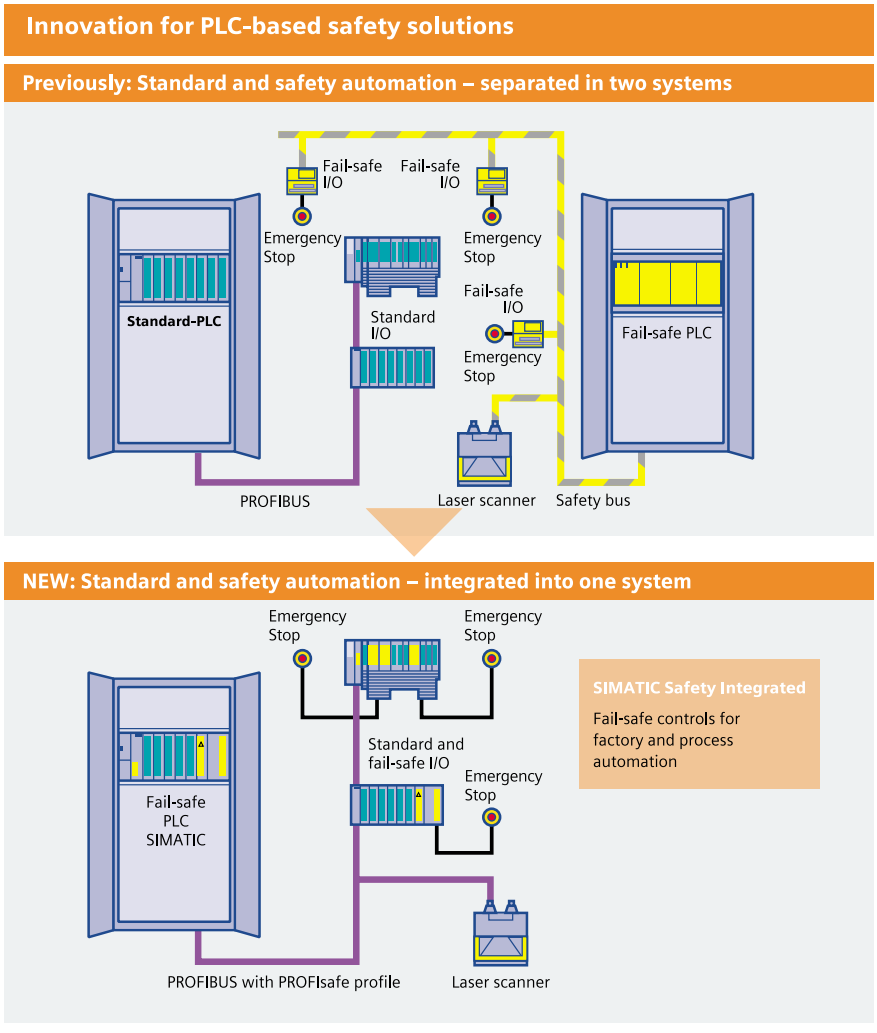


Fig. 7/1
Innovation with PLC-based safety solutions

Comparison between the previous and new solutions

Previous safety-related PLC solutions required two different controllers and, for distributed solutions, also a fail-safe bus. Standard and fail-safe field devices must be separately configured. Additional HMI devices had to be installed in order to read-out safety-related signals.

The new solution with SIMATIC Safety Integrated that has already proven itself worldwide, only requires one controller with standard engineering and the standard PROFIBUS running the PROFIsafe profile. Even when it comes to the I/O modules, the HMI devices and sensors, standard and safety-related automation are growing together. When required, these systems can also be separately configured as before. So in this case, the advantages associated with the standard engineering tools and integration without new interfaces are still kept.

The advantages - an overview

With SIMATIC Safety Integrated, the following benefit:

- Machinery and plant construction companies e.g. thanks to lower hardware costs.
- Plant operating companies, e.g. as a result of the higher plant availability and high degree of flexibility.

Advantages are obtained both when comparing to proprietary safety-related PLCs as well as also to conventional safety systems.

Advantages of SIMATIC Safety Integrated	With respect to proprietary safety PLC	With respect to conventional safety technology
Lower engineering costs	• Only one engineering tool to generate standard and safety-related programs	• A solution can be simply duplicated by copying the safety-related program
	• Common data management for standard and safety-related programs	• Higher degree of flexibility by programming instead of wiring safety-related logic
	• The standard and the safety-related components and communications are configured in a standard fashion	
Simpler and faster commissioning	• Only one PROFIBUS cable is required for standard and-safety-related communications	• The safety logic can be simply modified by making the appropriate program changes with automatic documentation update
	• Same operator philosophy for standard and safety-relevant automation	• Seamless, integrated diagnostics from the sensor through the control to the HMI system
	• All system components from a single source	
More efficient operating phase	• Shorter downtimes as a result of seamless, integrated diagnostics from the sensor through the control up to the HMI system	
	• Remote diagnostics via teleservice	
	• Simpler spare parts stocking by reducing the number of types and parts	

Table:
Advantages of SIMATIC Safety Integrated

7.3 Applications

Using SIMATIC Safety Integrated

The range of fail-safe SIMATIC controllers encompasses safety solutions that are widely scalable - both for production as well as process automation.

- Safety and the protection of people and machines have topmost priority in production automation.
- In process automation, it is especially important that the system availability is maintained. At the same time, protection must be provided against unexpected process hazards and the risk of an accident or incident must be appropriately reduced.

The use of SIMATIC Safety Integrated allows all of the important Standards to be fulfilled to protect man, machines and the environment.

At home in all industry sectors

The main applications of SIMATIC Safety Integrated are, for example, as follows:

- **Factory automation**
  Automobile industry, conveyor systems, presses, all types of processing machinery, machine tools, etc. passenger transport, e.g. cable railways, elevating platforms, amusement rides, etc.

- **Process automation**
  Oil & gas, chemical, pharmaceutical, petrochemical, refineries,
  Typical applications include:
  Furnace controls, emergency shutdown (ESD), process shutdown (PSD) and fire & gas (F&G)

The seamless, integrated characteristics of SIMATIC Safety Integrated are especially important for composite applications from the main sectors in the hybrid industry - among others, for communications and shared I/O.

Certified according to all important Standards

Fail-safe SIMATIC controllers fulfill all important Standards and regulations and are certified by the TÜV [German Technical Inspectorate].

Factory automation
- IEC 61508 (up to SIL 3)
- EN 954 (up to Category 4)
- NFPA 79-2002 and NFPA 85
- UL 1998, UL 508 and UL 991

Certificate under:
http://www4.ad.siemens.de/WW/view/de/17396090

Process automation
- IEC 61508 (up to SIL 3) and IEC 61511
- EN 954 (up to Category 4)
- NFPA 79-2002
- ANSI/ISA S84, API 14C, BLRBAC

Certificate under:
http://www4.ad.siemens.de/WW/view/de/17968956

PROFIBUS with PROFIsafe is a part of SIMATIC Safety Integrated and is certified according to IEC 61508 (up to SIL 3), EN 954 (up to Category 4), NFPA 79-2002, NFPA 85 - therefore fulfilling the highest requirements for the production and process industries. Not only this, PROFIBUS DP expanded by the data transmission version PA (IEC 1158-2), means that distributed automation can be seamlessly implemented in an integrated fashion down to the field level. The I/O modules fulfill SIL 3 (acc. to IEC 61508) and Category 4 (acc. to EN 954) and are therefore UL-listed and also certified by the TÜV (German Technical Inspectorate).

7.4 Product group/ product family

SIMATIC Safety Integrated family

SIMATIC Safety Integrated offers a scalable range of fail-safe controllers for production and process automation. A common set of I/O and communication platform are used.

ET 200S, ET 200M and ET 200eco are used as fail-safe I/O. The I/O are connected via PROFIBUS DP, the communications via the PROFIsafe profile.

SIMATIC Safety Integrated

Range for factory automation	**Range for process automation**
	
Controller	
SIMATIC ET 200S F-CPU, S7-300F, S7-400F Scalable portfolio of fail-safe controllers for all performance areas in factory automation.	**SIMATIC S7-400FH** Safety, fault tolerant controller for process automation
Engineering	
STEP 7 languages LAD and FBD are used to program the system together with TÜV-certified functions from **S7 Distributed Safety**. (TÜV= German Technical Inspectorate)	The safety functions are configured/engineered with **Continuous Function Chart** (CFC) or **SIMATIC Safety Matrix** (cause & effect matrix) using TÜV-certified function blocks from **S7 F systems**.
I/O	
The fail-safe I/O can be used in all industries and support safety functions, such as e.g. signal test (short-circuit, wire breakage) as well as discrepancy monitoring.	
ET 200eco The distributed block-type I/O with a high IP65/67 degree of protection with digital input module for cabinetless configurations. **ET 200M** The modular I/O for applications for a high number channels with digital I/O modules as well as analog input modules. **ET 200S** The finely modular I/O with digital input and output modules as well as fail-safe motor starters and frequency converters.	

Fig. 7/2
SIMATIC Safety Integrated for factory and process automation

Controllers for factory automation

The following F-CPUs are available 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 standard CPUs - their hardware and operating systems have been expanded by various protective mechanisms to be able to execute safety-related programs.

The safety-related program is completely programmed using STEP 7 in the standard languages LAD and FBD.
In addition to STEP 7, the "S7 Distributed Safety" option package is required. Using pre-configured, certified blocks, "S7 Distributed Safety" provides support when parameterizing the fail-safe I/O and when programming.

When executing non-safety-related programs there are absolutely no restrictions regarding the programming language.

Fig. 7/3
CPUs for factory automation

Controllers for process automation

The CPUs 414H and CPU 417H with safety-related functions from 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 system". Fail-safe applications up to SIL 3 can be handled using just one CPU. "S7 F systems" support the configuration of safety-related I/O and logic programming.

Two CPUs can be used to increase the level of system availability to fulfill requirements relating to fail-safety and fault tolerance. It is also extremely simple to integrate into the SIMATIC PCS 7 process control system. This results in the following advantages:

- One engineering system for standard and fail-safe applications.
- The safety-related system is homogeneously integrated into the automation system (AS) of SIMATIC PCS 7.
- User-friendly visualization of the process values integrated in the operator station (OS) of SIMATIC PCS 7.
- Safety-related fault messages are automatically incorporated in the process visualization, with the same time stamp.
- No complex coupling between the Distributed Control System (DCS) and SIMATIC Safety Integrated, e.g. via Modbus.

Safety-related functions are configured in the Continuous Function Chart (CFC). Certified function blocks provide support when engineering/configuring therefore saving both time and money.

In order to simplify configuring safety-related functions even further, a configuring tool is now available.
This tool allows causes and effects in the process to be quickly configured and that error-free.
The SIMATIC Safety Matrix is an engineering tool for processes that require safety-related responses to defined states and which can be simply configured using a Cause & Effects matrix.

Fig. 7/4
S7-400FH CPUs for process automation

Fail-safe I/O

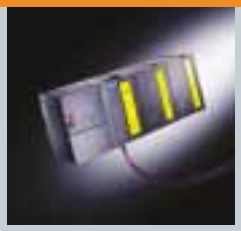
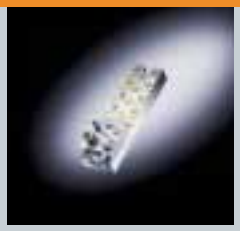
ET 200S, ET 200M and ET 200eco are available as fail-safe I/O to expand fail-safe CPUs.

The fail-safe ET 200M, ET 200S and ET 200eco fulfill SIL 3 (acc. to IEC 61508) and Category 4 (acc. to EN 954) and are both UL-listed and certified by the German Technical Inspectorate. The I/O are connected through PROFIBUS DP, communications use the PROFIsafe profile.

The fail-safe I/O can troubleshoot both internal and external faults, has an internal redundant structure and executes its own self-test routines (e.g. short-circuit, wire breakage). Fail-safe and standard modules can also be operated together in an ET 200S or ET 200M. Depending on the system structure, in this case, up to SIL 3 or Category 4 can be achieved. The main features of the available fail-safe I/O are shown in the following table.

Requirement	Structure	Safety class Safety Integrated Level
Fail-safe	Basic structure with one CPU	Up to SIL 3
Fail-safe and fault-tolerant	Redundant structure with two CPUs	Up to SIL 3

Table:
Safety classes for the various structures

	I/O ET 200S	ET 200M	ET 200eco*)
			
Features	Finely modular I/O with up to 8 channels per module in degree of protection IP20	Modular S7-300 I/O for applications with a high Number of channels with up to 24 channels per module in degree of protection IP20	Digital block I/O in a high IP65/67 degree of protection
Digital inputs	To connect digital sensors/encoders • 4/8 F-DI 24V DC	To connect digital sensors/encoders • 24 F-DI 24V DC • 8 F-DI NAMUR	To connect digital sensors/encoders • 4/8 F-DI 24V DC
Digital outputs	To connect digital actuators/loads • 4 F-DO 24V DC/2A	To connect digital actuators/loads • 10 F-DO 24V DC/2A • 8 F-DO 24V DC/2A (PM switch.)	
Analog inputs		To connect analog sensors/encoders • 6 F-AI 4-20 mA / 13 bit	
Power modules	To monitor and protect the load and encoder power supply voltages • PM-D F 24 V DC • PM-E F PM • PM-E F PP		
Motor starters	The fail-safe motor starters have, in addition to a circuit-breaker/ contactor combination, also a safety-related electronic evaluation circuit for fault detection. If, when an Emergency Stop situation occurs, the switching contactor fails, the evaluation electronics detects a fault and opens the circuit-breaker in the motor starter in a safety-related fashion.		
Frequency converters	The fail-safe frequency converters permit the following safety functions to be implemented for variable-speed induction motors: • Safe standstill, • Safe braking ramp, • Safely reduced speed.		

7.5 Engineering

Programming in factory automation

No additional programming know-how is required when using the "S7 Distributed Safety" software package. This is because the safety-related programs for the fail-safe CPUs are programmed using the usual STEP7 standard languages, ladder diagram (LAD) and function diagram (FBD). Using a special input when compiling, it is ensured that the program, generated by the user, is executed in a safety-related fashion.

The F library with pre-configured blocks for safety-related functions that have been certified by the Germany Technical Inspectorate is an additional component of this software package. This library includes function blocks such as Emergency Stop, protective door, 2-hand operator control, muting for light curtains etc.

Further, "S7 Distributed Safety" supports the comparison of safety-related programs. Finally, the acceptance of the plant or system is simplified as a result of the generated program printout.

An option package with certified furnace blocks is available for furnace applications.

Configuring and engineering in the process automation

"S7 F systems" is used to engineer the hardware and configure the safety-related process application according to IEC 61511 and expands the S7-400FH controller by safety-related functions. It makes it easier to generate the safety-related program by providing an F library with pre-configured blocks, certified by the German Technical Inspectorate according to SIL 3 IEC 61508. Further, it simplifies the documentation of the safety-related program, e.g. by managing and administrating the appropriate signatures.

The fail-safe safety-related program can either be configured using CFC or the Safety Matrix.

CFC is especially suitable for dynamic processes - e.g. in the chemical and petrochemical industries (hydrocrackers). Using CFC, certified blocks from the F library of S7 F systems or the optional furnace package can be called-up and interconnected. The optional furnace package includes an F library with blocks for industrial gas-fired and oil-fired furnaces. The blocks have been certified by the German Technical Inspectorate acc. to EN 61508 SIL 3 and TRD Standard 411 and 412 for thermo and steam boilers.

The Safety Matrix is an innovative engineering tool for processes that require safety-related responses to defined states and events and can be simply engineered using the Cause & Effects matrix. The Cause & Effects analysis is

Fig. 7/5
Example of the SIMATIC Safety Matrix for S7-400FH

part of the risk analysis of a plant or system. The specification of the safety-related program is simultaneously the input parameters for the Safety Matrix. After being entered, it derives the test specification of the plant or system. This means that potential fault sources can be reduced to a minimum.

This is associated with the following advantages:

- The safety-related CFC project is automatically generated.
- Documentation after safety checks and tests is automatically generated.
- The visualization is automatically generated and the Safety Matrix at the SIMATIC PCS 7 operator station is visualized in a user-friendly way.
- Project versions are automatically managed.
- The safety function can be easily changed and the specification can be simply adapted in the test mode - including bypass, reset and override functions.

7.6 Structure

Implementing the safety functions

The safety-related functions are executed by the safety-related program in the CPU in conjunction with fail-safe I/O modules. In so doing, standard I/O and fail-safe I/O can be combined. For the ET 200M, electrical isolation for SIL 3 and Category 4 applications is realized using an isolating module and for the ET 200S, by configuring load circuits with power modules (PMs).

Both safety-related as well as standard communications between the central module and I/O (safety-related or standard) are realized along PROFIBUS DP with the PROFIsafe profile.

Principle of the safety-related function for SIMATIC Safety Integrated

The principle of operation is time redundancy and diversity instead of structural redundancy. The safety-related input signals are processed diversely and redundantly in time.

If Fig. 7/6, the signals A, B are processed in parallel with an AND logic operation and negated with an OR logic operation. Output signals C and D are then compared with one another. If D is not equal to the complement of C, the CPU goes into the stop state. If the comparison is successful, then the output is set.

The CPU checks that the control is operating correctly by carrying-out regular self-tests, command tests as well as a program run check.

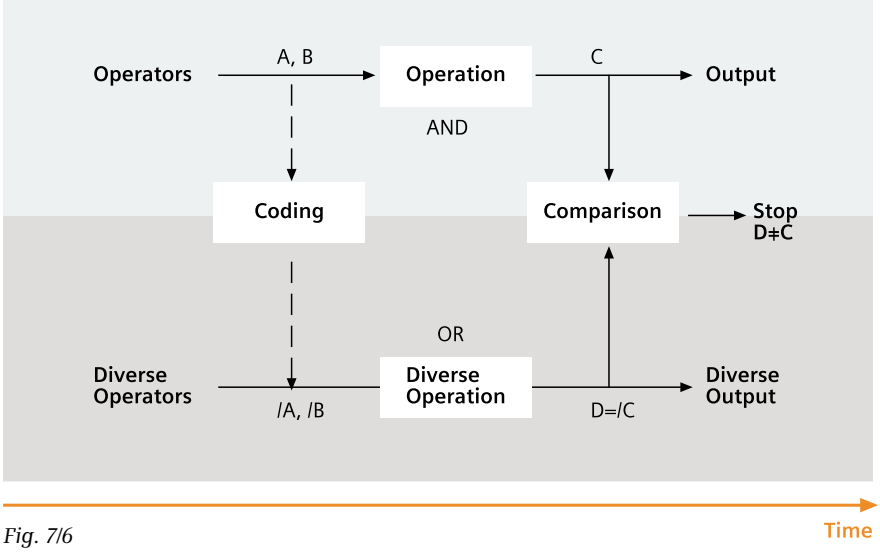


Fig. 7/6
Safety-related data transfer using time redundancy and diversity for S7 F systems

7.7 Functions

Functions of the fail-safe controller

The fail-safe CPUs have the following properties:

- Comprehensive self-tests and self-diagnostics in order to check the fail-safe CPU state.
- In addition to the fail-safe program, a standard program can also run on a CPU (coexistence) that is not subject to any restrictions.
- Fail-safe communications between CPUs.
- The same diagnostics and signaling functions as a standard SIMATIC S7-CPU.

Functions of the fail-safe I/O

The Fail-safe I/O can diagnose internal and external faults, have an internal redundant structure and execute their own self-test routines (e.g. short-circuit, wire breakage). Fail-safe shutdown is realized without any additional safety relay. Further, the discrepancy time, specified in the form of the parameterization, is autonomously monitored by the I/O module.

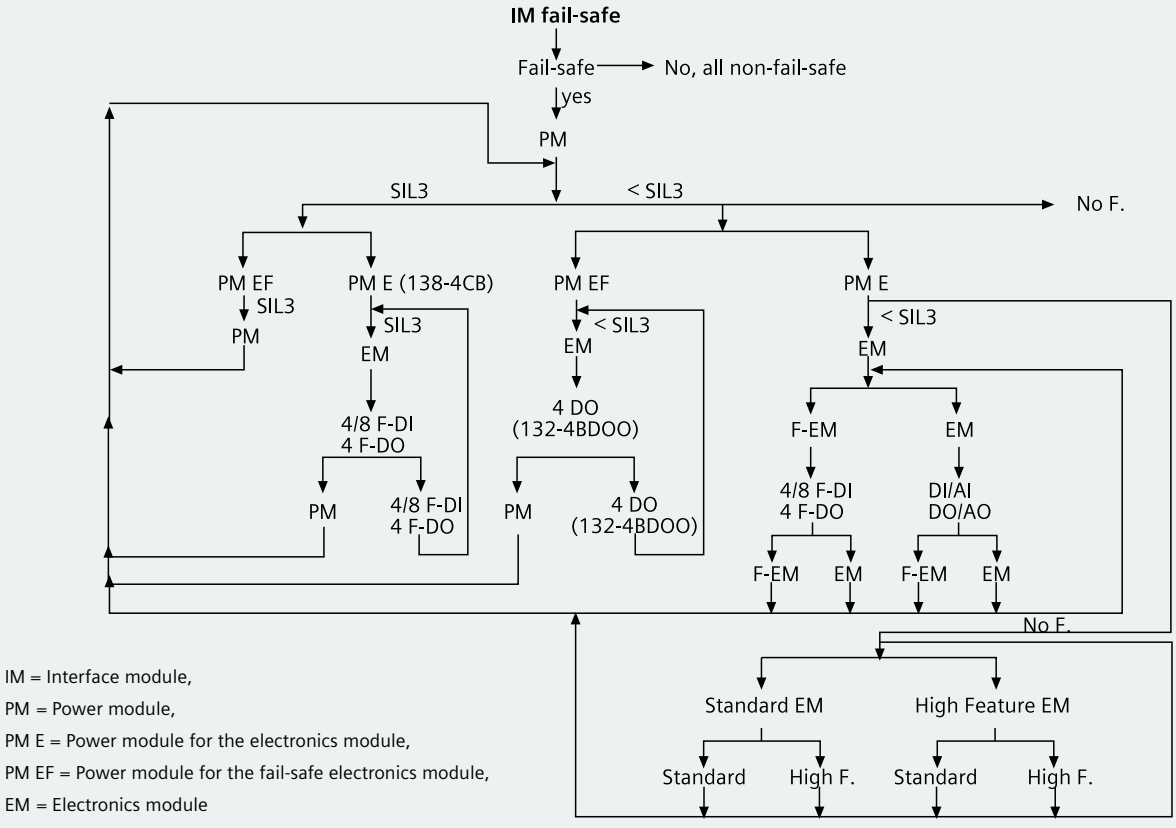


Fig. 7/7
Structure of the ET 200S configurator

Fail-safe and standard modules can also be combined in an ET 200S or ET 200M. Depending on the system structure, up to SIL 3 or Category 4 can be achieved.

Configurator for ET 200S

In order to correctly configure an ET 200S Station, an ET 200S configurator has been available from the electronic CA01 Catalog since April 2003. This provides support when combining modules according to the following specification. The configuration of I/O modules and motor starters with and without safety-related technology is analyzed.

Starting from the IM fail-safe header module, a decision must be made as to which safety Category the load circuits with the modules should fulfill. The modules can then be configured. The function of the configurator is explained in the following using 2 examples.

1. Standard configuration with PM-E, F-DI and F-DO modules to achieve Category 4 and SIL 3.

A load circuit with fail-safe F-DI and F-DO modules fulfills the highest safety category, Category 4 and SIL 3. Power is fed-in using a standard PM-E power module. If additional standard modules are configured in a load circuit with F modules, then as a maximum, safety Category 3 or SIL 2 can be achieved.

2. Favorably-priced configuration with PM-E F and downstream standard 4-DO modules to achieve Category 3 or SIL 2.

A load circuit with PM-E F modules and downstream standard 2-DO modules fulfills, as a maximum, safety Category 3 or SIL 2. It is even possible to shut down according to SIL 3 using a relay output integrated in the PM-E F.

7.8 Examples

Typical configuration examples

Two configuration examples for SIMATIC Safety Integrated are listed below – one with the focus on factory automation and one from the process automation environment

Both the standard communications as well as also the safety-related communications are realized along the same standard PROFIBUS cable using the non-proprietary PROFIsafe bus profile specifically developed for safety systems.

Factory automation

Controllers

- Fail-safe CPUs for ET 200S, S7-300, S7-400

I/O

- SIMATIC ET 200M with a larger number of I/O modules, finely modular SIMATIC ET 200S (IP20) and SIMATIC ET 200eco (IP65/67)
- NAMUR modules of SIMATIC ET 200S for hazardous zones
- Depending on the requirement, can be expanded by standard and fail-safe modules
- Fail-safe modules: The internal structure is completely redundant and diverse
- Extensive diagnostic functions to detect internal and external faults
- Safety functions are included in the fail-safe signal modules
- LS4 laser scanner with direct connection to PROFIsafe
- Motor starters for ET 200S
- Frequency converters for ET 200S

Communications

- Standard PROFIBUS DP with PROFIsafe profile

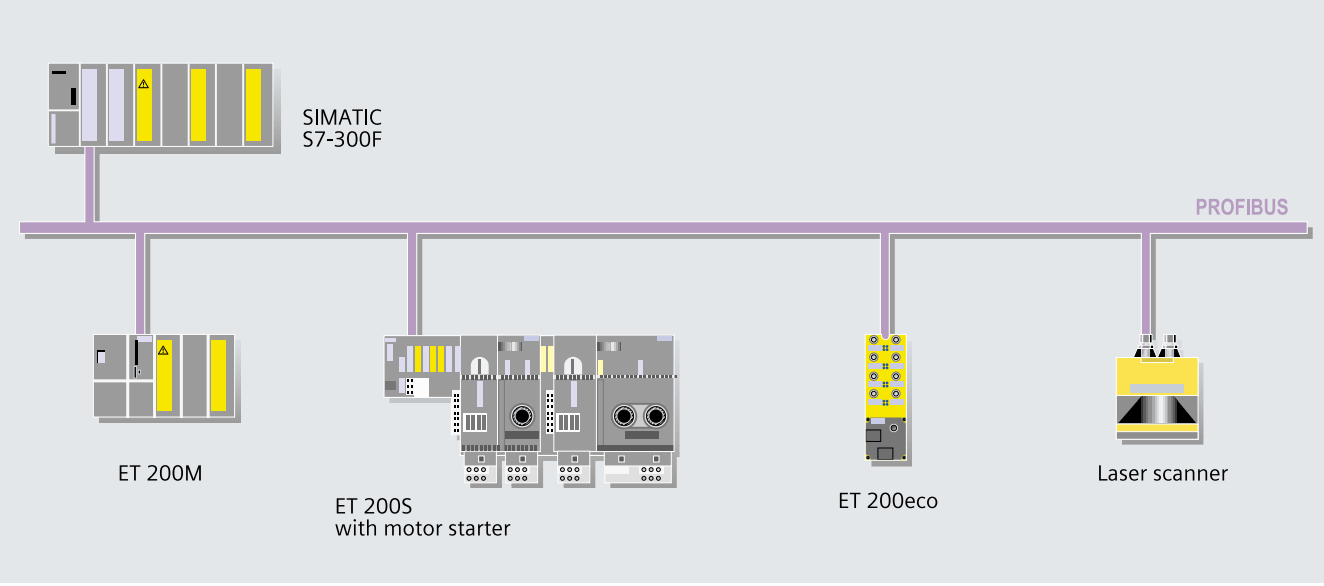


Fig. 7/8
Configuration example, factory automation with a simple structure

Process automation

Controllers

- Safety-related and fault-tolerant SIMATIC S7-400FH – this can be configured just like the Standard S7-400.
- Highest safety level, SIL 3 can be fulfilled using just one controller.
- Standard and safety-related functions can be optionally configured in a controller, either together or separately.
- High degree of availability is possible by redundantly configuring a second controller.
- Can be completely integrated into SIMATIC PCS 7, but can also be connected to any DCS (Distributed Control System).

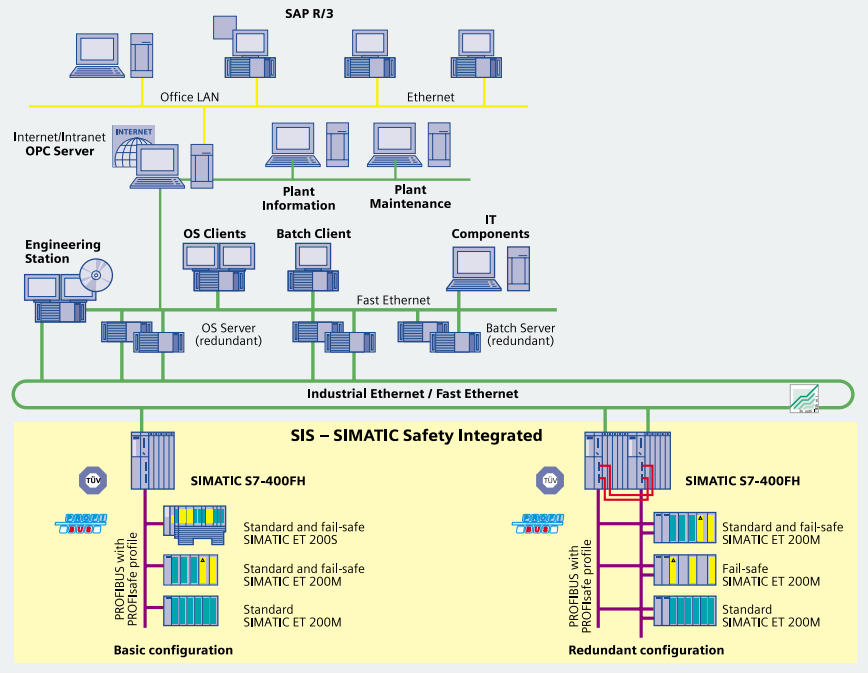


Fig. 7/9
Configuration example, process automation

I/O

- SIMATIC ET 200M with a high number of I/O modules and finely modular SIMATIC ET 200S.
- NAMUR module of SIMATIC ET 200M for hazardous zones.
- Depending on the requirement can be expanded by standard and fail-safe modules.
- Fail-safe modules: The internal structure is completely redundant and diverse.
- Extensive diagnostic functions to detect internal and external faults.
- Safety functions are included in fail-safe signal boards.

Communications

- Standard PROFIBUS DP with PROFIsafe profile

With SIMATIC Safety Integrated, we are offering a first class safety instrumented system solution (SIS) based on innovative and well-proven products, systems and standards. You can easily connect SIMATIC Safety Integrated to any production control system - today, it is already integrated in SIMATIC PCS 7.

Programming screen, factory automation

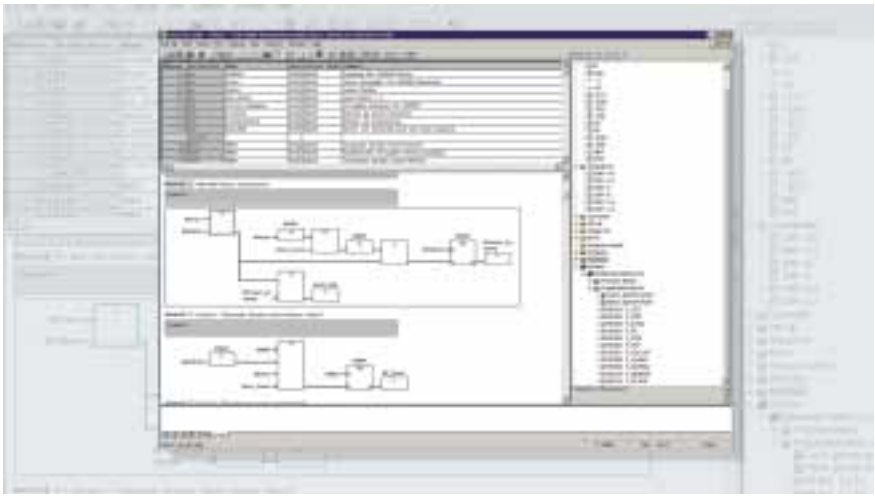


Fig. 7/10
Programming with a function chart

Programming example - factory automation

The Emergency Stop example in Fig. 7/11 shows how stop functions can be immediately (Category 0) implemented or with a delay (Category 1). The acknowledge button is used as start input.

Programming time and costs are minimized thanks to the distributed fault evaluation for ET 200 modules. For instance, the discrepancy time is configured when configuring the hardware. This is evaluated in the module and only a signal appears in the PLC program. The signal determined from the system can therefore be extremely easily processed in the program and complex calculations are eliminated.

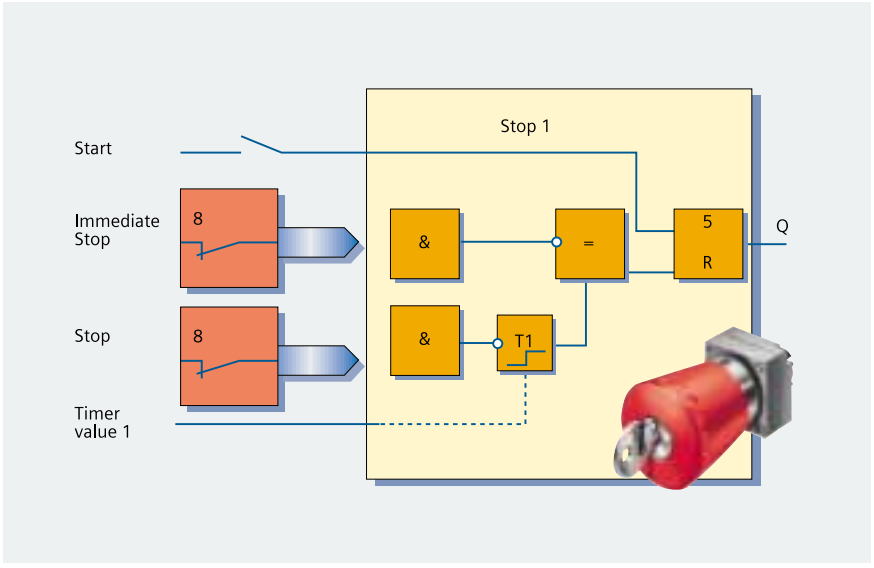


Fig. 7/11
Programming example for "Emergency Stop"

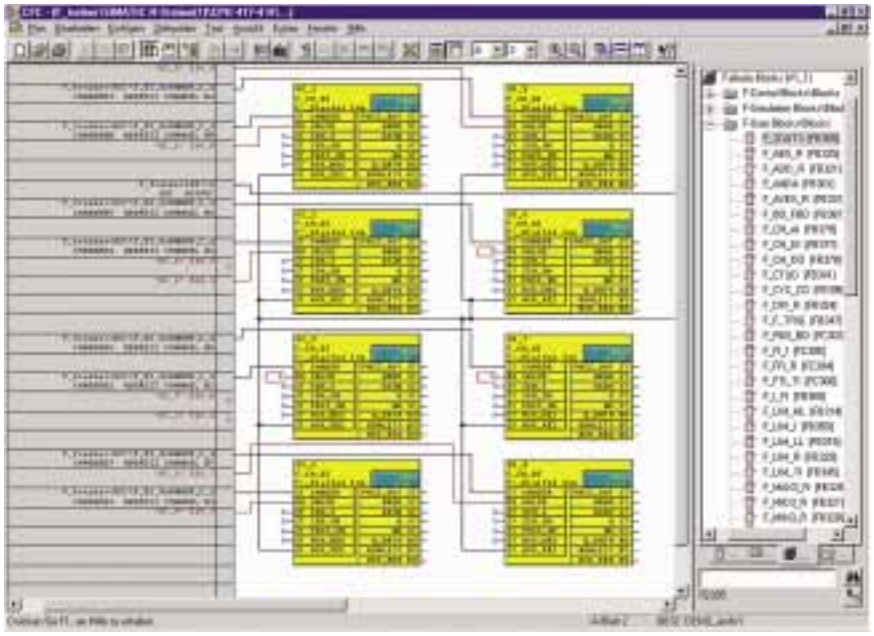


Fig. 7/12

Graphically configuring the S7-400 FH using the continuous function chart (CFC) engineering tool

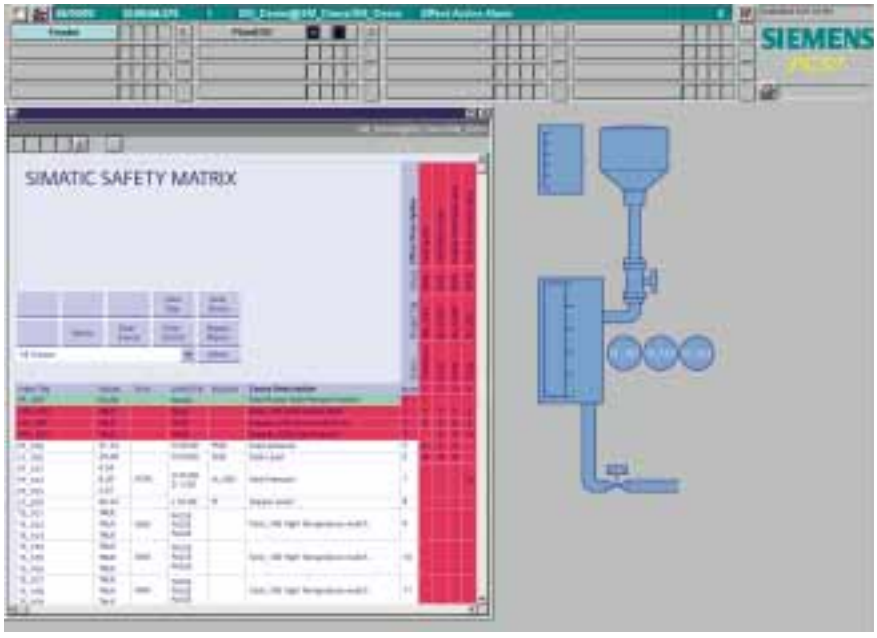


Fig. 7/13

From a Cause & Effect table, the Safety Matrix generates a program that can be run

Configuring screen process automation

CFC allows safety-related functions to be graphically configured. Certified functions blocks can be directly used from the library.

As an alternative, the SIMATIC Safety Matrix engineering tool can be used that automatically compiles cause & effect links in the CFC and can be easily integrated and visualized in PCS 7.

7.9 Technical data

CPU	IM 151-7 F-CPU	CPU 315F-2 DP	CPU 317F-2 DP	CPU 416F-2
				
Packaging design	ET 200S	S7-300 with central and/or distributed fail-safe I/O		S7-400 with distributed fail-safe I/O
Applications	• Distributed applications in the lower performance range • Stand alone systems	• Medium performance range	• Medium up to upper performance range	• Upper performance range
RAM	96 kB	192 kB	512 kB	1.4 MB data 1.4 MB code
Load memory (can be inserted)	64 kB - 8 MB	64 kB - 8 MB	64 kB - 8 MB	256 kb integrated 64 kB - 64 MB
Flags	2 kbit	16 kbit	64 kbit	128 kbit
FB/FC/DB	512/512/511	2048/2048/1023	2048/2048/2047	2048/2048/4095
Fail-safe I/O	Up to 28	Up to 320	> 500	> 1000
Peripheral address area I/O	244 B/244 B	2 kB/2 kB	8 kB/8 kB	16 kB/16 kB
Process image I/O	128 B/128 B	384 B/384 B	1 kB/1 kB	16 kB/16 kB
Interfaces	MPI/DP	MPI and DP	MPI/DP and DP	MPI/DP and DP
PFD*)	1.59E-05	2.38E-05	4.76E-05	4.76E-05
PFH*)	3.62E-10	5.42E-10	1.09E-09	1.09E-09
Dimensions	60 x 120 x 75	40 x 125 x 130	80 x 125 x 130	25 x 290 x 219
Main Order No.	6ES7 151-7FA..	6ES7 315-6FF..	6ES7 317-6FF..	6ES7 416-2FK..

*) *PFD = Average probability of failure on demand*

*) *PFH = Probability of a dangerous failure per hour*

Option package	S7 Distributed Safety	Furnace
Library	Certified blocks, e,g, Emergency Stop, 2-hand-control, muting, door monitoring	Certified furnace blocks
Prerequisite	STEP 7	S7 Distributed Safety
Engineering-Package	1 license is required per engineering station	
Runtime package		1 license is required per CPU
Main Order No.	6ES7 833-1FC..	9AL3 100-1AD..

CPUs process automation

CPU	CPU 414-4H	CPU 417-4H
		
RAM (integrated)	768 kB data 768 kB code	10 MB data 10 MB code
Load memory (integrated, RAM)	256 kB	
Load memory (can be expanded, RAM/FEPROM)	up to 64 MB	
Flags	64 kbit	
FB/FC/DB	2048/2048/4095	6144/6144/8192
I/O address area I/O	8 kB/8 kB	16 kB/16 kB
Process image I/O	8 kB/8 kB	16 kB/16 kB
Interfaces	MPI/DP and DP	
PFD*)	1.24 E-04	still not available
PFH*)	1.42 E-09	still not available
Dimensions	25 x 290 x 219	
Main Order No.	6ES7414-4H...	6ES7417-4H...

Option package	S7 F systems	Furnace
Library	Approx. 50 certified basic function blocks blocks	Certified furnace
Prerequisites	• STEP 7 • CFC • S7-SCL	• S7 F systems
Engineering package	1 license is required per engineering station	
Runtime package	1 license is required for each CPU	
Main Order No.	6ES7 833-1CC..	9AL3 100-1AA..

Common/shared I/O

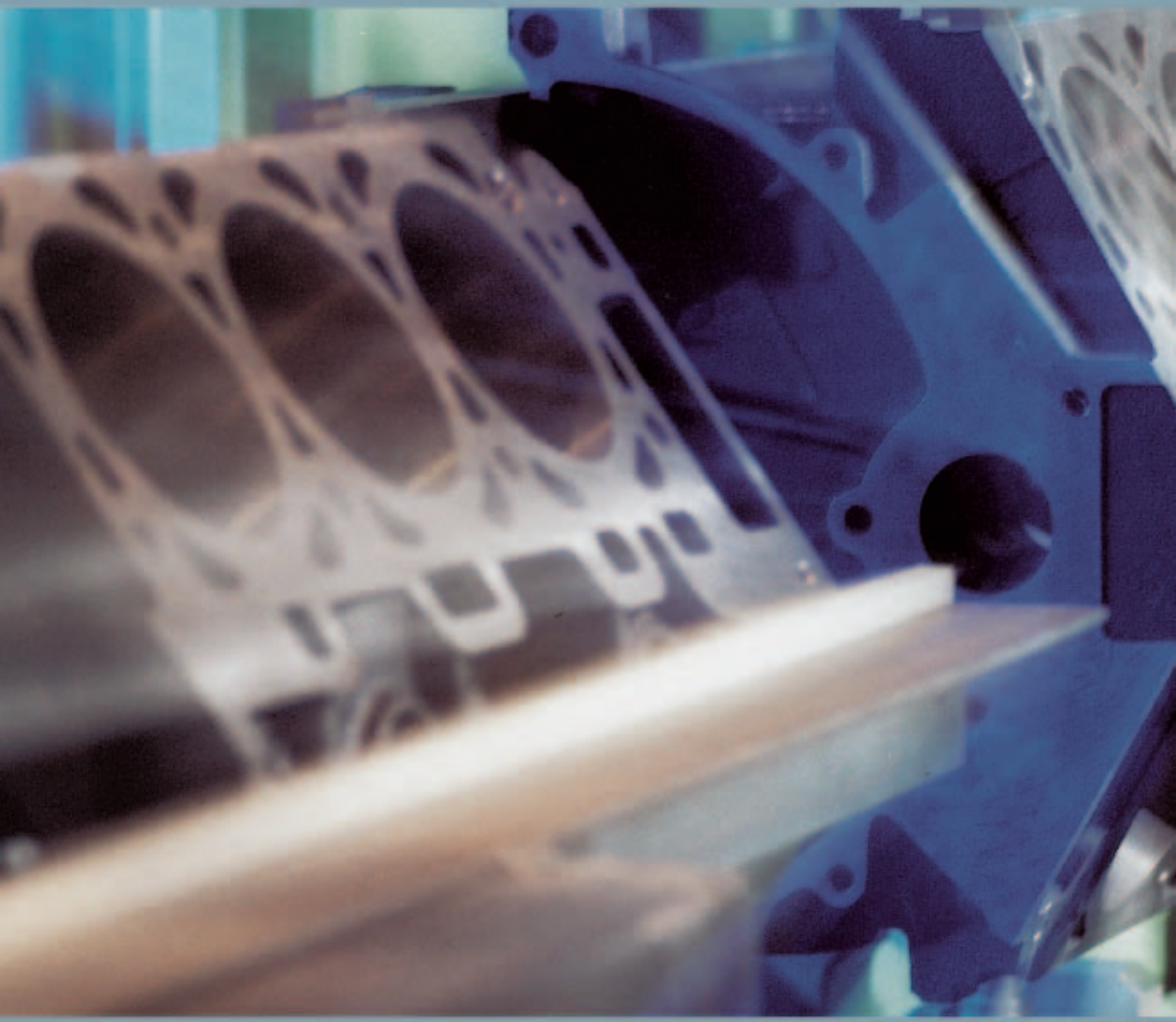
Fail-safe S7-300 signal-modules	Digital input SM 326 F DI 24 x 24 V DC	Digital input SM 326 F 8 x (NAMUR)	Digital output SM 326 F DO 10 x 24 V DC/2A	Digital output SM 326 F DO 8 x 24 V DC/2A	Analog input-module SM 336 F
Number of inputs and outputs	24 (1-channel for SIL 2 sensors) 12 (2-channel for SIL 3 sensors)	8 (1-channel) 4 (2-channel)	10	8	6 (2-channel for SIL 3-sensors) 13 bit
Input or output voltage	24 V DC	NAMUR	24 V DC	24 V DC P-M switching	--
Alarms	Diagnostic alarm	Diagnostic alarm	Diagnostic alarm	Diagnostic alarm	--
Input current/ output current	--	--	2 A per channel for signal "1"	2 A per channel for signal "1"	4-20 mA
PFD*)	SIL2: 1.55E-06 SIL3: 4.99E-08	SIL2: 2.74E-06 SIL3: 4.83E-08	6.97E-06	Still not available	4.96E-08
PFH*)	SIL2: 1.77E-11 SIL3: 5.70E-13	SIL2: 3.13E-11 SIL3: 5.51E-13	7.96E-11	Still not available	5.66E-13
Main Order No.	6ES7 326-1BK..-....	6ES7 326-1RF..-....	6ES7 326-2BF..-....	6ES7 326-2BF4.-...	6ES7 336-1HE..-....

Fail-safe ET 200S modules	Digital input 4/8 F-DI 24 V DC	Digital output 4 F-DO 24 V DC	Power module PM PM-D F 24 V DC	Power module PM PM-E F pp 24 V DC	Power module PM PM-E F pm 24 V DC
No. of inputs/outputs	4 (2-channel for SIL 3 sensors) 8 (1-channel for SIL 2 sensors)	4 for 24 V/2 A	6 shutdown groups each 3A (total current 5 A)	2 relays (total current 10 A)	Up to 2 SIL 3 outputs for 24 V/2 A, 2 relays (total current 10 A)
Input and output voltage	24 V DC	24 V DC	24 V DC	24 V DC	24 V DC
PFD*)	SIL2: << 1.00E-03 SIL3: << 1.00E-05	<< 1.00E-05	Still not available	Still not available	SIL2: << 1.00E-05 SIL3: << 1.00E-05
PFH*)	SIL2: << 1.00E-08 SIL3: << 1.00E-10	<< 1.00E-10	Still not available	Still not available	SIL2: << 1.00E-10 SIL3: << 1.00E-10
Main Order No.	6ES7 138-4FA..-....	6ES7 138-4FB..-....	3RK1903-3BA..-....	6ES7 138-4CF4.-....	6ES7 138-4CF..-....

Failsafe Motor Starter	
Power 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 shutdown groups
Main Order No., motor starters	3RK1301-0.B13-.AA2
Main Order No., terminal module	3RK1903-3A...
Failsafe Contact Multiplier F-CM	
Contacts	4 NO
Diagnostics	Power failure, device error
Switching capacity	1.5 A / 24 V
Main Order No.	3RK1 903-3CA..
Failsafe Power Module PM-D F X1 (input terminal module)	
Operation	Standalone with external safety system
Double terminals for shutdown groups	6
Diagnostics	power failure
Main Order No.	3RK1 903-3DA..

Fail-safe frequency converter	
Power rating	Up to 4.0 kW
Main Order No.	6SL32 44-05..-....

Digital block I/O ET 200eco	
No. of inputs	4 (2-channel for SIL 3 sensors) 8 (1-channel for SIL 3 sensors)
Input voltage	24 V DC
PFD*)	SIL2: << 1.00E-03 SIL3: << 1.00E-05
PFH*)	SIL2: << 1.00E-08 SIL3: << 1.00E-10
Main Order No.	6ES7 148-3FA..-....



Fail-safe motion control systems

8

sinumerik

8 Fail-safe motion control systems

8.1 SINUMERIK Safety Integrated – the safety package for machine tools

Drives and CNC control systems with integrated safety

We have extremely high demands to fulfill when it comes to our Motion Control systems and variable-speed drives for machine tool and production machines: They integrate all of the requirements relating to production, market and industry sector. For our customers, this plays a significant role in increasing quality and productivity. Certified safety functions represent an integral component of our standard products and in addition to affording highly effective protection for man and machine, they also have a significant positive impact on increasing the productivity of our customers.

Safety measures must be provided on machines to protect personnel against potentially hazardous machine motion. These are especially used to prevent hazardous machine motion when protective devices and guards are open. These functions include monitoring positions, e.g. end positions, monitoring speeds and stopping or shutdown in hazardous situations.

Up until now, external devices were mainly used to implement these safety measures. These include contactors, switches, cams and monitoring devices.

When a hazardous situation is detected, generally, these devices initiate contact-based switching operations in the power circuit that stop the potentially hazardous motion - refer to Fig. 8/1.

When integrating safety functions, drive systems and CNC controls handle, in addition to their actual function, also safety functions. Extremely short response times can be achieved due to the short data path from sensing the safety relevant information, e.g. speed or position, up to evaluation.

Generally, systems with integrated safety technology respond extremely quickly when limit values are exceeded or violated, e.g. position or speed limit values. This can be extremely significant for the required monitoring result. The integrated safety technology can directly control the power semiconductors in the drive control unit without using electro-mechanical switching operations in the power circuit. This also means that the system is less prone to faults and disturbances. The wiring and cabling costs are reduced as a result of the integration.

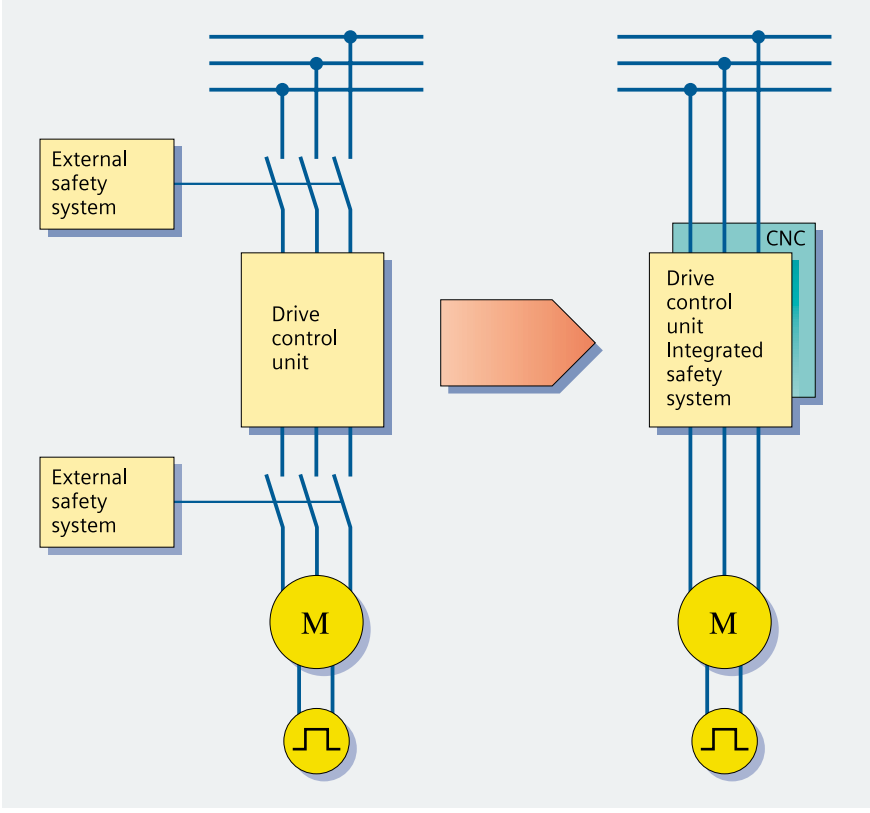


Fig. 8/1
External safety technology, integrated safety technology

Fig. 8/2
The basic SINUMERIK/SIMODRIVE system

Brief description

Functional scope

"SINUMERIK Safety Integrated" offers type-tested safety functions that can be used to implement highly effective personnel and machine protection in line with that required in practice. All safety functions fulfill the requirements of Category 3 acc. to EN 954-1 and are permanent components of the basic system. Neither additional sensors nor evaluation units are required.

This means the following:

Lower installation costs at the machine and a low-profile electrical cabinet.

The functionality includes:

- Functions to safely monitor the speed, standstill and positioning
- Functions to logically interlock signals in a safety-related fashion

Sensors and actuators, for example, EMERGENCY STOP pushbuttons, light curtains, valves or brakes, can be directly coupled to a two-channel I/O or to fail-safe modules. The logical combination and the responses are realized internally using safety-related technology. All safety-related system errors always result in the potentially hazardous motion being safely brought to a standstill, or the power feed to the motor is quickly and contactlessly disconnected. The drive can always be stopped optimally adapted to the operating state of the machine. This means, for example, in the setting-up mode, when the protective door is open, the machine can be stopped as quickly as possible (this is optimum for personnel protection) and in the automatic mode with closed protective door, along the machining path (optimum for machine protection).

In all of the operating modes, the safety functions are available and can communicate with the process itself via safety-related input/output signals. They fulfill the requirements of Category 3 (acc. to EN 954-1). The complete functional scope was certified in the form of a prototype test by the BGIA [German Institute for Safety and Health] in St. Augustin.

This means the following:

A high degree of protection for personnel in the setting-up mode and additional protection for the machine, tool and workpiece in the automatic mode.

These safety functions offer an intelligent intervention, previously unknown, directly down to the electric drives and measuring systems. Reliable function, fast response and a broad acceptance mean that these certified safety systems are highly effective.

Basic structure

A two-channel system structure with diversity is created using the existing-multi-processor structure. The safety functions are redundantly incorporated in the NC, drive and internal PLC. The process quantities and safety-related system data are cross-monitored; also refer to Fig. 8/3.

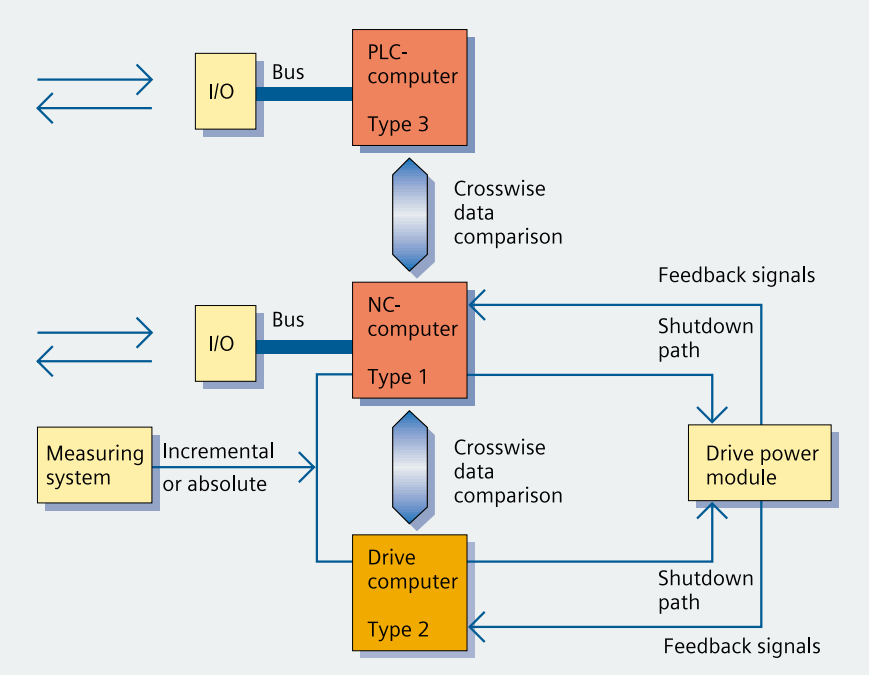


Fig. 8/3
Existing computers form a 2-channel system structure with diversity

Safety-related software and hardware functions are tested at defined time internals using an automated forced checking procedure.

The special feature of this safety concept is that Category 3 acc. to EN 954-1 can be implemented with just one measuring system - the standard motor measuring system. A second sensor is not required. However, it can be incorporated as an additional direct measuring system (e.g. linear scale).

Increased availability using integrated safety technology

Completely new operator control concepts for machines with the widest range of requirements can be implemented by combining the safety functions of SINUMERIK Safety Integrated.

The operator can continue to work - e.g. in the magazine or at the re-equipping station (setting-up) - in parallel with production.

However, topmost priority is always given to protection of the operating personnel. The correct use and operation of the machine, specified as a result of the process, must remain.

The machine protection (machine itself, workpiece, tool, ...) can benefit to a high degree as a result of these new possibilities.

Due to the integrated safety technology, the trend is away from solutions which are distinguished by pure hardware and electromechanical concepts, to software and electronics. This means that the safety technology with parts and components which are subject to wear, will be successively replaced.

Furthermore, integrated safety technology allows an intelligent system intervention directly down to the sensors and actuators which was previously unknown. Completely new diagnostic functionaliy is created, which permits preventive fault detection and identification. Even for faults which suddenly occur during production, the risk of personnel injury or machine damage can be significantly reduced by quickly detecting the fault and stopping in a coordinated, safety-related fashion.

Integrated safety technology permits:

- Optimized processes
- Sub-processes can run in parallel
- Simpler machine infrastructures
- Machine operator control concepts in line with that required in practice.

Impact on the availability:

- Less potential for faults and errors
- Longer production times
- Shorter downtimes.

When consequentially used, integrated safety technology offers a significant potential to increase system availability.

Equipment components

The Motion Control Systems business division belonging to the "Automation and Drives Group" develops, manufactures and markets numerical controls and drive systems under the SINUMERIK and SIMODRIVE product names. These systems are especially used for complex and fast motion control and positioning applications when special demands are placed on precision.

CNC control SINUMERIK 840D – compact high technology

SINUMERIK 840D is a CNC control for up to 31 axes. It is an integral component of the modular SIMODRIVE 611 drive system. Thus, communications with the drive modules are realized through the shortest path.

Based on the modular SIMODRIVE 611 system, a module has been conceived in the form of SINUMERIK 840D, which provides significant technical advantages over comparable individual solutions.

The highlights include:

- Up to 31 axes can be positioned
- Precision better than 1 µm
- Integrated SIMATIC S7-300-CPU with PROFIBUS-DP interface
- Just 50 mm wide in the SIMODRIVE 611digital design
- Scalable processor performance
- Integrated, certified safety functions

Fig. 8/4
SINUMERIK 840D – NCU and NCU box

SIMODRIVE 611 digital AC drive converters

SIMODRIVE 611digital is a flexible configurable drive converter system, which is fully aligned to the technical requirements placed on state-of-the-art machines, both economically as well as ecologically. With SIMODRIVE 611digital, Siemens is offering a drive converter system with digital closed-loop control, which is guaranteed to fulfill the highest requirements regarding dynamic performance, speed control range and smooth running characteristics.

Thanks to the modular drive system design, drive configurations can be implemented with almost any number of axes and main spindles. The axis modules are designed for 1FT6, 1FK6, 1FK7 and 1FN feed motors as well as 1PH main spindle and 1FE built-in synchronous motors.

The SIMODRIVE 611digital drive converter system offers the following advantages:

- The EMC Directive is fulfilled and line supply infeeds compliant with EMC requirements
- Lower stressing on the line supply thanks to sinusoidal current operation and regenerative feedback into the line supply
- Compact design by using low-loss power semiconductors
- High degree of functionality in the tightest space using highly integrated closed-loop control electronics

SIMODRIVE 611digital control units are used in conjunction with the SIMODRIVE 1FT6/1FK6/ 1FK7 three-phase servomotors and 1FN linear motors for feed drives as well as 1FE and 1PH motors for main spindle drives. They evaluate the optical sine-cosine encoders, which are integrated in the 1FT6/1FK6/1/FK7 and 1PH motors. This means that up to 4.2 million increments/motor revolutions can be achieved as measuring circuit resolution. For 1FN motors, a linear incremental or absolute-coded measuring system with EnDat interface is required to sense the position, actual speed and pole position. 1FE motors require a hollow shaft encoder with sinusoidal-cosinusoidal signals for the closed-loop speed and position control. For control modules with direct position sensing, a direct measuring system can be connected. The certified safety functions are available for all encoder versions.

Fig. 8/5
SIMODRIVE 611digital drive converter system

Fig. 8/6
Digital control module

Various drive-related versions can be implemented using the modular SIMODRIVE 611digital drive converter system, and combined as required in a drive group.

1FK6/1FK7 and 1FT6 servomotors

These represent the optimum solution when the highest dynamic performance and precision are demanded. Users are especially enthusiastic about the simple and good controllability, combined with features such as freedom of maintenance and high overload capability.

1FK6/1FK7 and 1FT6 three-phase servomotors are compact permanent-magnet synchronous motors, which have been specifically developed for operation with the SIMODRIVE 611-digital drive converter system. The fully digital closed-loop control and the new integrated encoder system (motor measuring system) fulfill high demands placed on the dynamic performance, speed control range, smooth running and positioning accuracy.

Special speed-controlled 1PH induction motors

Based on the Transvector control (field-vector control), which was developed and patented by Siemens, an induction motor can be just as simply controlled as a DC motor. An induction motor controlled by SIMODRIVE 611digital has many advantages over DC motors, such as freedom of maintenance and full availability of the rated torque even at standstill. 1PH motors are equipped with a high-quality encoder system for closed-loop speed control and positioning.

1PM main-spindle motors with hollow shaft

1PM4 liquid-cooled motors and 1PM6 air-cooled motors are designed so that they can be directly mounted onto mechanical spindles. The hollow shaft allows the feed of cooling-lubricating medium for internally cooled tools. The motors have an integrated hollow-shaft measuring system to detect the motor speed and indirect position.

1FN linear motors

1FN three-phase linear motors together with SIMODRIVE 611digital form a linear drive system specifically harmonized and coordinated to machine tool applications. The motors consist of a primary section and a secondary section with rare-earth magnets. When suitable measuring systems are used, the motors can be positioned in the nanometer range. The high traversing velocities and the extremely high dynamic performance which can be achieved with the motors, are just some of the highlights worth mentioning.

1FE build-in synchronous motors

1FE build-in motors are water-cooled synchronous motors that are supplied as components and can be especially used as main spindle drive. These motors are mainly used together with the SIMODRIVE 611digital drive module where the highest demands are placed on the machining quality, precision, smooth running characteristics and extremely short accelerating times.

Fig. 8/7
1FT6 servomotors

Fig. 8/8
1PH induction build-in motor

Fig. 8/11
1PH7 induction motor

Fig. 8/9
1FN3 linear motor

Fig. 8/10
1FE synchronous build-in motor

Fig. 8/12
System components and connection systems

Accessories

The Siemens SINUMERIK and SIMODRIVE automation systems are designed for all types of machine tools and processing equipment. With its MOTION-CONNECT family of cables, Siemens offers the associated pre-fabricated cables, sold by the meter, and connectors for the systems, optimally adapted to the particular application.

The customer benefits of Siemens pre-fabricated cables include:

- System functionality and compatibility are guaranteed
- EMC EC Directives are fulfilled
- Insulation in compliance with VDE
- In conformance with DESINA
- No mounting problems
- No special tools are required
- A tailored solution for every application using MOTION-CONNECT 800, 700, 500
- Guarantees that the complete system functions perfectly

The supplementary system components such as encoders, hand wheels, operator control and handheld programming devices are also harmonized with the overall system.

SIMODRIVE sensor measuring systems for measuring distances, angles and velocities are available from Siemens as either incremental encoders or absolute value encoders. For incremental encoders, the interfaces are harmonized with the particular control system. Absolute-value encoders are available in versions with SSI, EnDat and PROFIBUS-DP. The encoders can be quickly and easily commissioned as they can be parameterized. High machine availability is achieved using system-tested components.

The original Siemens accessories are an essential component of SINUMERIK Safety Integrated applications.

System prerequisites

Ordering data, refer to Catalog NC 60 and ST76

SIMODRIVE 611digital

- Safety Integrated is available with digital drives
- The High-performance and the High-Standard controls of the 611digital can be used
- The control modules must always be ordered with DMS measuring circuit,
- At least one measuring system must always be available

SINUMERIK

For SINUMERIK, Safety Integrated is available for the 840C and 840D types in conjunction with SIMODRIVE 611 digital. In this particular case, all of the CPU versions can be used.

- Input/outputs for safety-related signals.
  1. NC I/O and PLC I/O form a 2-channel I/O structure,
  or
  2. Fail-safe modules can be connected via PROFIBUS to the extended PROFIsafe protocol (not with SINUMERIK 840C)
  or
  3. NCU onboard I/Os and PLC form a 2-channel I/O structure (not with SINUMERIK 840C)
- SINUMERIK Safety Integrated is a software option and comprises a basis and axis options.
- System resources of the CPUs involved (NC, PLC, drive) are required for the SI functions - these resources are dependent on the scope of the user functions and the number of drives. In boundary cases, it may be necessary to use a higher-performance NC-CPU.

Encoders and measuring circuit

- Every measuring system can be essentially used that is compliance with the measuring circuit specifications of SIMODRIVE 611D.
- 1-encoder concept: At least one measuring system is required that is generally covered by the indirect motor measuring system (IMS) as incremental encoder or absolute value encoder.
- 2-encoder concept: A second measuring system is not required; however, it can be incorporated as direct measuring system (DMS).
- The measuring circuit cable must correspond to the specifications of SIMODRIVE 611 digital, e.g. shielded pairs.

SIMATIC

- Standard SIMATIC components can be used.
- Inputs/outputs for safety-related signals.
  1. NC I/O and PLC I/O for a 2-channel I/O structure
  or
  2. Fail-safe modules can be-connected via PROFIBUS using the non-proprietary PROFIsafe profile

HMI

- The operator control and display devices (OPs) are not integrated into the safety concept. They are only used to display safety-relevant data for diagnostics and commissioning.

Safe stopping process

The safe stopping process is not an autonomous function, but describes a procedure that can be implemented using "SINUMERIK Safety Integrated" functions. The safe stopping process safely stops the motion and brings the drive to a standstill when a monitoring function or a sensor responds (e.g. light curtain).

All safety-related faults and errors in the system or if an appropriate sensor responds, always result in a coordinated, safe stopping of the hazardous motion. Depending on the system engineering specifications, the power feed to the motor can be quickly disconnected. This power disconnection between the drive converter and motor, required in special cases (where the drives go into a torque-free condition), is realized contactlessly and can be initiated on an axis-for-axis basis with an extremely short response time. This means that it is no longer necessary to discharge the DC link in the drive. The drives are always shut down in an optimum fashion according to the actual operating status of the machine.

The integrated functions are supplemented by activating external braking mechanisms, and, for the safe stopping process, results in the shortest possible braking travel. External braking mechanisms can include, for example:

- External mechanical brakes, stopping or operating brakes
- External electrical brakes, such as e.g. armature short-circuit brakes.

Principally, a line contactor is no longer required if the machine has a main switch, which allows it to be electrically disconnected from the supply.

Stop responses

A high degree of fail-safety is achieved as a result of the two-channel monitoring structure with its permanent cross-comparison. If differences occur between the two monitoring channels, alarms and stop responses are automatically initiated. The stop responses will safely shut down the drives corresponding to the particular requirements of the machine. A differentiation is made between STOP A, B, C, D, E, F and test stop versions. The system can specify a preset stop response type when a fault/error occurs or the machine OEM can configure the required response. When the limit values, defined using machine data are violated, the stop responses of the machine OEM can be initiated. Stops A, C and D can also be selected, referenced to an external event, via safety-related inputs (SGE). The stop versions are implemented as follows:

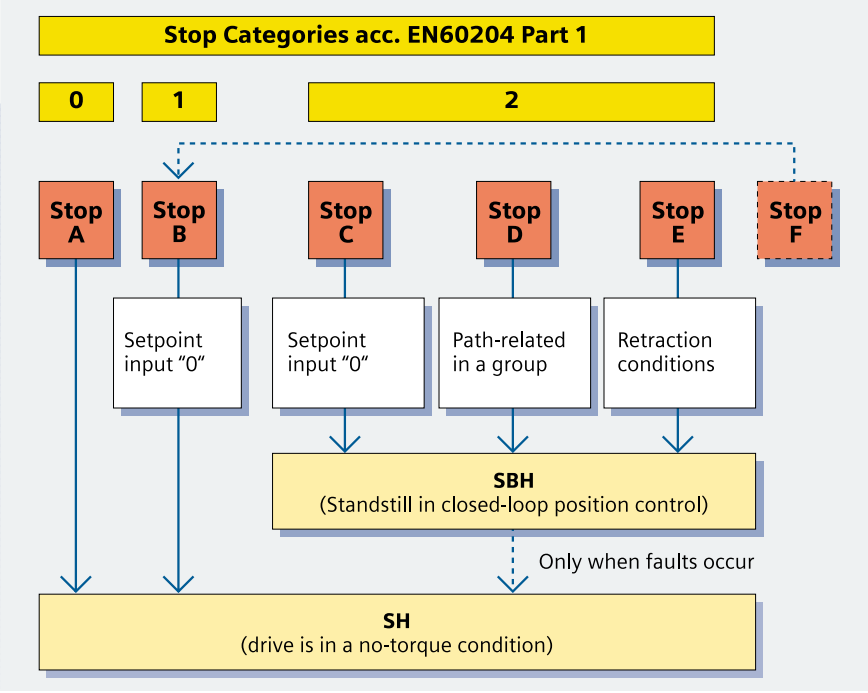


Fig.8/13
Stop versions for different stopping types

- **Stop A**

Using a Stop A (corresponding to a Category 0 stop acc. to EN 60204, without electrical isolation), the drive is directly switched into a no-torque condition using the “safe standstill” function. A drive that is at a standstill can no longer undesirably start. A drive that is still moving coasts down. This can be prevented by using external braking mechanisms such as armature short-circuit braking, holding and operating brakes. The axis-specific alarm results in a mode stop - this means as a result of the response in one axis, all of the axes and spindles in a mode group are stopped. At the end of a Stop A, the axis is at a “safe standstill”.

- **Stop B**

The drive is braked along the current limit, closed-loop speed controlled and is then transitioned into “safe standstill” (SH) - (this corresponds to a Category 1 stop according to EN 60204, without electrical isolation).

- **Stop C**

The drive is braked along the current limit in the closed-loop speed controlled mode and goes into the “safe operating stop” state.

- **Stop D**

The drive, as a group, including the synchronous axes, is braked along the machining path and goes into the “safe operating stop” state.

- **Stop E**

The drive, as a group, including retraction motion, is braked path-related and goes into the “safe operating stop” state.

- **Stop F**

The stop F response is permanently assigned to the cross-monitoring result and data comparison. This means that faults/errors in the drive and on the control side are detected. Depending on the configuration, a Stop B or A response is initiated. “Safe standstill” is effective at the end.

When configuring the stop responses, personnel protection has topmost priority. The optimum stop response for machine protection can be configured in the automatic mode with the protective door closed. The goal is always to optimally stop the machine in any particular situation.

Example 1: Grinding machine with open protective door (setting-up operation):

- Feed drives with Stop C:
  The drives are braked as quickly as possible at the current limit on an axis-for-axis basis and are then transitioned into “safe standstill”.
  This means that they remain in the closed-loop position controlled mode.

- Grinding wheel spindle with external Stop A:
  In this operating mode, the drive is kept in a no-torque condition using the external Stop A with “safe standstill”.

Example 2: Grinding machine in the automatic mode:

- Feed drives with Stop E:
  As a group, the drives retract (cutting- free/moving away), are braked along the contour using a ramp and are then transitioned into “safe operating stop”.
  This means that they remain in the closed-loop position controlled mode.

- Grinding wheel drive with Stop D:
  The drive is braked along a ramp and is then kept below the rupture limit using the torque load. It is transitioned into “safe operating stop” and kept in closed-loop position control.

Safe standstill – SH

When a fault occurs or in conjunction with a machine function, the “safe standstill” is used to safely disconnect the power feed to the motor. This is realized for each axis and the power is disconnected contactlessly. The basis for the "safe standstill function" is the safety-related pulse cancellation integrated into the SIMODRIVE 611D drive modules.

The machine OEM must take the appropriate measures to stop axis movement after the power feed to the motor has been disconnected (e.g. to prevent hanging vertical axes from dropping).

Features
- The motor cannot undesirably start.
- The power feed to the motor is safely interrupted.
- The motor is not electrically isolated from the drive module or the DC link of the drive converter.

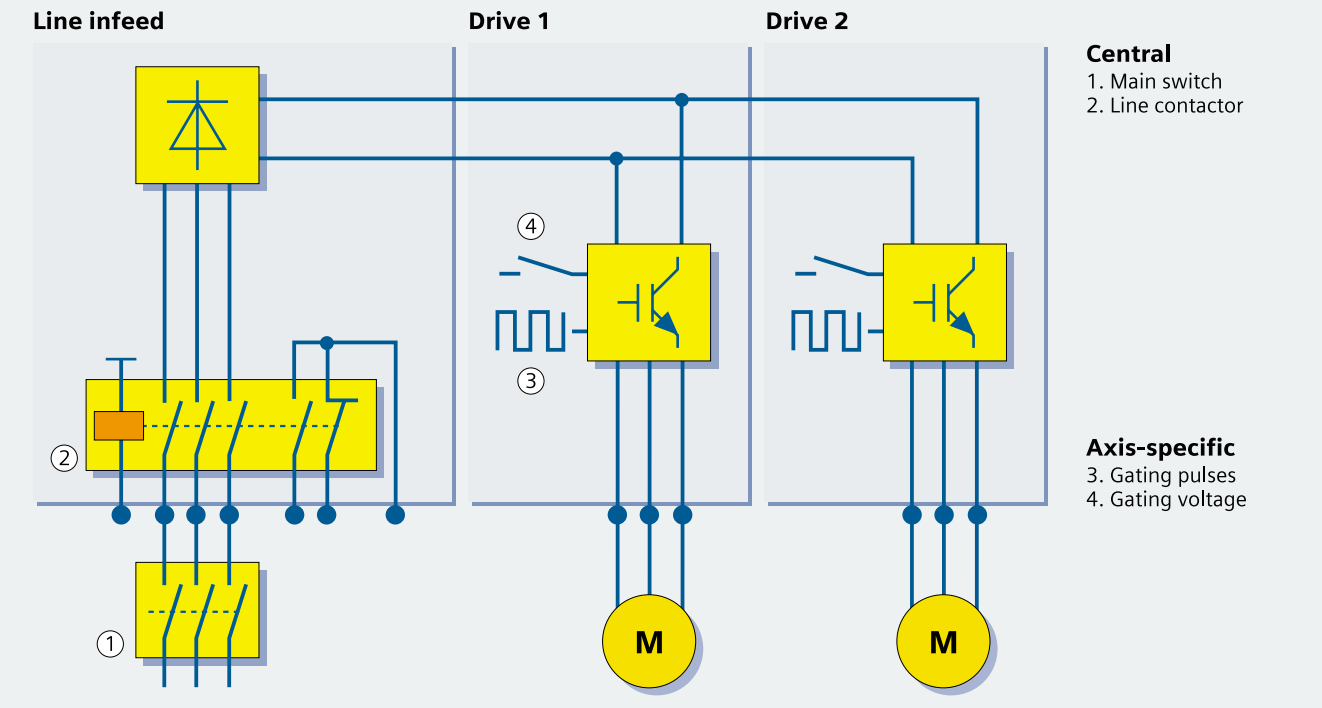


Fig. 8/14
Safe standstill - electronically and contactlessly disconnecting the power

4 basic ways of bringing a motor into a no-torque condition are shown in figure 8/14. These all have a different mode of operation.

① **Main switch:**
Mode of operation ⇨ central
Every machine must be equipped with at least one disconnect switch that allows the machine to be electrically isolated from the line supply. This is generally realized using the main switch. This measure protects personnel working on the equipment against electric shock. When opened, the switch must be locked-out so that it cannot be undesirably closed.

② Integrated line contactor:
Mode of operation ⇨ central
The complete drive converter can be electrically isolated from the line supply using the line contactor in the infeed module. When referred to the drive converter, this measure corresponds to a Category 0 stop. In the past, for an Emergency Stop, the integrated line contactor switched the drive converter/motor into a torque-free condition in conjunction with a Category 1 stop. However, electrical isolation is not mandatory for EMERGENCY STOP.

(Refer to the System Manual, Chapter 1)

③ Pulse cancellation in the gating unit
Mode of operation ⇨ axis-for-axis
The fastest way of bringing a drive, axis-for-axis into a torque-free condition is to cancel the pulses via the gating unit. However, this measure is, when applied by itself, not a safety-related operation.

④ Control voltage of the optocoupler
Mode of operation ⇨ axis-for-axis

If the optocoupler control voltage is removed, then when a fault occurs, the gating unit pulses cannot be converted into a torque in the drive power module. However, this measure is, when applied by itself, not safety-related. It is not possible to electrically isolate the drive converter DC link (600 V) from the motor. This is also not required for "functional safety".

Conclusion:

Measures 3 and 4 are physically decoupled and together form an effective and safety-related method of canceling the drive converter pulses on an axis-for-axis basis. They form the basis for "safe standstill" and can be independently initiated from the drive and the NC. The concept is rounded-off by integrating it into cyclic tasks (forced checking procedure).

This means that a complete safety-related concept is created from individual measures that completely fulfill the requirements for EMERGENCY STOP.
It is no longer mandatory to open the line contactor.

However, when carrying-out work (e.g. service, maintenance...) on live components the equipment must always be electrically isolated from the line supply.

Comment regarding Emergency Stop in the US

NFPA 79, the „Electrical Standard for Industrial Machinery" published by the National Fire Protection Agency in the US, war revised and has been in effect since 2002. For the first time, appropriately qualified software, electronics and bus communication systems are permitted for Category 0 Emergency Stop. However, contrary to the EU for Category 0 Emergency Stop, it as also mandatory to subsequently electrically isolate the safety-relevant equipment from the line supply through electromechanical means. This requirement can be engineered by the machine OEM as simply a supplement for the US version.

Safe operating stop - SBH

This function is used to safely monitor the standstill position of an axis or spindle. In this case, the drives remain fully functional in the closed-loop position controlled or closed-loop speed controlled mode.

Features

- The axis remains in the closed-loop controlled mode.
- Parameterizable standstill tolerance window.
- Configurable stop response when the monitoring responds (Stop B or A).

Safe braking ramp – SBR

With this function, the expectation that after a stop command, the actual velocity must be reduced is used as basis (the speed characteristic is monitored).

When a stop command is initiated, the disabled velocity plus a velocity tolerance, specified using machine data, is activated as velocity limit. This limit is compared with the actual velocity (must be less than or remain the same) and is cyclically corrected.
This means the system quickly detects if the axis re-accelerates during braking; a subsequent response is then initiated.

Features

- The system quickly detects if the drive starts to accelerate while braking.
- The "safe braking ramp" is automatically activated if a stop B or C was initiated.
- A Stop A is directly initiated if the "safe braking ramp" is initiated.

Example, Emergency Stop

Safety-related signals and the required responses are logically combined internally using safety-related technology. The electric drives are safely stopped and are then disconnected from the power source via the electronics. An undesirable restart is also safely prevented. External potentially hazardous energy sources, for example, hydraulic systems or lasers etc. can be disabled using safety-related outputs associated with the integrated Emergency Stop logic and downstream actuators (power contactors, valves). The coordinated safe stopping process prevents or reduces subsequent damage (e.g. crash) when shutting down and also permits a fast, simple restart.

Test stop

Using the test stop, for each monitoring channel, the complete shutdown path is tested with the external circuitry.

When executing the test, the comparators and stop modules of the two monitoring channels, which are responsible for the stop function, are executed one after the other. For more information on the forced checking procedure, also refer to the Section "Forced checking procedure" for SINUMERIK Safety Integrated.

Monitoring speed and position

Safely reduced speed - SG

The “safely reduced speed” function is used to safely monitor the speed of a drive.

To realize this, the actual speed of the drive is cyclically compared, in the monitoring clock cycle, with the speed limit, selected via safety-related inputs. The speed limits are defined in the machine data.

Different applications and operating states at the machine can be monitored using the speed limit values for SG1, SG2, SG3 or SG4. Further, the limit values safely-reduced speed 2 and safely-reduced speed 4 can be graded in 16 steps using “safety-related inputs” (4 bits). The entry is made as a % (1 to 100%) and is saved in a table in the machine data. Thus, a total of 34 freely selectable speed limits are available for each drive. This allows personnel and machine protection to be implemented in the setting-up mode and also in the automatic mode.

Comment: For changeover gearboxes, the correct gearbox ratio must be selected!

Features

- The load-side speed limit values are safely monitored.
- The monitored limit values can be adapted to various operating states (e.g. test, setting-up, automatic operation).
- Configurable, SG-specific stop responses.

Safely reduced speed-specific setpoint limiting

Using this function, for the first time, in addition to the speed actual value, the speed setpoint is also considered. The “safely reduced speed-specific setpoint limiting” automatically limits the setpoint to the currently effective limit of the safely reduced speed. If this value changes for a drive, then the setpoint limit is automatically corrected. If the drives operate in a group, then the function acts on all of the coupled drives. This means that the machined contour is always maintained.

Applications

- When testing NC programs (operating mode 3), e.g. when the protective door is open. Now, no test-specific changes have to be made to the program parameters.
- If a safety-related area is entered, e.g. using traversing keys, where the lower SG limit values are active, then the drive is not shut down, but instead is automatically reduced to the speed setpoint that is permissible there.

Features

- The setpoint limit acts in the NCK through 1-channel.
- Effective when traversing drives via traversing keys or when NC programs are executed.
- The value of the limit lies beneath the active SG limit value by an adjustable percentage value.
- The axes involved are accelerated or braked without any delay, interpolating.
- The function is only executed if the programmed setpoint lies above the active SG limit value.
- If the programmed setpoint is less than the active SG limit value, then the drives traverse as specified in the program.

Safe software limit switch - SE

A working zone/protective zone demarcation or traversing range limiting can be implemented for each axis using this “safe software limit switch.” This means, for example, that hardware limit switches are not required on the mechanical system. Two limit switch pairs per axis are available. Each limit switch pair consists of a positive switch (safe limit switch 1+ and safe limit switch 2+) and a negative switch (safe limit switch 1– and safe limit switch 2–). It is possible to toggle between safe limit switch 1 and safe limit switch 2 using the safety-related inputs.

Features

- End positions are defined and evaluated per software in a safety-related fashion.
- Configurable stop response when passing end positions.
- The stop response when passing end positions is realized inside the software.

Safe software cam - SN

Safe range identification can be implemented for each axis using the safe software cam function. This means that today's "hardware solution" can be replaced

4 cam pairs (safe software cam 1 to safe software cam 4) are available for each axis. Each cam pair comprises a positive cam (safe software cams 1+, 2+, 3+ and 4+) and a negative cam (safe software cams 1–, 2–, 3– and 4–). Each cam signal can be individually configured via the machine data. The cam signals are output via safety-related outputs.

Features

- Cam positions can be safely defined and evaluated using software.
- Safety ranges are defined.
- SN dependent, safety changeover of safety-related functions (e.g. safety-related changeover/selection of SG stages dependent on the actual position).

Logically combining safety-related process signals

Safe programmable logic - SPL

The "safe programmable logic" allows, for the first time, safety-related sensors and actuators to be directly connected and logically combined. The logic is redundantly incorporated in the NC and in the internal PLC. This means that all safety-related sensors and actuators, e.g. Emergency Stop or interlocking concepts for protective doors can be configured using the SINUMERIK Safety Integrated software. In conjunction with "safe standstill", the Emergency Stop can now be implemented in the evaluation logic up to the power disconnection contactlessly and using safety-related technology.

Discrete hardware contacts can be eliminated which is reflected in a simplified cabinet design. Only the power contacts (e.g. contactors) are required to directly control the external actuators.

Features

- Universal, programmable logic in safety-related technology
- The logic is immediately activated after run-up
- Cyclic sequence independent of the user program
- Integrated timer for the forced checking procedure
- Effective in all operating modes.

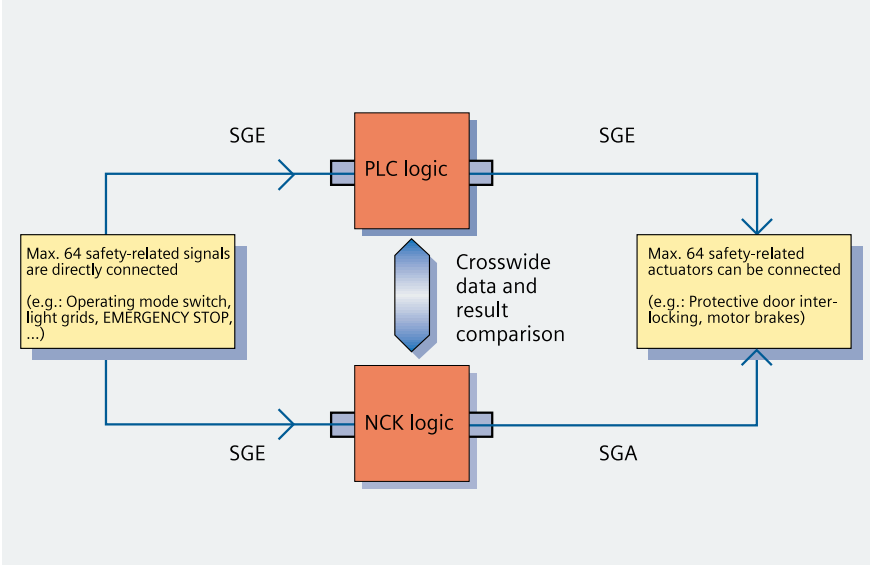


Fig. 8/15
Basic structure - safe programmable logic

Safety-related I/O - SGE/SGA

The safety-related input and output signals represent the interface to the process. They are digital signals that are entered into the system or are output from the system through two channels. The safety-related inputs and outputs need not be routed via hardware terminals.

In conjunction with the safe programmable logic, when required, they can be internally processed as software signal.

Features

- Safety functions can be selected and de-selected
- Limit values can be selected and changed-over
- Status signals can be fed back
- Cam signals can be output
- Sensors can be directly connected
- Actuators can be directly connected.

Vertical axes are protected from dropping

General requirements

When drives are shut down, axes or mechanical assemblies can drop due to the force of gravity. For vertical linear axes (hanging/suspended axes) or for rotary axes or spindles with a non-symmetrical weight distribution, this can result in potentially hazardous motion. This is the reason that these axes or mechanical assemblies must be safely kept at a standstill using suitable measures. Measures to achieve this can include, for example:

a) Temporarily active
Holding brakes
Operating brakes
Electric drives

b) Continuously active
Mechanical weight equalization

c) Active in exceptional cases
Pins
Various types of supports

The measure or measures which is/are selected depends on the type of work which is to be carried-out in the dangerous area. Is work to be directly carried-out under a suspended load or only close to it? Also the time spent in the dangerous area must be taken into account in the design phase as this may make it necessary to combine several measures. The hazardous analysis is always the basis for this and must be carried-out for each and every machine. The overall concept must be designed so that it fulfills the requirements for personnel protection according to the EEC Machinery Directive and all other applicable standards and directives.

Comment:

When carrying-out work on live parts and components (with the exception of safety extra-low voltage), electrical isolation from the line supply is always required.

Requirements from the German Trade Association data sheet (EM II, Mainz)

The requirements placed on machines with the appropriate hazard potential are described in this data sheet.

Here are some of the most important requirements as excerpt:

- Safety-related, redundant holding system in order to prevent vertical axes dropping"
- Testing mechanical brakes (control category 2 acc. to EN 954-1)
- Protection to prevent electric drive unintentionally/accidentally restarting (control category 3 acc. to EN 954-1)
- Acceptance test using a form

The actual document is available in the Internet under
www.smbg.de/Sites/downloads/005-MFS-A04_Vertikalachsen.pdf

Concept to prevent vertical axes dropping

The existing systems, electric drive and mechanical brake form, together, the safety-related, redundant holding system. The safety concept of SINUMERIK Safety Integrated integrates these standard components so that their effect is safety-related.

1. Safety-related drive achieved by applying safety functions, e.g.:
   - "Safe standstill"
   - "Safe operating stop"
   - "Safely reduced speed"

2. Safe braking function achieved using the "safety relevant brake management" with the sub-functions:
   - "Safe brake control"
   - "Safe brake test"

The safe drive forms the 1st holding system and is the main holding system element - the mechanical brake forms, as safety-related brake function, the 2nd holding system and is (open) in the standby mode.

When the drive fails, the brake is automatically and safely activated and assumes the function of holding the mechanical system. It is not absolutely necessary to use a second brake.
This means that for the first time there is an extensive and integrated solution regarding " preventing vertical axes dropping" as well as rotary axes and spindles with non-symmetrical weight distribution.

The risk when working with hanging/ suspended loads is, using this functionality, significantly reduced and therefore provides an additional role in protecting personnel. Not only this, machine damage as a result of dropping axes is essentially avoided and the availability of machines and systems increased.

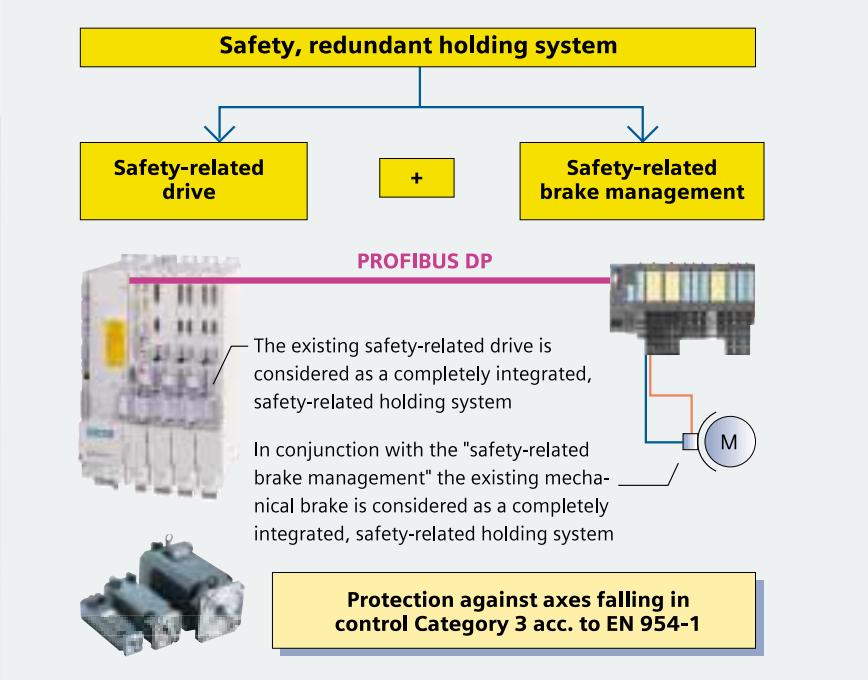


Fig. 8/16
Protection against vertical axes dropping

Depending on the particular requirement, the safe redundant holding system can be used in the following applications:

1. The drive is active if the brake is open and is in the standby mode

   Objective: Minimize the sag to < 25 mm
   - The drive can move or remain stationary
   - The brake automatically and safely closes as soon as the drive fails e.g. due to a system-fault.

   Result:
   Depending on the speed, direction of motion, system response time, brake closing time and friction in the mechanical system, then the vertical axis sags (drops) - which cannot be avoided.

2. The drive and the brake are simultaneously active (drive with adapted control parameters / filters)

   Objective: Minimize the sag to < 1 mm
   - The drive is stationary, the brake is closed
   - A signal is automatically output as soon as one of the two holding systems fails
   - Now, the holding system that is still intact, only holds the mechanical system

Result:
The vertical axis does not drop any significant distance that would be relevant for personnel protection.

Comments:

- Acceptance report
  The amount of sag should be measured and documented in the acceptance report!

- When the drives are shut down for operational reasons

The drive is operationally shut down independent of any system faults - e.g. for an Emergency Stop. In this case, the brake is closed before the drive is shut down and the vertical axis is mechanically clamped. This involves a specific operation which means that the vertical axis does not drop any significant distance that would be relevant for personnel protection (< 1 mm).

Safe brake management - SBM

The reliability of a mechanical brake is a significant component when protecting vertical axes from dropping. Analyses of accidents indicated that both faults in the control as well as in the mechanical system of the brake were responsible for vertical axes dropping. The analysis also indicated that these accidents could have been avoided by using safety technology.

With this as background, we are offering our customers a solution with “safe brake management”.

“Safe brake management” (SBM) comprises two function elements:

1. Safe brake control (SBC)

2. Safe brake test (SBT)

Brakes which are generally used today are not safety-related components. By integrating the standard brake (a component proven in operation) in the safety concept of SINUMERIK Safety Integrated, a safe brake function is obtained.

The brake is safely controlled and is subject to a forced checking procedure. Extended test measures are required as there is no feedback signal for the holding torque. The safe brake test can fulfill this requirement. Faults in the control and in the brake mechanical system can be detected using the extended test measures.

Depending on the result of the hazard analysis, there are various ways of mounting the brake:

1. A brake in the motor, transmission elements with overload factor > 2 (BG EM II, Mainz) [German Regulatory body]

2. A brake connected to the load transmission elements with overload factor < 2

3. A brake in the motor - special requirement and a brake connected to the load

In case of doubt, the preferred solution is to mount the brake at the load, e.g. on the linear guide instead of mounting it in or on the motor.

Safe brake control

The brake (operating or holding brake) is, in control Category 3 (acc. to EN 954-1) safely and electrically controlled. The control is realized through two channels (P/M switching) with:

- Safety-related outputs with separate PLC and NC hardware

- Fail-safe outputs of the F-DO in ET 200S PROFIsafe

Using these two versions, it is possible to detect faults on the control lines, for example, short-circuits, broken cable etc. Even if a channel fails, the brake can still be controlled.

Comment:

Intermediate relay stages increase the response time when controlling the brake - this increases the distance that the vertical axis drops. This is the reason, if possible, that a direct electronic control is preferred. This is possible up to 2 A.

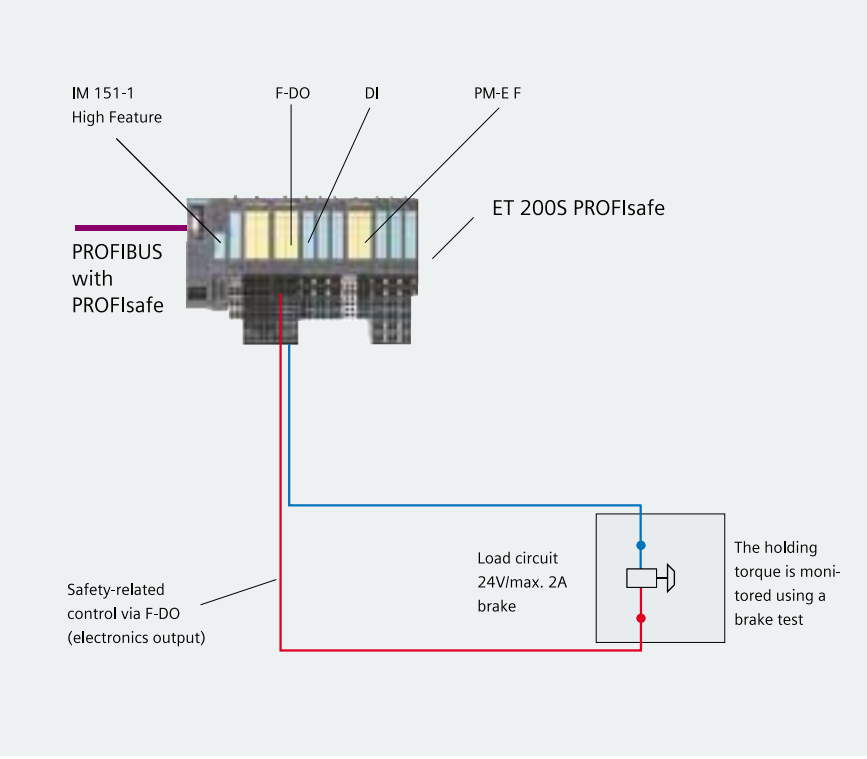


Fig. 8/17
Safe brake control

Safe brake test

The safe brake test cyclically tests as to whether the expected holding torque is still available. In this case, the drive deliberately moves against the closed brake and subjects this to a test torque - when successful without the axis moving. However, if the axis moves, then it can be assumed that the brake holding torque is no longer sufficient to hold the vertical axis. The test is then canceled and a fault signal is output. The axis should then be traversed into a safe position and the vertical axis disengaged or clamped using the appropriate pins. This can also be automatically realized. The protective door remains interlocked until the "resting position" is reached. This can be interrogated using "safe software cams". If all of the conditions are fulfilled, then the brake must serviced.

The safe brake test is executed as part of the forced checking procedure before testing the shutdown paths. If a brake defect is identified, then the shutdown path test that would result in a pulse cancellation, is no longer initiated and a fault message is generated.

The safety brake test is implemented in Category 2.

Comment regarding stop Category 1 according to EN 60204 for Emergency Stop

After regenerative braking, the Standard specifies that the electric drives must be isolated from the power source as protection against undesirable restart. However, an Emergency Stop has the goal of providing protection against potentially hazardous motion and not to protect against electric shock. EN 60204 does not taken into account that safe drives for Emergency Stop with stop Category 2 must at least guarantee the same quality. For a stop Category 2, safe drives after stopping, go into the "safe operating stop" mode and remain fully functional in the closed-loop controlled mode.

The following scenario with conventional technology will clearly show this:

1. The holding torque of the mechanical brake connected to a vertical axis is zero as a result of a fault (control/mechanical system). Emergency Stop is configured/ engineered acc. to EN 60204 with stop Category 1.

2. For conventional safety concepts, the fault is not detected in the brake control and in the brake mechanical system – this represents a "dormant fault".

3. An operator now presses Emergency Stop!
   Result:
   As the holding brake is defective, and the drive is isolated from the power source with a Category 1 stop, the vertical axis drops and, in conjunction with an Emergency Stop, results in a potentially hazardous motion!

Here is the same scenario using safe drives

1. The holding torque of the mechanical holding brake at a vertical axis is zero due to a mechanical fault (a fault in the brake control is directly detected, and the brake is closed via the second channel).
   The Emergency Stop is configured acc. to EN 60204 with a Category 1 stop.

2. The fault is detected by the brake test. An appropriate fault signal is displayed. The protective door remains interlocked, and the axis must be moved to a safe position.

3. An operator now presses the Emergency Stop before reaching the safe position!
   Result:
   In spite of the fact that the Emergency Stop has been activated, the drive with the defective brake is not isolated from the power source, but safely stopped and then is safely monitored at standstill using the safe operating stop. No hazardous motion-occurs.

Integrated and partially-automated acceptance report

For every drive control, the system behavior is adapted to the requirements of the particular machine using parameters that can be set. For instance, the maximum permissible speeds or the braking characteristics when stopping a drive are defined. In so doing, when configuring/engineering the system or when entering parameters via a PC or a programming device, errors can be made. This is the reason that as part of commissioning procedure, all of the safety functions of electric drive systems should be tested and documented in the form of a machine acceptance test. This must be done independently of whether safety functions are implemented using control systems with integrated safety or using external monitoring equipment and devices.

A differentiation is made between a complete and a partial acceptance test. With a complete acceptance test, all of the safety functions provided (e.g. maintaining limit values, functions of command transmitters/sensors, functions of actuators) must be carefully checked. With this test, the complete fault response chain - from the sensor through the control up to the actuator - is run-through and the safety functions carefully checked in order to ensure that they operate correctly. This applies for all electric drive systems in machines. For a partial acceptance test, only the safety-related parameters must be tested that were changed with respect to the complete acceptance test, or have been added.

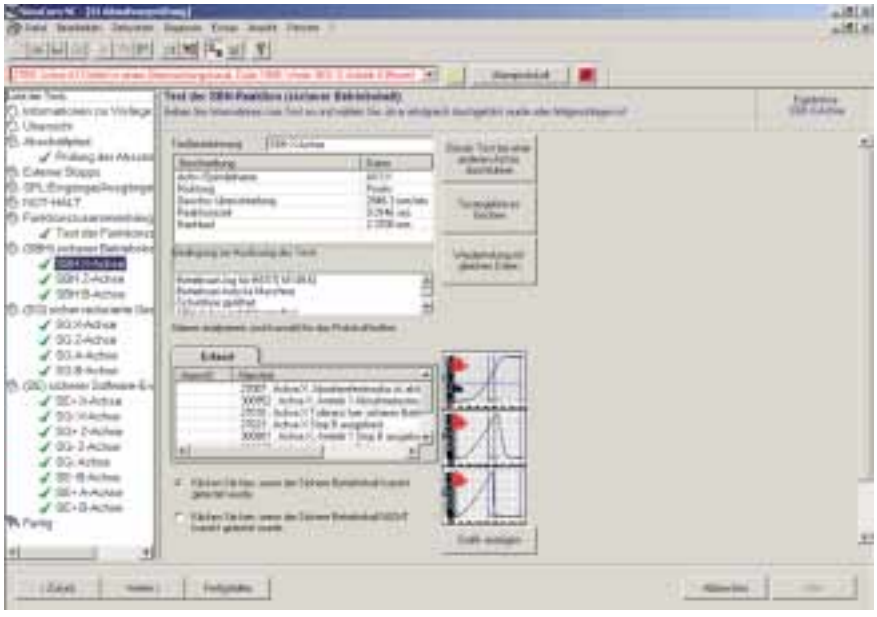


Fig. 8/18
Acceptance test for the safe operating stop

With the integrated acceptance test, the machinery construction OEM has an operator prompted tool that can be used semi-automatically carry out this test. In so doing, the required trace functions are automatically configured. The automatically generated acceptance test report certifies the tested functional safety of the machine – both for the machinery construction OEM as well as the end user actually operating the machines. The time saving that can be achieved with a prompted acceptance test is quite significant.

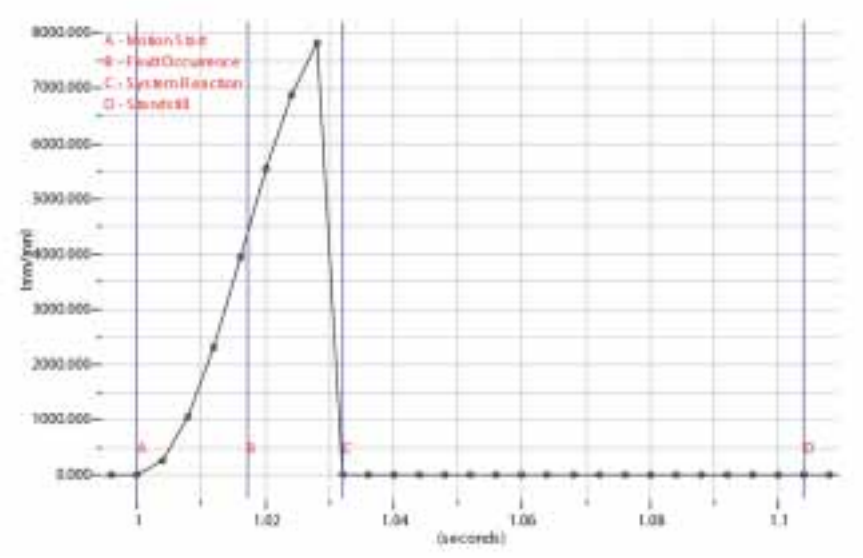


Fig. 8/19
Setpoint velocity

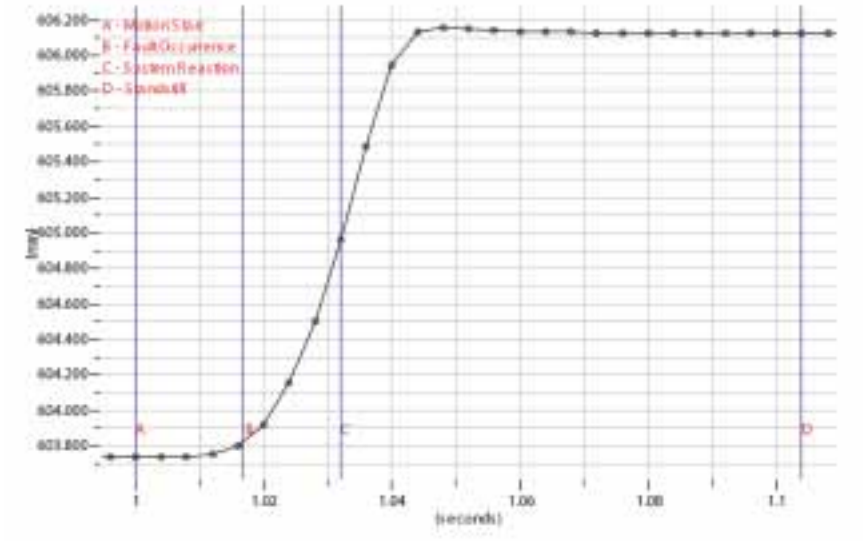


Fig. 8/20
Actual position

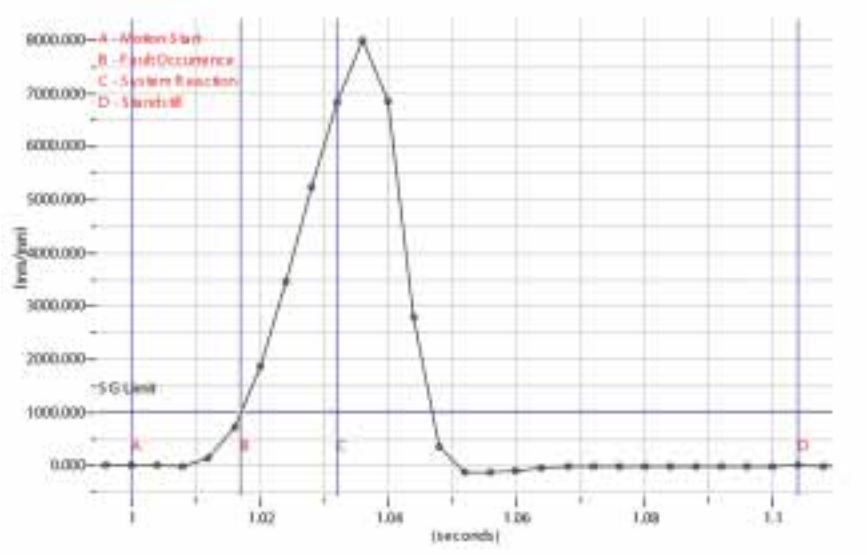
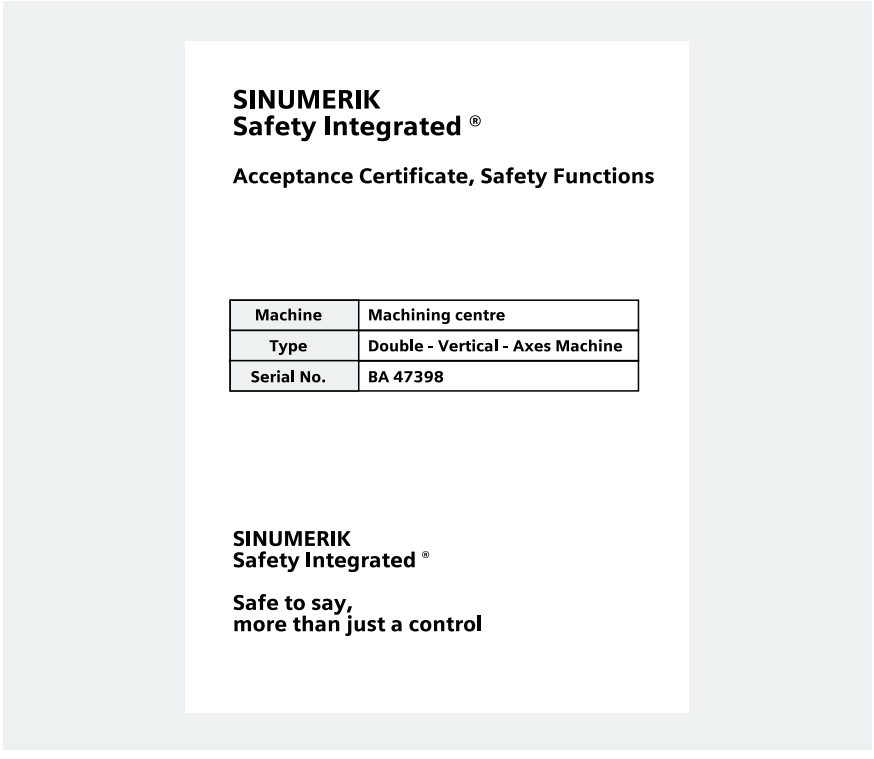


Fig. 8/21
Actual velocity



SINUMERIK
Safety Integrated ®

Acceptance Certificate, Safety Functions

Machine	**Machining centre**
Type	**Double - Vertical - Axes Machine**
Serial No.	**BA 47398**

SINUMERIK
Safety Integrated ®

Safe to say,
more than just a control

Fig. 8/22
Acceptance test certificate

Forced checking procedure for SINUMERIK Safety Integrated

The forced checking procedure is used to detect faults in the software and hardware of the two monitoring channels. In this case, the safety-related components in the two channels must be processed at least once within a defined time period and in all safety-related branches. A fault in a monitoring channel results in deviations and is detected by the crosswise data and result comparison.

The user must initiate the forced checking procedure of the shutdown path (test stop) or it must be automatically integrated into the process - for example:

- With the axes stationary after powering-up the system
- When opening the protective door
- In a specified cycle (e.g. every 8 hours)
- In the automatic mode - dependent on the time and the event

The forced checking procedure also includes testing safety-related sensors and actuators. In this case, the complete signal chain, including the “safe programmable logic” is checked to ensure that it is functioning correctly.

Comment:

For the duration of automatic operation (with the protective door closed), the fixed 8-hour cycle isn't mandatory. In this case, the forced checking procedure can be logically combined, after 8 hours have expired, the next time that the protective door is opened. As a result of the crosswise comparison, errors are detected in the safety-related data of the two monitoring channels. For “changing” data, there are tolerance values specified by the machine data. The results of the two channels can deviate within these tolerances without a response being initiated. An example is the tolerance for crosswise comparison of the actual positions. Faults that are detected due to the forced checking procedure and the crosswise data comparison result in a stop F response and this initiates additional strop responses (refer to the section “Stop responses”).

Connecting sensors/actuators - basics

In order to integrate sensors and actuators in a safety-related fashion, their process signals must be fed to the “safe programmable logic” SPL for further processing.

The following connection types are available:

1. Via separate PLC and NC hardware in degree of protection IP20

2. Via PROFIsafe with the ET 200S-PROFIsafe I/O modules with degree of protection IP20

3. Via PROFIsafe as direct, safe communications with a safety-related PROFIsafe sensor / actuator

This applies for process signals from:

- Sensors, e.g. switches, protective door contacts, Emergency Stop pushbuttons, light curtains, laser scanners

- Actuators, e.g. load contactors, valves, interlocking solenoids, brakes

These are directly connected without using any external evaluation devices and transferred to the “SINUMERIK Safety Integrated” platform.

Comments regarding the mechanical sensor design

A differentiation should be made between the following cases:

1. The sensor (e.g. protective door interlocking) is a safety-related component and is certified. This means that faults can be excluded - and no additional measures are required.

2. The sensor is an operationally-proven component acc. to EN 954-2. Faults can be excluded under the following conditions:

   - Regular maintenance is carried-out according to the manufacturer's specifications

   - Sensors are regularly replaced after the product lifetime has expired

   - Faults are detected by the downstream electronics and cyclic tests as a result of updates carried-out by the process (e.g. protective door), or as a result of the forced-checking procedure.

3. The sensor is not an operationally-proven component acc. to EN 954-2. A fault cannot be excluded.

   - The two elements issuing the signal (e.g. switching contacts of a pushbutton) of the sensor must be mechanically de-coupled – or two separate sensors are used.

   - Faults are detected using the downstream electronics with cyclic tests using dynamic update by the process (e.g. protective door), or using a forced checking procedure.

Comments on the mechanical actuator design

A differentiation should be made between the following cases:

4. The actuator (e.g. safety-related motor starter) is a safety component and has been certified. This means that a fault situation can be excluded - no additional measures are required.

5. The actuator is a component, which has been well-proven in operation, in accordance with EN 954-2 (e.g. a valve)
   A fault can be excluded under the following conditions:

   - Regular maintenance is carried-out according to the manufacturer's specifications
   - An actuator is replaced after its product lifetime has expired
   - Faults are detected using the feedback signal from the process and cyclic tests using dynamic updates by the process or the forced-checking procedure.

6. The actuator is a standard component
   Faults cannot be excluded.

   - Two separate mechanically de-coupled actuators are required.
   - Faults are detected using the feedback signal from the process and cyclic tests using dynamic updates by the process or the forced-checking procedure.

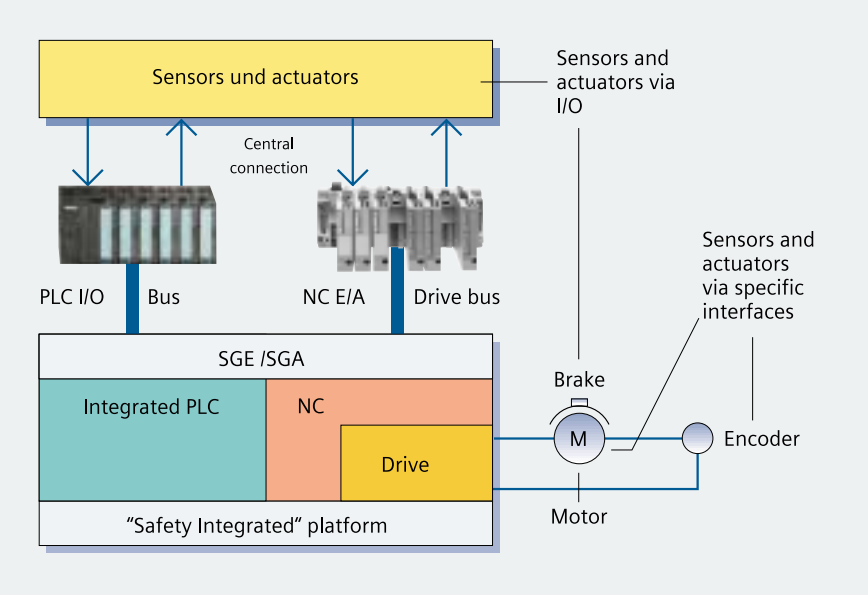


Fig. 8/23
Connecting sensors/actuators through S7 I/O and the DMP module of the NC

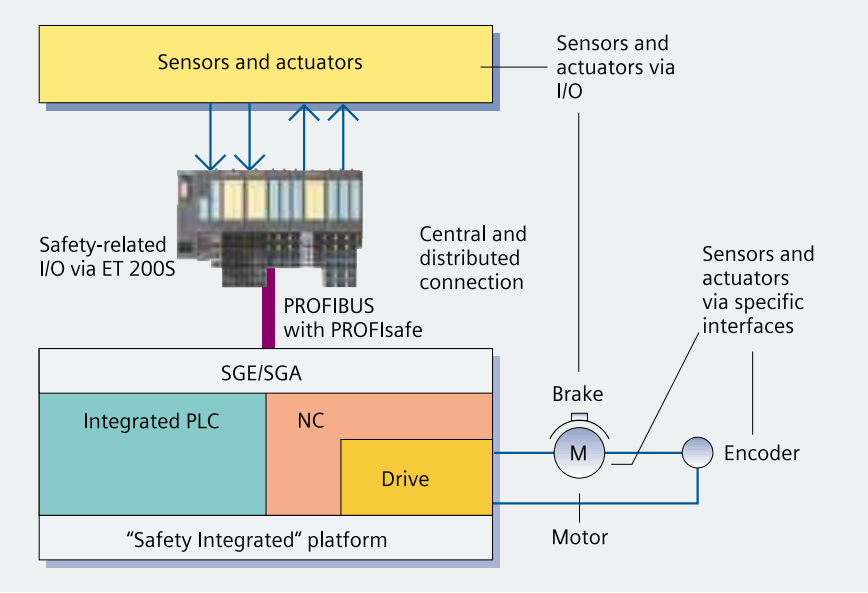


Fig. 8/24
Connecting sensors/actuators through ET 200S PROFIsafe

Connecting sensors/actuators via separate hardware I/O from the PLC and NC

Basic structure

The sensors and actuators are directly coupled to the standard I/O modules of the PLC and NC without using any external evaluation units. The signals are then available to the "SINUMERIK Safety Integrated" platform via separate buses. The 2-from-2 evaluation technique is always used when connecting sensors.

Features

- Standard I/O modules
- Separate hardware channels
- Separate busses

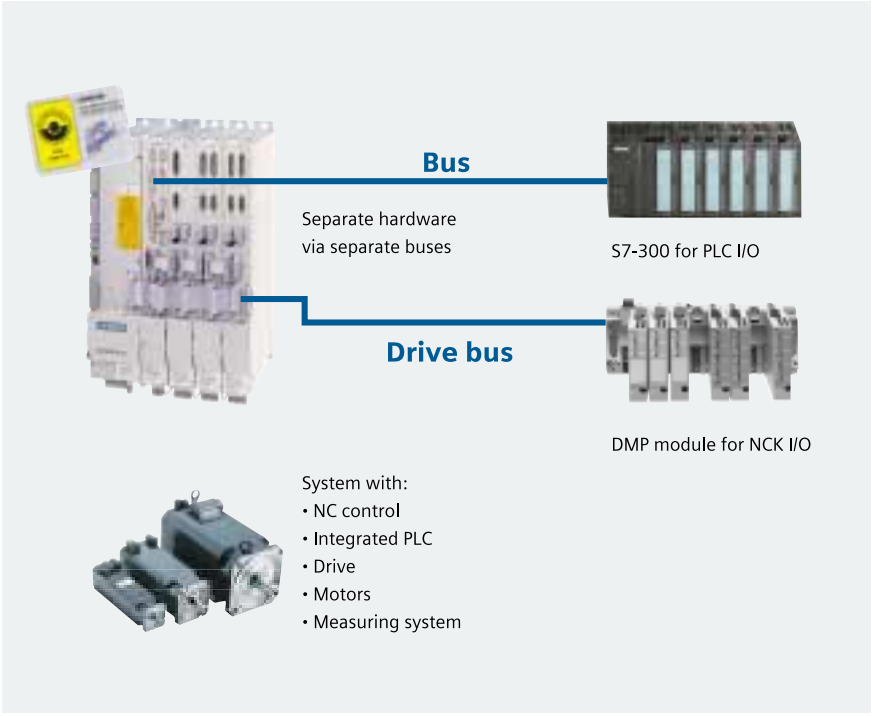


Fig. 8/25
Connecting sensors/actuators through S7 I/O and the DMP module of the NC

Connecting sensors/actuators according to the 3 terminal concept

Connecting sensors

For sensors that are connected via the I/O of the PLC and NC, a 3-terminal concept can be used as basis. If the signals are read-out from a sensor through 2 channels then a 1-channel test output for control Category 3 is sufficient. Thus, to connect the sensor in a safety-related fashion, three terminals at the I/O periphery are required.

2 inputs + 1 test output

Connecting actuators

For actuators that are connected through the I/O of the PLC and NC, a 3-terminal concept can also be used as basis. If an actuator is controlled through 2 channels, then for control Category 3 it is sufficient to read-back the process signal through one channel. This means that 3 terminals are also required at the I/O peripherals in order to connect the actuator in a safety-related fashion.

2 outputs + 1 test input

Cross-circuit fault safety

If the connecting cables are routed, protected in the cabinet or parts of the system, then it can be assumed that faults are extremely improbable (short-circuit, cross-circuit,...). As defined in EN 954-2, so-called fault exclusion can be assumed for the connecting cable. This means that it is completely sufficient to configure the sensor according to the 3-terminal concept.

The measures applied for cross-circuit fault safety are independent of the control category (3 or 4).

Safety-related hardware input signals

All safety-related process signals (sensors such as e.g. Emergency Stop, protective door, light curtain, ...) must be provided redundantly and connected separately as "safety-related inputs" (SGE) to the 2-channel PLC and NC I/O. In this case, it is not permissible that the input terminals are directly jumpered.

Application example: Emergency Stop

Features

- The sensor is controlled with 24 V from a PLC test output through a common connection and fed to the safety-related control via the two input channels 1 and 2.
- In conjunction with the crosswise data comparison and the forced checking procedure, faults (P and M short circuit) can be detected in the connecting cables.
- A pure cross-circuit fault between the two inputs of channel and 1 and 2 cannot be detected using the 3-terminal concept.

It must be ensured that the signal state of the "safety-related inputs" does not differ. Depending on the tolerance timer (approx. < 1 sec.) when the tolerance time is exceeded, a monitoring function responds and the machine is automatically shut down.

Comment 1:

For sensors that offer just pure electronic outputs - i.e. no contacts - that to some extent is possible for light curtains - the external circuit at the PLC and NC inputs remains the same. However, the test output of the PLC is directly connected to the special test input at the sensor. The 3-terminal concept is essentially kept.

Comment 2:

If a safety component (e.g. Emergency Stop button) is not used as sensor, then the two signal-generating elements (e.g. switching contacts for a pushbutton) must be mechanically de-coupled.

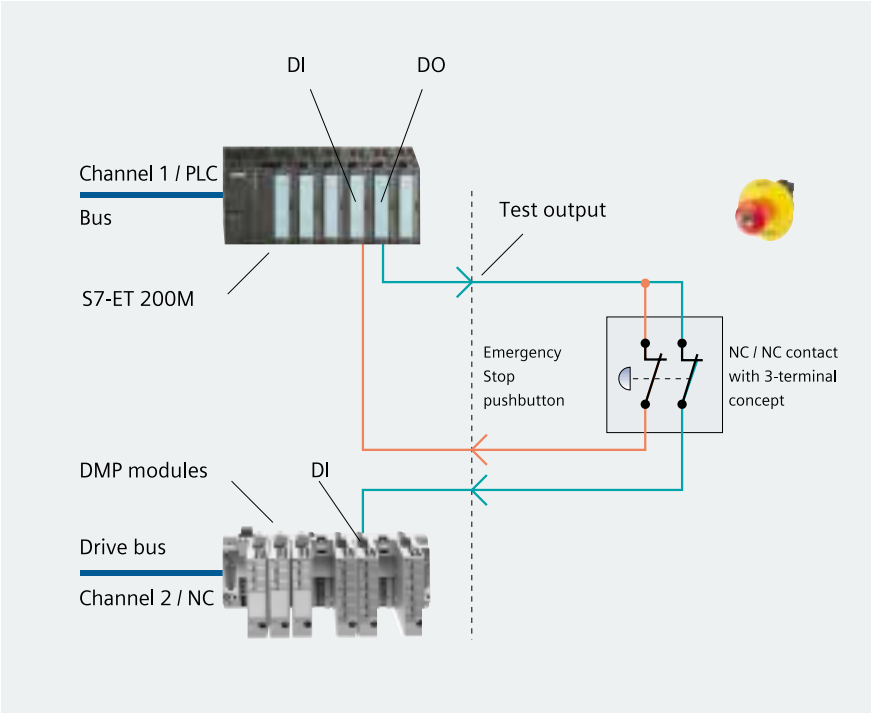


Fig. 8/26
Connecting sensors using the 3-terminal concept – using Emergency Stop as an example

Connecting sensors acc. to the 4-terminal concept

If connecting cables cannot be completely protected against crushing (e.g. cables used to connect handheld/ programming terminals), or if higher requirements apply as a result of the application, then a pure cross-circuit (no P or M short-circuit) must be assumed in the hazard analysis. This means that the sensor must be connected using the 4-terminal concept. In this case, two separate cables are connected to the two signal-generating elements (e.g. contacts). 4 terminals are required at the I/O periphery to integrate the sensor in a safety-related fashion.

2 inputs + 2 test outputs

Cross-circuit fault safety

Using this technique, with standard modules, it is possible to implement complete fault detection functionality for the sensor connecting cables. The connecting cables do not have to be routed in any special way.

Safety-related hardware input signals

The basic principle corresponds to that of the 3-terminal concept. The extended measures are designed to detect a pure cross-circuit fault (i.e. no connection to M or P potential) between the two cables.

Application example: Emergency Stop

Features

- The sensor is directly controlled with 24 V from each of the 2 PLC test outputs and fed to the safety-related control via the two input channels 1 and 2.
- Test output 1 is delayed by tx with respect to test output 2. The expected response is a clear, unique signal characteristic at input channels 1/2.
- A 1-channel test routine in the PLC tests this expected response. This test can be carried-out as part of the forced checking procedure.
- In conjunction with the crosswise data comparison and the forced checking procedure, all faults (P and M short-circuit) incl. a pure cross-circuit fault can be detected in the connecting cables.

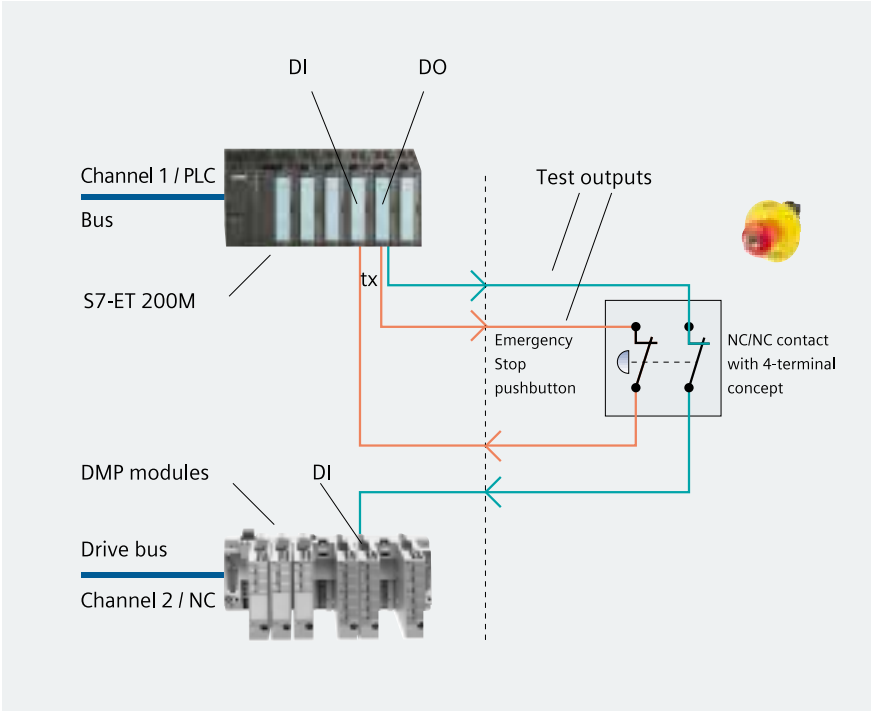


Fig. 8/27
Connecting sensors using the 4-terminal concept – using Emergency Stop as an example

Comment 1:

The concept presented here can only be used with sensors using contacts and in closed circuits (closed-circuit principle). For electronic signals, the sensor must implement the cable monitoring function.

Comment 2:

If a safety component (e.g. Emergency Stop button) is not used as sensor, then the two signal-generating elements (e.g. switching contacts for a pushbutton) must be mechanically de-coupled.

Safety-related hardware output signals - P/P switching

For P/P switching versions, two actuators are always switched in series in the load circuit. Both channels (NC and PLC) control the actuators with a positive potential (24 V) (positive-positive switching). Commercially available contactors with positively-driven feedback signal contacts can be used, for example to control motors.

The feedback signal from the load circuit should be derived as directly as possible from the process quantity. For example, a direct feedback signal of the hydraulic pressure supplied from a pressure sensor or a feedback signal from the moved mechanical system (endstop) using a Bero is preferred over an indirect feedback signal from the hydraulic valve.

Application example: 400 V load voltage

- Safely shutting down the 400 V load voltage of standard induction-motors
- Safely shutting down the 400 V load voltage of distributed units

Features

- The load circuit is always controlled through 2 channels
- The actuator is available twice - this means that the load is always interrupted or connected through 2 channels
- Commercially available (standard) components can be used as actuators - e.g. contactors, valves etc.; the reason for this is that two devices are always used.
- The positively-driven feedback signal contacts (NC contacts) of the actuators are permanently at 24 V, are connected in series, and are read-back from the PLC through one channel.
- In conjunction with the forced checking procedure, faults in the control and at both actuators can be detected.
- When an actuator fails, the load can be still be shut down using the second channel
- It is only possible to switch the actuator through 1-channel, as a function of the process, via the PLC.

Safety-related hardware output signals – P/M switching

For P/M switching versions, only a single actuator is used to control the load circuit. The NC channel controls the actuator with a positive voltage (24 V); the PLC channel controls the actuator with a negative potential (0 V) (positive-negative switching). This control

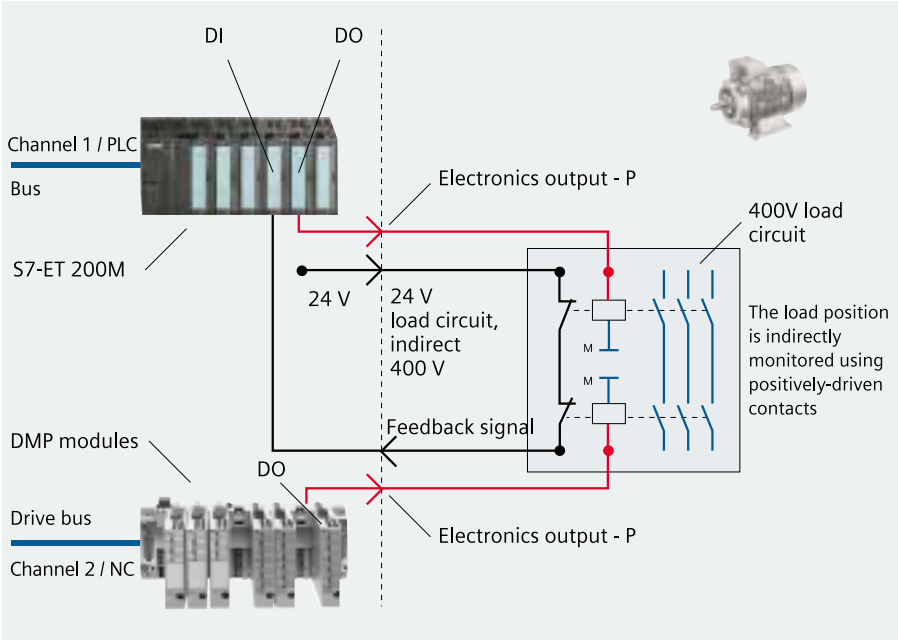


Fig. 8/28
400 V load circuit – P/P switching – example of a standard asynchronous motor

version is always required if there is only one solenoid to directly control the load circuit. This is, for example, the case for:

- Tumbler solenoids at protective doors
- Holding brakes integrated in the motor
- Operating brakes hydraulically controlled through valves (e.g. for linear motors)

The feedback signal from the load circuit should be derived as directly as possible from the process quantities. For example, a direct feedback signal of the hydraulic pressure from a pressure sensor or a feedback signal of the moved mechanical system (endstop) using a Bero is preferred over an indirect feedback signal from the hydraulic valve. If there is only one actuator in the load circuit, as is the case here, then additional measures are required, for example, the actuator must be subject to a cyclic function test.

Comment:

If there is no feedback signal contact available, then it is possible to proceed as described in the application example “safe brake control – P/M switching”.

- In conjunction with the forced checking procedure, faults can be detected in the control and at the actuator
- If the actuator fails, then the load can no longer be safely shut down using the specific path. In this case, depending on the hazardous analysis and the actuator design, additional measures must be applied; these can include, e.g. central shutdown and extended test measures.
- The actuator can be solely switched via the PLC through a single channel, depending on the process.

Application example: Safety-related brake control – P/M switching

The basic principle is described in the Section “Safety-related hardware output signals – P/M switching”.

The “safe brake control” is part of the “safe brake management” function.

For a description, refer to the “protection against vertical axes dropping".

Features

- The load circuit is always controlled through two channels.
- The brake as actuator is only available once. In this case, the process quantity - the braking torque - is only applied through 1 channel.
- The feedback signal is generated from the solenoid coil connection on the ground side. This means that M short circuits and P short circuits can also be safely detected and the 3-terminal concept can also be used here.
- The electronics output - P is switched, with delay tx with respect to the relay output - M. This results, as expected response, in a unique signal characteristic at the feedback signal input.
- A 1-channel test routine in the PLC checks this expected response and this can be carried-out as part of the forced checking procedure.
- A safety-related brake test is provided as extended test measure. This test checks the braking torque that is actually available. This function is available with the safe brake management" function. The braking torque test is incorporated in the forced checking procedure for the test stop (testing the shutdown paths).
- When the power fails or a cable is interrupted, then the safe brake state is automatically and mechanically assumed using the return springs.
- Only operationally-proven components according to EN 954-2 may be used as actuators.

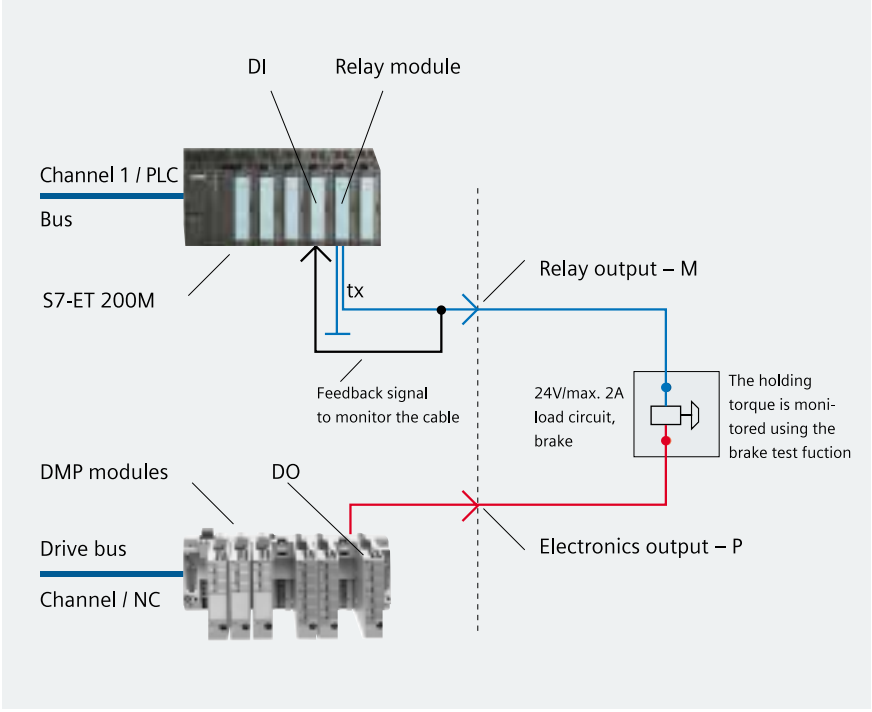


Fig. 8/29
24 V load circuit – P/M switching – an example using safe brake control

Safety-related hardware output signals – P/M switching with intermediate relay stage

With this example, contrary to the previously described direct P/M switching version, the load circuit is controlled through an additional intermediate relay stage to amplify the current. The intermediate relay stage must be used if there is no 2 A output module of the NC I/O and/or no S7 relay module available or if the load current to be switched is > 2 A.

The outputs used in the NC and PLC are standard outputs where the intermediate relay stage is switched P/P.

Caution!

When using the intermediate relay stage, when compared to the best case (fast, contact-free NC path switching), the response time is extended by the relay switching time. This results in longer response times which in turn means that the axes drop further (sag) when faults develop.

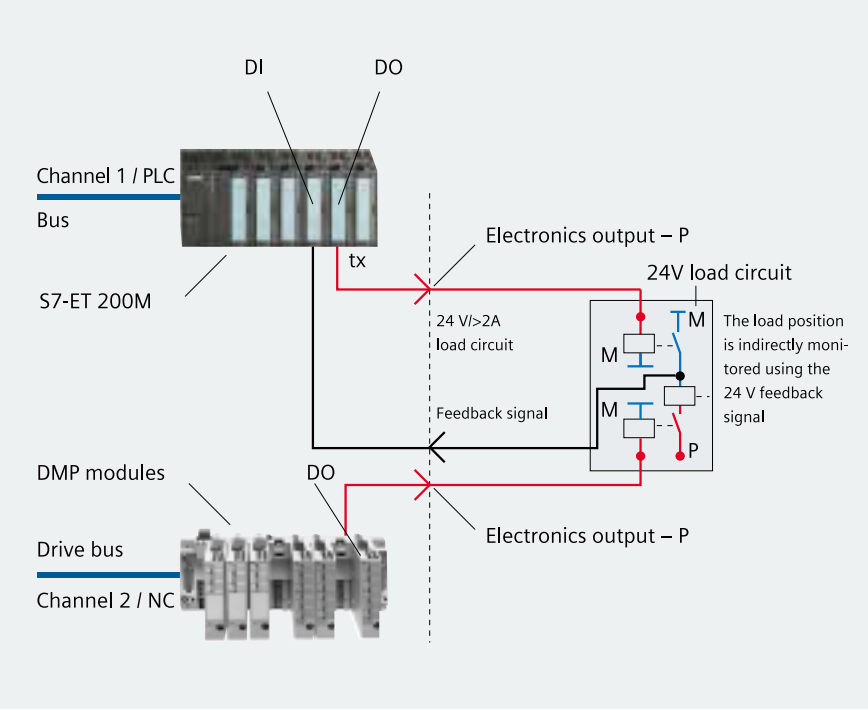


Fig. 8/30
24 V load circuit – P/M switching with intermediate relay stage for > 2 A

Application example: 24 V load voltage > 2 A

- Load power supply from distributed units with > 2 A
- Brakes with > 2 A

Features

- Principally, the same features apply as for the direct P/M switching control.
- The control in the 24 V load circuit remains as already shown in Fig. 8/30: "24 V load circuit – P/M switching up to 2 A and up to 10A" - P/M switching.
- It is not absolutely necessary to incorporate the positively-driven feedback signal contacts of the intermediate relay stage. This means that standard relays can be used without positively-driven feedback signal contacts. However, in this case, the direct feedback signal from the M potential of the load circuit must be directly connected.
- Incorrect functions in the load circuit path are detected by the direct feedback signal from the M potential, e.g.
  – When the relay does not switch/drop-out (e.g. due to welded contacts, relay contacts caught)
  – Short-circuits on the 24 V control lines and the load circuit.

Connecting sensors/actuators via ET 200S PROFIsafe fail-safe modules

Basic structure

The sensors and actuators are directly connected, without any external evaluation units, to the safe inputs and outputs of the ET 200S PROFIsafe. The signals are then available to the "SINUMERIK Safety Integrated" platform through safe communications with PROFIsafe. It is far easier to connect sensors and actuators by using ET 200S PROFIsafe.

It is:

- Simpler to install
- Modular design
- Higher degree of flexibility
- More transparently documented

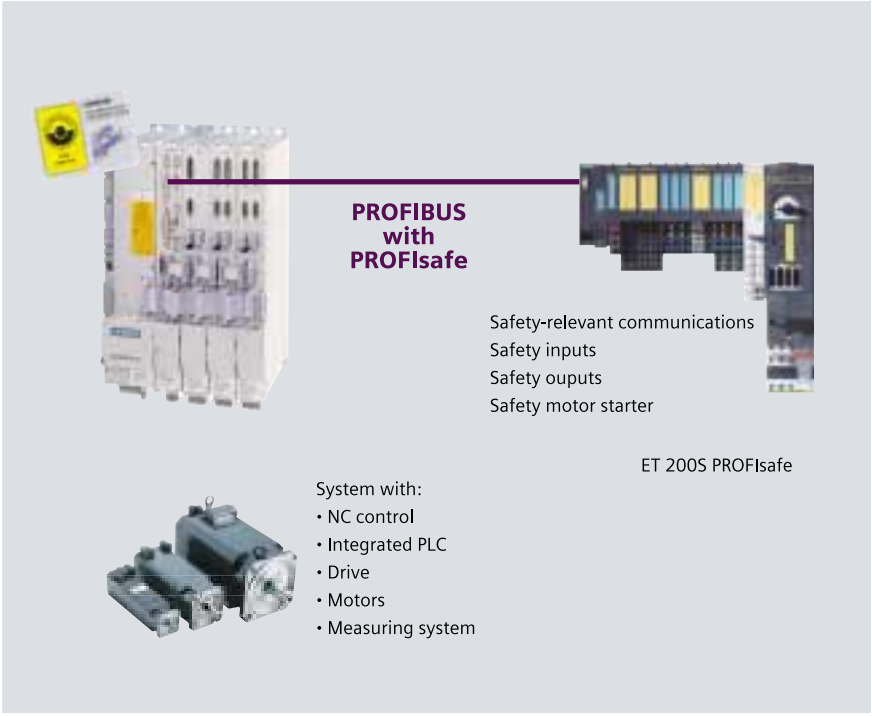


Fig. 8/31
Connecting sensors/actuators through ET 200S PROFIsafe

Features

- Fail-safe ET 200S modules for F-DI inputs, for F-DO outputs and for group shutdown operations using the PM-E F power module
- Safety-related communications via PROFIBUS-DP using the PROFIsafe Profile
- Standard configuration concept where for control Category 3 safety-related and non-safety-relevant modules can be mixed
- Safety-related motor starters via the PM-D F power module with 6 load groups
- Distributed Safety engineering tool from SIMATIC S7

For some examples for connecting sensors/ actuators via the fail-safe modules of the ET 200S PROFIsafe, refer to Chapter "Connecting sensors/ actuators".

Application examples

- Setting-up operation with the protective door open
  When the protective door is open, the feed or spindle drives can be operated at a safely-reduced speed or can be safely monitored for stand-still. This means that the drives can always be controlled and monitored by the electronics and do not have to be disconnected from the power supply. Working and protective areas can be implemented using safety-related technology including functions for area identification and limiting areas of movement. In conjunction with SINUMERIK Safety Integrated, it isn't mandatory that an agreement button is used. However, depending on the requirement, e.g. to change over safety functions, it can be used. For standard applications, the drives may only be moved using the jog keys in deadman operation*.

- Test operation with the protective door open
  For the first time, program test operation is possible where the complete programs or program sections are executed with safely-reduced speed in a “dry run”. Here, the operator allows the program to be continually run by pressing a button - generally the start button.
  If the operator identifies a program error during the test, then he can stop the program by releasing the start button or by pressing the Emergency Stop. The safety functions are also active during this test phase. When the limit values are violated, they respond and automatically stop the drives.

- Integrated, contactless Emergency Stop
  The two contacts of the Emergency Stop button can be directly connected to the redundant PLC and NC I/O without having to use any additional evaluation logic. The two contacts can also be connected to the fail-safe ET 200S PROFIsafe input modules. The logical operations and the required responses are internally implemented using safety-related technology. The electric drives are safely stopped and are then contactlessly disconnected from the power source using electronic measures. Restart is safely prevented. External power sources - e.g. hydraulic or laser systems, etc. - can be shut down using safety-related technology via the redundant or fail-safe outputs from the integrated Emergency Stop logic and downstream actuators (power contactors, valves, ...).

Certification

The Safety Integrated functions that have been described have been certified in compliance with DIN V VDE 0801, EN 954-1 and EN 60204 since 1996.

The Safety Integrated functions that have been described have been certified acc. to EN 954-1 (Category 3) and IEC 61508 (SIL 2), they have also been NRTL listed.

* Deadman operation

This term originally comes from the railways.

Significance: The function only remains effective as long as the actuating element (button) is pressed. If the actuation element is released, the function is interrupted and the potentially hazardous motion is stopped.

8.2 Safety Unit

The safety package for metal forming technology

Measures have to be applied to all production machines - especially on presses - to protect the operating personnel. These measures eliminate any potential hazards in the operating process. This can be realized by securing machines using protective doors or light grids. However, if operators must frequently intervene in the operational production process, then the machine responses must be monitored, e.g. using speed monitoring functions. This avoids hazardous machine motion for fault-related failures at the control and mechanical system.

The Safety Unit TM 121 was developed to cover such requirements.

It has been designed so that the following safety requirements are fulfilled:

- EN 954-1 safety-related parts of controls.
  Here, the unit is in compliance with Category 4.

- IEC 61508 Functional Safety of electrical/electronic/programmable safety-related systems
  In this case, the unit is in compliance with SIL 3.

- EN 61496 Safety of Machinery, contactless (electro-sensitive) protective devices and equipment

Fig. 8/32
Safety Unit TM 121C

Redundant (two-channel) electronic processor system with:

32 safety-related inputs, 24 V
8 safety-related outputs, 24 V, 2 A
8 standard outputs, 24 V, 0.5 A
2 safety frequency inputs, 24 V, 500 Hz

Supply:
24V DC

Mechanical strength:
Fulfills a higher degree of severity regarding mechanical load/stress in compliance with EN 61496

Fig. 8/33
Safety Unit – technical data

Excerpts from this have been taken into account, i.e. a higher severity level, e.g. for mechanical loads or EMC.

This means that the prerequisites to implement safety functions at the machine, including manually operated presses, are fulfilled and that throughout Europe.

Standard blocks - that are required to provide protection at all types of machines - are permanently saved in the control. These include protective fence and protective door monitoring functions and also Emergency Stop circuits. In addition, special versions have been implemented that are used with certain machine types, such as **mechanical**, **hydraulic** and **edging presses**.

These blocks are interconnected using a parameterizing tool supplied with the equipment.

Example:
Function blocks for mechanical presses

- 2-hand operation
- Safety-related cam inputs (run-up, run-on, transfer)
- Operating mode selection
- Emergency Stop (“switch into a no-voltage condition”), engage inhibit function
- Coupling - braking combinations can be controlled /(with monitoring)
- Protective door / protective grid / light curtain
- Running monitor (via frequency input)

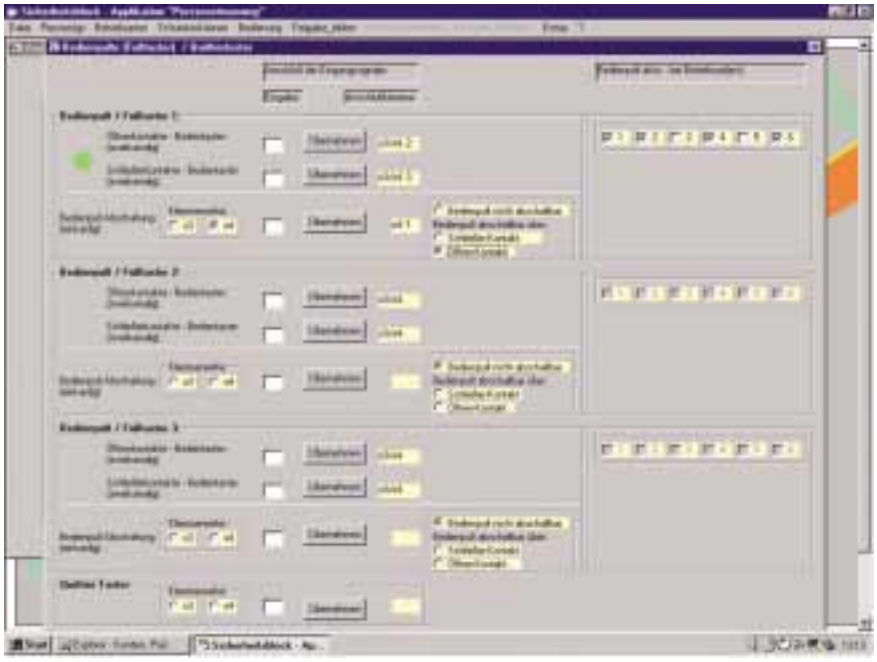


Fig. 8/34
Typical parameterizing software mask

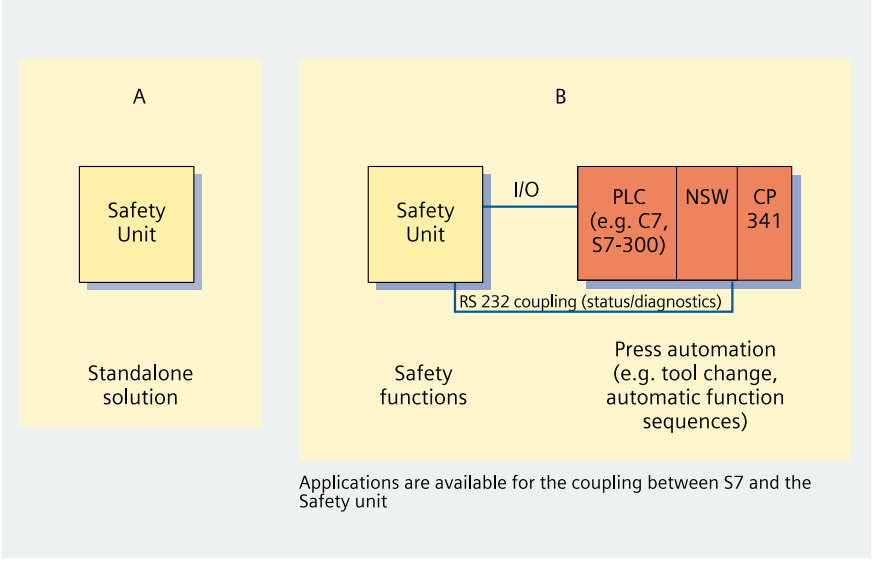


Fig. 8/35
Safety Unit – topology

8.3 Safety Integrated for Motion Control Systems

Our range of services

Overview

Our portfolio of Safety Integrated products is complemented by an extensive range of services. The range of services for machinery construction OEMs and machine operating companies includes:

- **Generating a concept**
  Starting from the hazard analysis and the required operator control philosophy, together with customers, the safety functions are appropriately adapted to the machine.

- **Hardware engineering**
  The safety-related concept is integrated and incorporated in the circuit diagrams. In so doing, safety-related sensors and actuators are selected and their wiring defined.

- **SPL configuring**
  All of the modules and objects necessary for the safe programmable logic (SPL) are generated and these are incorporated in the overall system.

- **Commissioning**
  Starting from the engineering specifications, safety-related functions are commissioned.
  To be able to do this, the customer ensures that with his machine, the drives can be moved and that the electrical cabinet is connected-up corresponding to the engineering specifications.

- **Acceptance test with subsequent acceptance report**
  All of the safety functions are carefully checked corresponding to the requirements. The test results and the measuring diagrams obtained are documented in an acceptance report. For both the machinery construction company as well as the machine operating company, this represents a clear proof of quality regarding the functional safety of the machine.

- **Workshops**
  Workshops on the subject of machine safety are adapted to specific customer requirements, and when requested, can also be carried-out at the customer's site.

- **Hotline**
  If faults or problems occur while commissioning the system, experts on the subject of Safety Integrated can be contacted under the hotline 0180/50 50 222.

- **Inquiry for support**
  You can directly contact our engineers by sending a support inquiry via the Internet.

www.siemens.de/automation/support-request

- **On-site service**
  Experts analyze faults on site.
  The causes are removed and/or a solution concept is drawn-up and when required, implemented.

Benefits

- **Time saving**
  from generating the concept up to accepting the safety-related function.
- **Fast and competent support**
  when problems are encountered during the commissioning phase and when machines develop faults.
- **Know-how can be quickly enhanced**
  thanks to effective know-how transfer of our safety-related solutions.

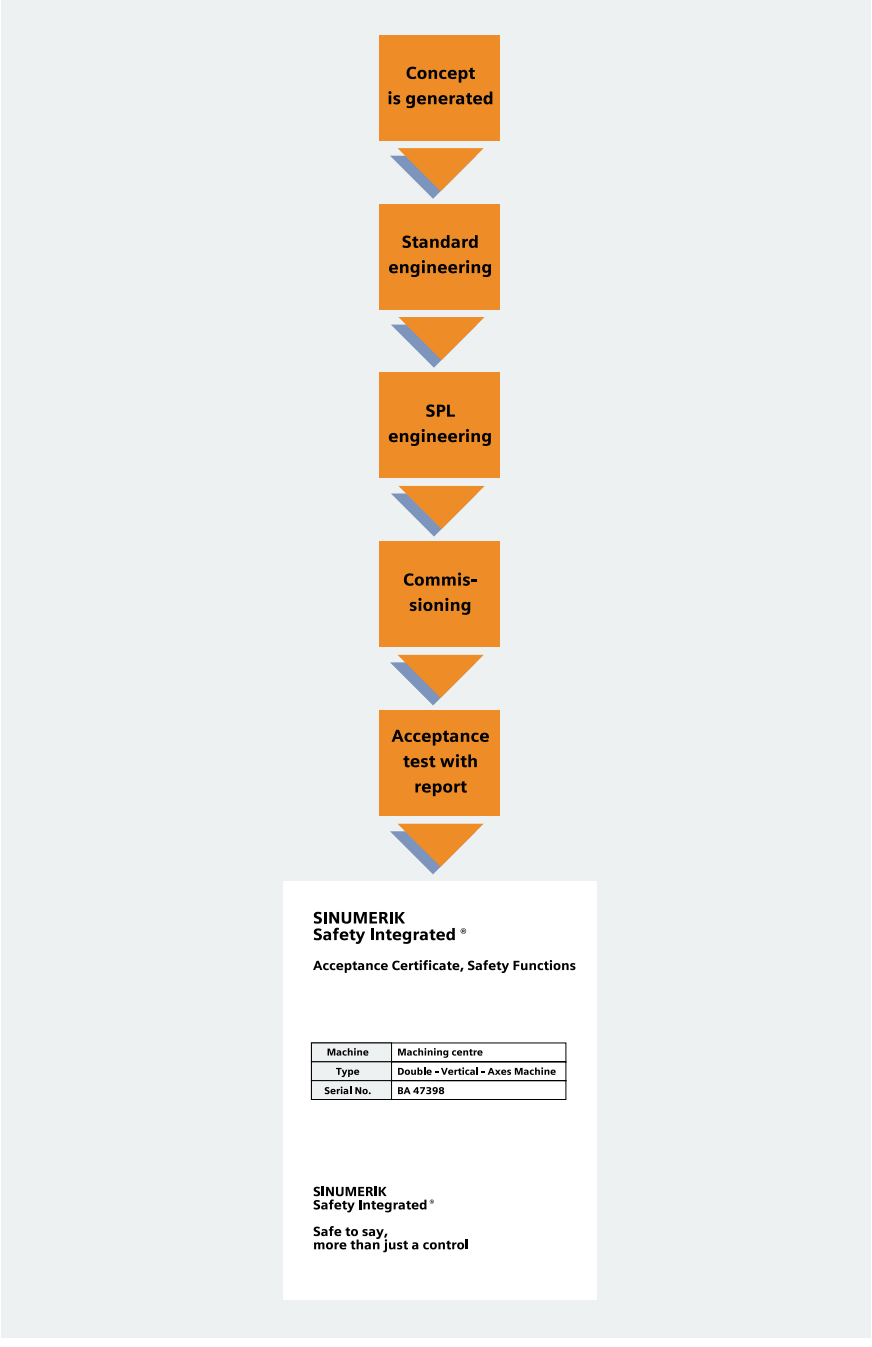


Fig. 8/36
Flowchart of our portfolio of services

Fail-safe drives

9

sinamics

9 Fail-safe drives

9.1 MASTERDRIVES and SIMODRIVE 611 universal

Overview

Measures to set-up machines with isolating, protective equipment and guards in the open condition are available in compliance with most of the European product Standards. The minimum requirement for drives is to avoid unexpected starting.

The SIMOVERT MASTERDRIVES and SIMODRIVE 611 universal drive systems support this requirement in the form of the "safe standstill" function. The function has been certified for Category 3 according to EN 954-1 in the form of a type test carried-out by the appropriate regulatory body. This means that the essential requirements specified in the EC Machinery Directive can be simply and cost-effectively implemented.

Fig. 9/1
SIMOVERT MASTERDRIVES Compact PLUS

Benefits

- **Lower costs:**
  Contactors on the motor side, that today are still often used, can be eliminated. Engineering and wiring costs are reduced and at the same time more space is available in the electrical cabinet.
- **Simple to implement:**
  The safe standstill function can be simply realized as application using defined, external circuitry (e.g. SIRIUS safety relays) and integrated safety relays.
- **Simplified machine acceptance:**
  The circuit principles have been certified and have already been implemented a multiple number of times in practice. This therefore simplifies the acceptance of machines and plants by the appropriate testing institute.

Applications

Thanks to their compact and modular design, SIMOVERT MASTERDRIVES and SIMODRIVE 611 universal drive units offer high performance but at the same time cost-effective drive solutions. They are suitable for many applications - in the area of printing and paper machines, packaging machines, textile machines, plastic machines, machines for metal forming technology or machines for working wood, glass and stone.

"Safe standstill" is used, in conjunction with a machine function or when a fault develops, to internally and safely disconnect the power fed to the motor. "Safe standstill" can also be used when stopping using an Emergency Stop according to stop Category 0 or 1 (acc. to EN 60204-1).

Design

The "safe standstill" function is implemented as application. This is based on safely inhibiting the gating pulses for the power transistors used in the drive. A defined, external circuit ensures, via terminals, that the safety relay integrated in the drive is controlled in a safety-related fashion. This safety relay interrupts the power supply that transfers the pulses in the power module. The switching state of the relay can be externally evaluated via positively-driven contacts.

Fig. 9/2
SIMODRIVE 611 universal

Safe standstill function (SH)

Using the “safe standstill function”, the drive pulses are cancelled and the power feed to the motor disconnected. The drive is in a safety-related no-torque condition. A feedback signal contact is used to display its switching status which means that it can be monitored.

Technical data

SIMOVERT MASTERDRIVES / SIMODRIVE 611universal	
Safety function	• Safe standstill
Safety classes that can be achieved	Up to Category 3 acc. to EN 954-1
Degree of protection	IP20
Control versions	• Closed-loop servo control • Closed-loop vector control (only MASTERDRIVES) • V/f open-loop control (only MASTERDRIVES)
Additional features	• Technology functions • Positioning • Free functional blocks (only MASTERDRIVES)

9.2 SINAMICS Safety Integrated

Safety functions integrated in the drive itself

Overview

The SINAMICS S120 drive system supports the requirement for "avoiding unexpected starting" using integrated safety functions. In addition to the "safe standstill", for the first time, "safe brake control" has also been integrated into the drive. These functions have been certified according to Category 3 (EN 954-1) and SIL 2 (IEC 61508) by the appropriate regulatory body in the form of a prototype test. This means that the essential requirements specified in the EC Machinery Directive can be simply and cost-effectively implemented.

Fig. 9/3
SINAMICS S120

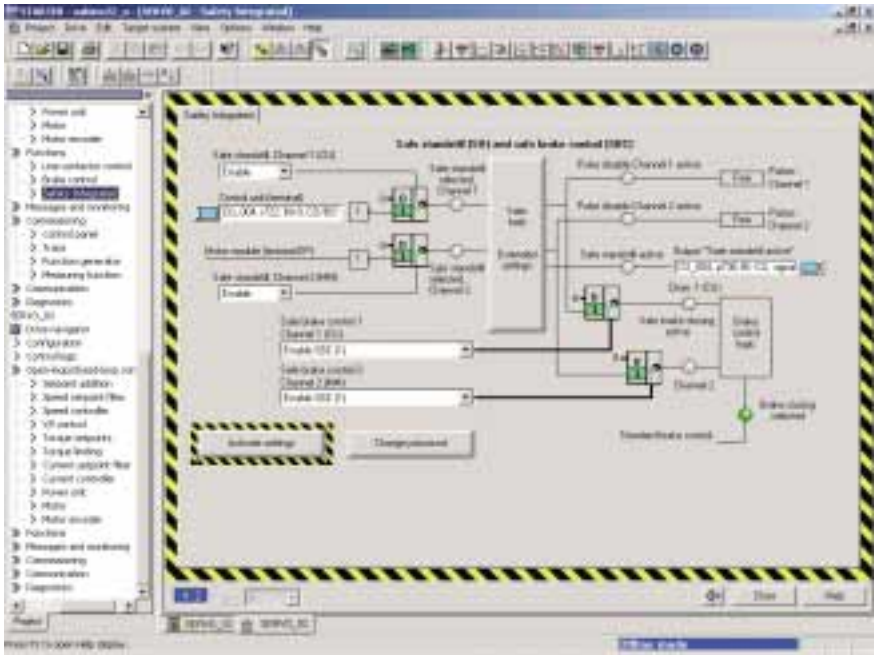


Fig. 9/4
Configuring the safety function

During engineering, commissioning and diagnostics, the "Starter" engineering software supports all of the safety functions.

Benefits

- **Lower costs:**
  In many cases, external switching devices can be eliminated. Integrating the safety technology allows safety concepts to be created in-line with those required in practice and at the same time the installation system is simplified. Not only this, but less space is required in the electrical cabinet.

- **Higher degree of reliability:**
  The functionality has been implemented completely electronically. This means that components with contacts that were used earlier - e.g. integrated safety relays and line contactors - can be eliminated.

- **Simplified machine acceptance:**
  Acceptance of machines and plants by the appropriate testing institute is simplified thanks to certified, integrated safety-related functions.

Applications

As a result of its innovative features and characteristics, SINAMICS S120 is predestined as a drive system in all types of production machines.
For example, printing and paper machines, packaging machines, textile machines, plastic machines, machines for metal forming technology and machines to work wood, glass and stone.

With these applications, the integrated safety functions form the basis to implement safety concepts for machines and plants that are in line with those required in practice.

Design

These safety-related functions are completely integrated in the drive system and have drive-specific interfaces:

- 2 input terminals for "safe standstill"
- 2 output terminals for "safe brake control"

They are implemented using safety-related systems and are completely electronic. This is the reason that they provide short response times. Integrated self-test routines are used to detect faults.

Functions

- **Safe standstill (SH)**
  The "safe standstill" function directly interrupts the power supply for the pulse transfer in the power module. This mean that the drive is safely in a no-torque condition. A feedback signal is not required - however it can be configured using an output or using software. A higher-level, upstream main contactor is no longer required to implement the "safe standstill" function.

- **Safe brake control (SBC)**
  The brake is controlled through two channels - P/M switching (plus/minus). The control cables are monitored when selecting or de-selecting the motor brake.

The control cables used to control the brake can be directly connected to the power module together with the motor cable. The brake may not draw more than 2A.

These functions act on specific drives or groups. This means that one or several safety circuit(s) can be assigned. This in turn increases the plant availability.

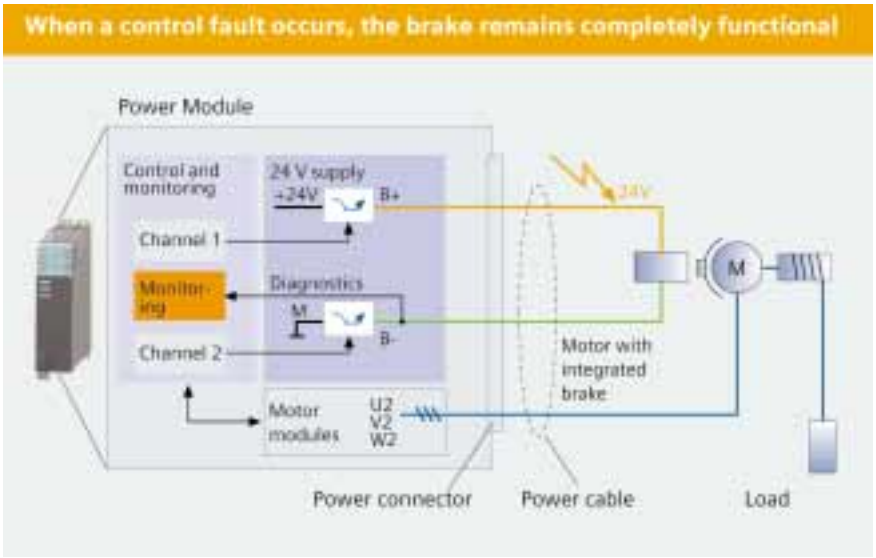


Fig. 9/5
Safe brake control

Technical data

SINAMICS S120	
Safety classes that can be reached	• Up to Category 3 acc. to EN 954-1 • Up to SIL 2 acc. to IEC 61508
Characteristic safety quantities	Characteristic quantities (PFD/PFH values) - not dependent on components, but dependent on the system (values and calculation in the associated product documentation)
Safety functions	• Safe standstill • Safe brake control
Degree of protection	IP20
Additional features	• Modular design • Electronic rating plates • Closed-loop servo control • Closed-loop vector control • V/f open-loop control

9.3 SIMATIC ET 200S FC frequency converters

Overview

The frequency converter supplements the distributed SIMATIC ET 200S I/O system. The SIMATIC ET 200S has a finely modular design comprising components with distributed intelligence, inputs and outputs, motor starters and safety technology. The frequency converters - designated SIMATIC ET 200S FC - continuously control the speed of induction motors. They also solve drive applications using simple open-loop frequency control up to sophisticated closed-loop vector control.

ET 200S FC frequency converters are available in a standard version and in a fail-safe version. In addition to the "safe standstill" the fail-safe frequency converter offers integrated safety functions - "safely reduced speed" and "safe braking ramp". These can also be used for the first time in conjunction with sensorless standard induction motors. All of the safety-related functions have been certified according to Category 3 in compliance with EN 954-1 and SIL 2 in compliance with IEC 61508.

Fig. 9/6
ET200S station with inputs/outputs, motor starters and ET 200S FC frequency converters

Fig. 9/7
ET200S FC fail-safe frequency converters, size B (2.2 kW or 4.0 kW)

ET 200S FC frequency converters are commissioned using "Starter" - a screen-based engineering tool. Starter" also supports the commissioning and diagnostics of the integrated safety functions.

Benefits

- **Flexible solution**
  In an ET 200S station fail-safe and standard components can be operated together. This also applies to frequency converters. This means that flexible solutions that are easy to engineer can be implemented with low hardware costs and for the widest range of drive applications.

- **Lower costs**
  In many cases, external switching devices can be eliminated by using the "safe standstill" function. The integration of safety technology allows safety-relevant concepts to be created in line with those required in practice - and at the same time the installation system is simplified. Not only this, less space is required in the electrical cabinet.

  Up until now, it is also unique in so much that the "safe braking ramp" and the "safely-reduced speed" functions neither require motor encoder nor encoder - and can be implemented with minimum costs.

- **Higher degree of reliability**
  The "safe standstill" is purely electronic without any contacts and therefore ensures the shortest and most reliable response times.

- **Simplified machine acceptance**
  The acceptance of machines and plants by the appropriate testing bodies is simplified thanks to the certified, integrated safety functions

Applications

- In addition to basic drive applications - for instance conveyor belts - the frequency converter also supports applications such as winder and unwinder drives and hoisting gear. When equipped with a motor encoder, the applications extend up to precise closed-loop speed and current control.

- The ET 200S FC frequency converter can regenerate into the line supply. This significantly simplifies applications with permanent regenerative operation. Examples include unwinders, lowering loads in crane applications or electrically braking loads with higher moments of inertia.

- The "safe braking ramp" function allows a drive to be safely stopped and monitored, even when sensorless induction motors are being used. After the drive has been stopped, the drive is prevented from restarting by the "safe standstill" function.

- The "safely reduced speed" allows a drive to be slowly moved in hazardous areas. For instance, when setting-up or loading materials. This function can also be implemented without a motor encoder when standard induction motors are used.

Comment:

The "safe braking ramp" and "safely reduced speed" functions of the SIMATIC ET 200S FC frequency converter may not be used for loads that drive the motor.

Design

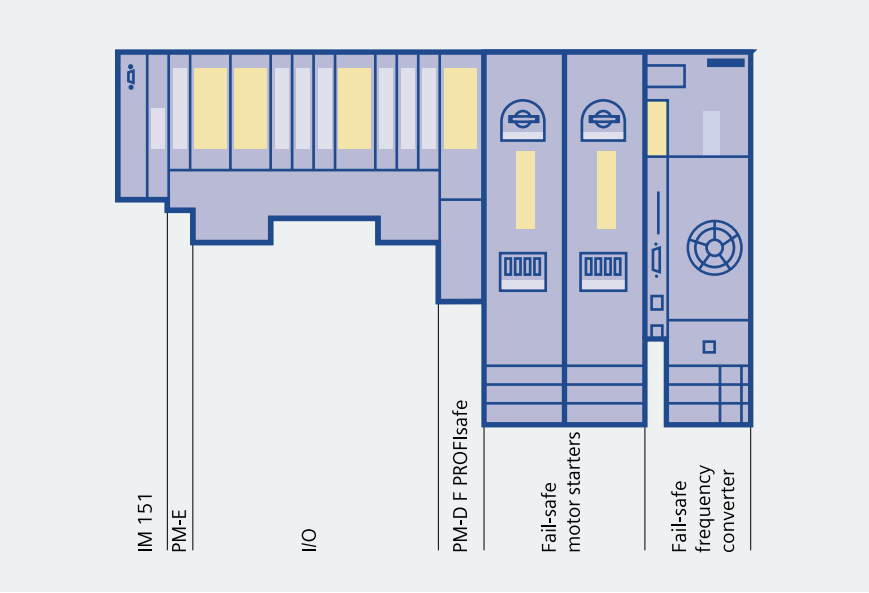


Fig. 9/8
ET 200S station with IM 151, fail-safe and standard inputs/outputs, fail-safe motor starters and frequency converters

The fail-safe ET 200S FC frequency converters comprise the following components:

- ICU24F control module
- IPM25 power unit (this is available in two sizes with power ratings from 0.75 kW, 2.2 kW and 4.0 kW)
- Terminal modules to connect the wiring and to accommodate the control unit and power unit

After the modules have been inserted, the control unit and power unit of the frequency converter are connected with one another.

Functions

- **Safe standstill (SH):** "Safe standstill" interrupts the power supply for the pulse transfer in the power unit and also cancels the pulses. This means that the drive is safely in a no-torque condition and is protected against restarting.

  In addition, when shutting down via the individual shutdown paths, a process update is carried-out by checking the expected status resulting from the particular switching action.

- **Safe braking ramp (SBR):** This monitors the drive while it is stopping. The drive is braked along a selectable ramp. While stopping, a check is continuously made as to whether the actual speed tracks the specified ramp function. "Safe standstill" is activated after a minimum speed has been fallen below (this can be parameterized).

  If the braking function fails, "safe standstill" is immediately initiated and the drive goes into - the fault condition.

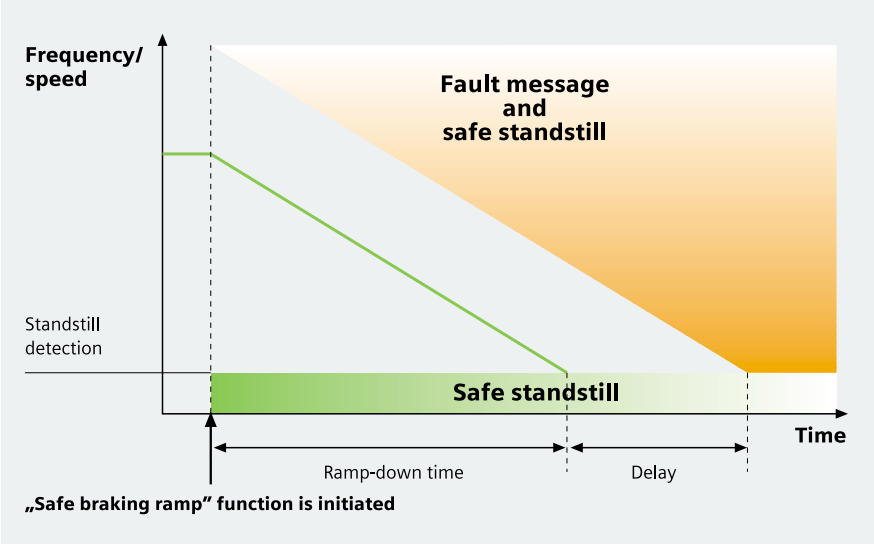


Fig. 9/9
Safe braking ramp of the SIMATIC ET 200S FC frequency converter

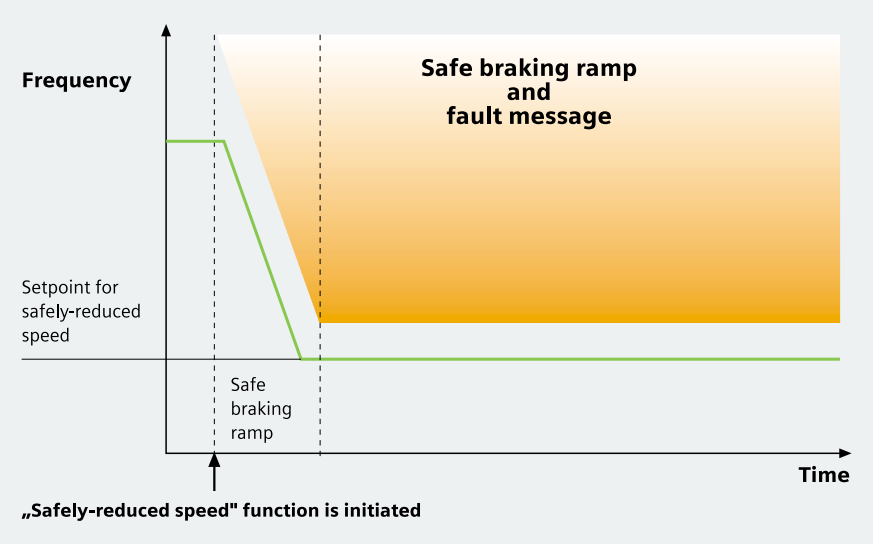


Fig. 9/10
Safely reduced speed of the SIMATIC ET 200S FC frequency converter

- **Safely reduced speed (SG):**
  Monitors the speed against an upper limit value.

  If, when initiating "safely reduced speed", the speed is greater than the safety-related limit value, then the drive speed is initially reduced using the "safe braking ramp". In this case, zero speed is not the target speed, but the safe speed limit value.

  If, when initiating "safely-reduced speed", the speed is less than the safety limit value, the monitoring for the reduced speed limit value immediately becomes active.

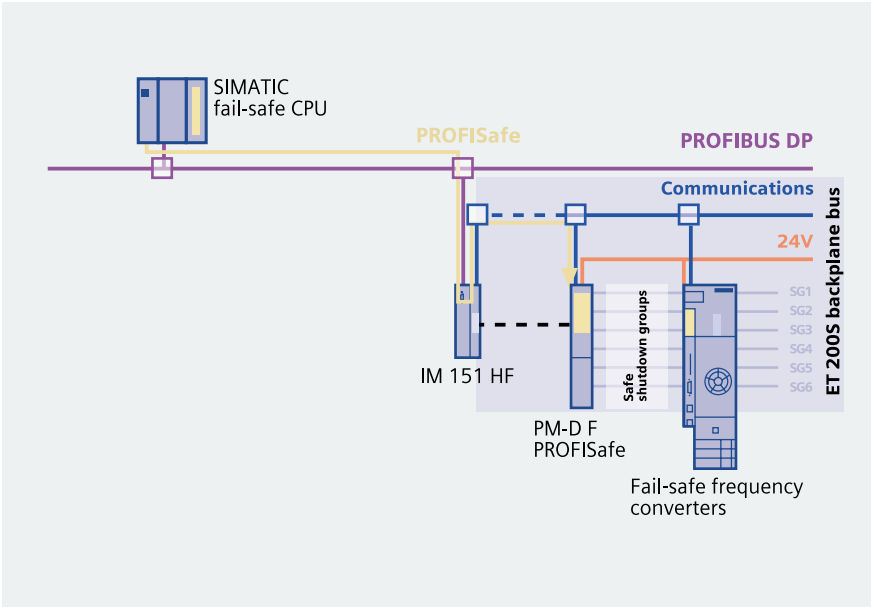
  When the monitoring function responds, the drive is stopped using the "safe braking ramp". The frequency converter then goes into the fault condition.

Integration

The ET 200S FC frequency converter is completely integrated into the ET 200S system and therefore has none of its own inputs and outputs. The converter fail-safe functions are controlled, within the ET 200S, using signals in the backplane bus - more precisely using safety shutdown groups of a PM-D F power module. The frequency converter evaluates two of these shutdown groups via safety-related inputs.

SIMATIC ET 200S provides three basic ways of configuring fail-safe plants/systems - and therefore to control the fail-safe frequency converter functions.

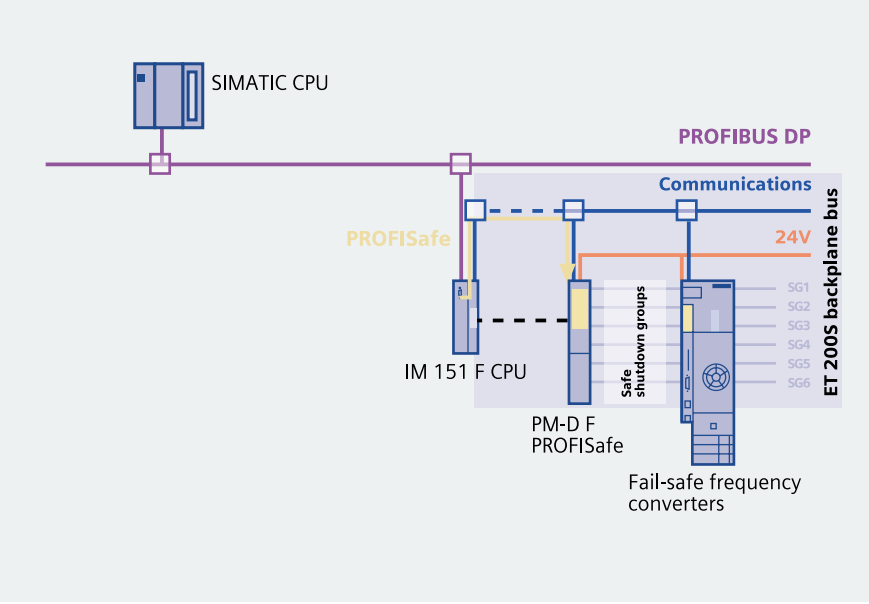
- **Controlling the safety functions via PROFIsafe**



Safety-related signals are evaluated by a central fail-safe CPU and the fail-safe functions of the ET 200S FC frequency converter are controlled via the PM-D F PROFIsafe power module.

The IM 151 High Feature interface module is used to transfer PROFIsafe data communications along the ET 200S backplane bus.

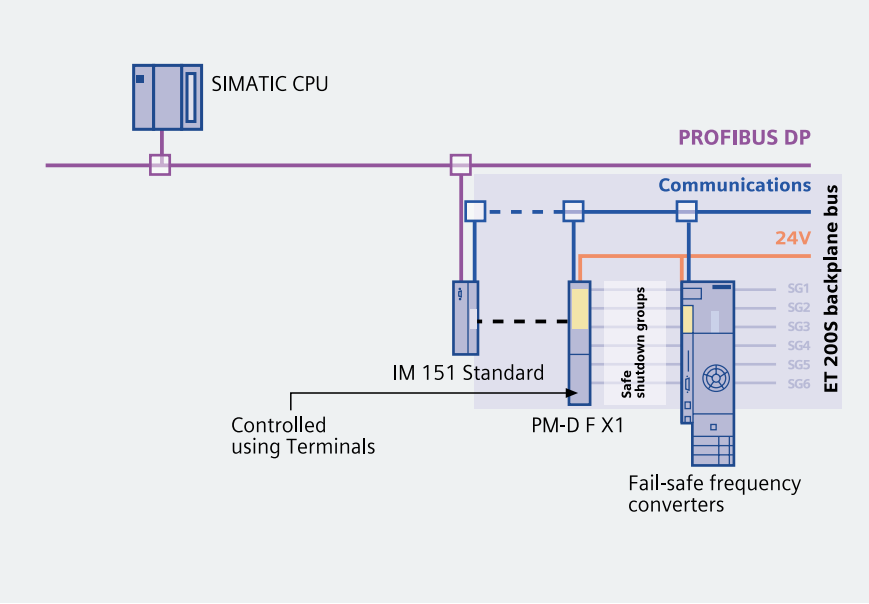
- **Controlling the safety functions using a fail-safe IM 151-7 F-CPU**



An interface module with integrated fail-safe CPU (IM 151-7 F-CPU) permits fail-safe input modules to be evaluated and the frequency converter to be controlled within the ET 200S station. This means that the fastest response times are guaranteed.

A fail-safe central CPU is not required in this configuration

- **Controlling the safety functions directly**



A conventional, local solution to control the safety functions can be implemented using a PM-D F X1 power module.

The shutdown groups are fed directly through the terminals of the PM-D F X1 power module - for example from an external 3TK28 device.

For this solution, any IM 151 interface module can be used. A fail-safe CPU is neither required in the ET 200S nor centrally.

Technical data

Fail-safe SIMATIC ET 200S FC frequency converters	
Safety classes that can be reached	• Up to Category 3 acc. to EN 954-1 • Up to SIL 2 acc. to IEC 61508
Safety functions	• Safe standstill • Safe braking ramp • Safely reduced speed
Degree of protection	IP20
Additional features	• Safety functions for sensorless standard induction motors • Modular design/configuration in the distributed ET 200S I/O • Standard and fail-safe frequency converters can be operated in one station • Fail-safe and standard inputs via an ET 200S station • Regenerative operation with regenerative feedback into the line supply - without chopper or braking resistor • V/f open-loop control • Closed-loop vector control with and without an encoder • Closed-loop torque control

References

10

10 References

10.1 Fail-safe SIMATIC controllers in the body shop of Opel Belgium

For Opel Antwerp/Belgium, recently, the first automation and safety project was implemented based on Safety Integrated with fail-safe Simatic controllers. In addition to the unique Safety Integrated technology of Siemens, decisive for the project success was also the close cooperation between the engineering team of Opel in Antwerp, the system integrator Imtech and Siemens Automation and Drives.

Opel Belgium n.v., an important Opel plant located in the Port of Antwerp and one of the crown jewels of Belgium automobile assembly is presently building various models of the Opel Astra for more than 100 international plants and facilities.

From safety relay to fail-safe control

Francis Luyckx, responsible for engineering at the Opel Belgium body shop, explained the situation before the retrofit: "In the body shop, all of the machine and transport movements (involving robots and conveyors) that could be potential sources of danger, are protected by safety cages, light curtains, safety switches and emergency stop devices. However, all of this, as before is controlled using relay circuits.

“We wanted to change all of this”, explained Francis Luyckx. "And it essentially comprises two projects, or more precisely, a double project: On one hand, the robots that were newly installed, had to be equipped with a control and a safety system - while on the other hand, the existing control and safety system had to be replaced. This was because the old installation based on safety relays had already been frequently upgraded to take into account different situations. In the meantime this system could no longer conform to the latest safety standards and the required additional safety functions."

The combination of new safety standards and functionality, especially in terms of detailed and reliable fault reporting, should be able to be easily expanded and favorable lifecycle costs achieved. Francis Luyckx added: "The decision between a system with separate PLC for the control and safety relays for the safety system on the one hand, and a real fail-safe control on the other hand, was quickly made: The latter is not only flexible, but it also reports faults down to the last wire. And, when all is said and down, the complete system is even more cost-effective."

The almost obvious choice...

"We specifically selected the Siemens solution. The reasons were extremely convincing: Firstly, here at Opel we like to use Profibus. In addition to the positive experience with this fieldbus, in the meantime, internally we have established a lot of experience with Profibus. As we now have access to the new Safety Integrated technology through Siemens, then the decision to select a fail-safe PLC with completely integrated safety functions was a clear cut case. And, the positive spin-off - we are open for future developments in the automation environment."

Opel Belgium sees the advantage of Totally Integrated Automation, last but not least, due to the specific characteristics of this huge automobile plant. Endless preparation cells and typical feeder systems to the assembly line of the Opel Astra are increasingly demanding more and more smaller distributed automation units. The practical advantages are obvious: Flexibility, shorter cables, extensive networking capabilities and integration on Profibus. And – what is extremely important – we have the necessary time to run tests. "Everything that can happen offline and therefore beforehand is to our benefit," explained Francis Luyckx.

Further refining

We now want to further integrate the safety functions in the requirement specifications. Initially, this involved the fault reporting. Fault reports were to be generated by making the appropriate parameter assignments with the standard Siemens software on the HMI panels. Of course, it is also possible to implement additional types and forms of safety-related intelligence - for example "muting functions" (programmed and safety-related suppression of safety functions that can be required for normal production operations) by using safety light curtains.

For Eric Moons, the E-mail card that is in fail-safe PLC plays a central role. "The central Opel safety/security services in Antwerp now have, as requested, a new option to monitor the safety-related software. As soon as the safety-related software is modified, an E-mail is automatically sent to the security services."

Together with the machinery construction company Comau, the specialists from Siemens Automation & Drives commissioned and programmed the first fail-safe SIMATIC S7-315F. Imtech the system integrator handled the second fail-safe S7-416F fail-safe control – independently and without any problems. Wim Van Goethem, a project engineer with Imtech briefly outlined his experience: "With help in the form of training from Siemens, we were able to create a basis so that we were able to very quickly program and implement the system".

The positive experience of the Opel team after two months use says it all: "The system was installed and started-up and then we literally immediately forgot about it" explained Francis Luycks. "It operates completely smoothly – not a single problem was encountered. We must now get used to the fact that we have a system in which the safety is really and completely integrated. Previously, the safety-related functions had to be separately programmed and therefore had to be explicitly seen. Now, everything is embedded in the system. Although we know and understand this, from time to time, we still have the reflex to want to see things separately - as if we really want to see that Standard 61204 is fulfilled."

On the shop floor

Both fail-safe SIMATIC controllers are used in the metal finishing area - where the basic automobile bodies are finished. One of the fail-safe controllers handles the function of the stud-welding system as well as the transport system which transports the automobile body to where the trunk lid or tailgate is mounted.

The second fail-safe controller is used for finishing - for example, polishing - visually checking the surface quality and fitting. This includes fitting and opening the doors as well as opening the trunk lid before the automobile body is transported to the painting shop. Both of the systems require complex transport movements without the whole area. This is all supplemented by highly specialized manual work carried-out by technicians so that numerous potentially hazardous movements must be reliably screened-off and secured.

"The physical security system comprises trip lines, standard Emergency Stop switches, light curtains with and without "muting" functions and classic safety cages with safety-related locks - explained Francis Luyckx. "This is an extremely complex arrangement where the fail-safe SIMATIC really comes into its own. This is because it checks everything and communicates with standard control systems via Profibus DP/DP couplers. However, during the year, we want to take the next step and make it essentially superfluous. Just one fail-safe SIMATIC control should handle both the safety-related control as well as also the standard control of the production process."

(from move-up 1-2/2003)

10.2 Safety technology for Toyota Canada

Toyota Canada chose a safety solution with Siemens AS-Interface at Work and SIMATIC S7-300F for their new Lexus factory and a plant retrofit. In addition to the enhanced safety, the automobile manufacturer also profits from the higher availability and thus increased productivity.

Toyota Motor Manufacturing Cambridge (TMMC) in the south of the Canadian province of Ontario is a real reference plant in the automobile industry. It is consistently rated under the Top 10 by JD Power and Associates and was honored by the parent company when it became the first Lexus plant outside Japan in which the brand new Luxus Offroader RX 330 is to be built - a model from the Lexus series.

For the new Lexus factory as well as the existing Corolla plant, safety systems are now used which, in addition to a maximum degree of safety, also offer increased diagnostic capabilities - therefore allowing production to be boosted. Together with Siemens Canada and consulting engineers Stantec, TMMC developed a leading-edge solution with AS-Interface Safety at Work and a fail-safe SIMATIC S7-300F PLC. This will be cost-effectively used in both the new Lexus plant as well as when retrofitting the Corolla plant. Siemens machine safety program manager Ondrej Benjik, together with the TMMC project manager Scott Bartlett, defined the retrofit strategy. He recalls: "For the retrofit it was important that the new safety solutions could be integrated into the existing control platform. Existing field devices and cabling were to be replaced. The retrofit was to be executed with either none or a very limited scheduled downtime. Further, Toyota placed considerable significance on the effective use of the new systems in operation such as quickly resolving operational faults.

All safety regulations met

The Siemens Actuator-Sensor Interface products have proven themselves well suited to the challenge. The requirements of the Canadian safety at work regulations that specifies safety tests before production starts for all safety-related devices and equipment was complied with in full.

"The retrofit went extremely smoothly" recalled Bartlett, "Toyota employees readily accepted the concept and immediately understood the significance of the system." Performed on weekends and during the holiday shutdown, the robot cells in the Corolla paint shop were retrofitted without any production downtime.

The "anti-chip" booth which applies a protective coating to a vehicle's rocker panels and the "blackout" booth which applies underbody protection, were upgraded to the new safety-related system with minimum changes to the existing PLC control system. The AS-Interface safety network from Siemens is based on a non-proprietary standard which means that it can be easily integrated into almost every PLC. Light curtains, laser scanners, safety interlocks and Emergency Stop switches can be directly connected through AS-Interface and a bus - whereby the safety requirements of Category 4 are fulfilled. Thanks to the unique direct connection system of the AS-Interface system it was no longer necessary to have distributed I/O stations for the safety components and/or the safety input modules. This reduced the costs for hardwiring to almost zero. Thanks to the simple and straightforward installation, the commissioning costs and retrofit time are significantly reduced. Further, complete function tests are able to be carried-out before commissioning.

SIMATIC S7-300F for Lexus

The new Lexus RX 330 plant uses Siemens safety-related solutions that are in full compliance with EN 954-1 and the IEC 61508 Standards. The AS-Interface is used in the new paint shop. The fail-safe SIMATIC S7-300F PLC on Profibus is used in the body shop.

"The Toyota installation clearly proved that the best safety solutions not only ensure a higher degree of safety at work", summarized Benjik from Siemens - but also that business goals such as high availability and fast troubleshooting are also supported."

Toyota Motor Corporation

Toyota Motor Corporation is the world's third largest automaker, producing a full range of models - from mini vehicles to large trucks. Global sales of its Toyota and Lexus brands, combined with those of Daihatsu and Hino, totaled 5.94 million units in 2001. As of March 2002, besides its 12 own plants in Japan, Toyota has 54 manufacturing companies in 27 countries/locations that produce Lexus and Toyota vehicles and components - employs 246,700 people worldwide (on a consolidated basis), and markets vehicles in more than 160 countries and regions. Automotive business, including sales finance, account for more than 90 percent of the company's total sales. Diversified operations include telecommunications, prefabricated housing and leisure boats.

Toyota minivan production fail-safe

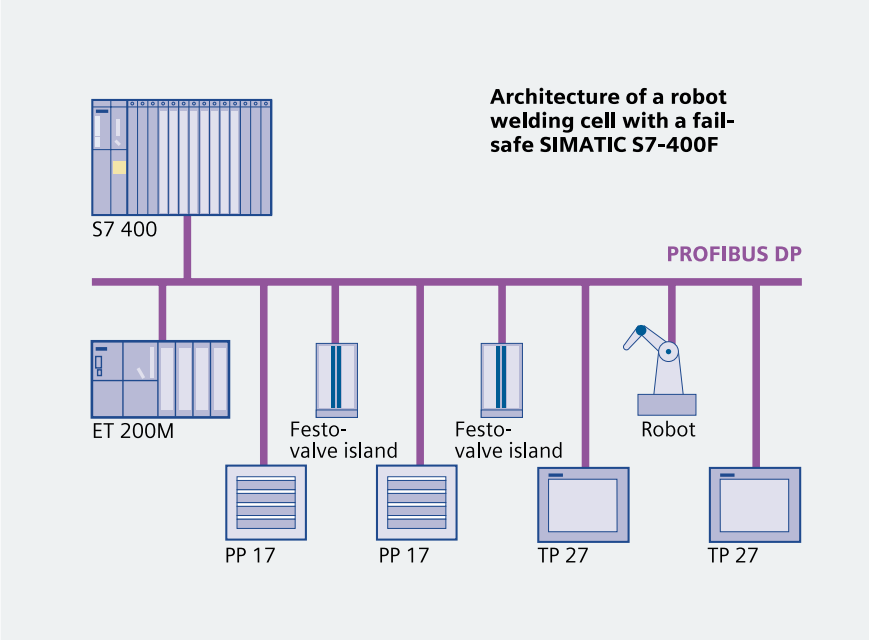
After a long and intensive pilot phase, for its body shop of the "Sienna" minivan, Toyota decided to use the new fail-safe technology based on fail-safe SIMATIC S7 PLC controllers and PROFIsafe. Since a production line gets continuously modified due to model changes, the use of a safety PLC with distributed system allows a fast, easy and cost-effective adaptation. Toyota rated the Siemens safety PLC as the most efficient solution in terms of functionality and reliability in an automated line among several other safety PLC suppliers evaluated. Presently, projects are running in three Toyota plants worldwide: Tahara (Japan), Indiana (USA) and Cambridge (Canada). A total of 170 PLC controllers with approximately 2000 safety I/O modules are installed in the three factories.

(from move-up 3/2003)

10.3 Building automobile bodies with distributed safety for Ford Australia

The safety system for the recent Body Sub-Assembly Robot Welding Cells at the Ford plant in Geelong, Australia, are implemented using SIMATIC fail-safe PLC technology and PROFIsafe. Effective use of Profibus distributed components has resulted in cells with a minimum of hard-wired components and field wiring as well as excellent diagnostic capabilities.

Ford Australia is enjoying broad praise for its BA "Falcon". The limousine, released in October 2002 is a six-cylinder car that was designed in Australia and leaves the assembly line at the Victoria plant. The Body Sub-Assembly components for the "Falcon" are manufactured in the Ford Geelong plant southwest of Melbourne. In the past, the Geelong plant was equipped with PLCs from a variety of manufacturers. When the planning for the production equipment was kicked-off for the new model, numerous automation technologies were evaluated in order to select an automation platform fit-for-the-future. Ford was looking for a flexible platform that was simple to program and troubleshoot for the service and maintenance personnel The new system also had to be in a position to easily integrate third-party equipment and devices such as robots and valve blocks.



Architecture of a robot welding cell with a fail-safe SIMATIC S7-400F

SIMATIC selected

Detailed investigations and tests ultimately resulted in Ford selecting the SIMATIC product range. The selection of safety system technology was then the next consideration. Having traditionally utilized a combination of hard-wired traditional safety relays to implement their cell safety, Ford investigated concepts for use of the new SIMATIC S7-400F fail-safe PLC as an alternative. The concept design was supported by Industrial Control Technology pty Ltd (ICT) - the local Siemens Solution Provider. ICT worked closely with Siemens Australia and specialists from the Competence Center Automotive (CCA) belonging to Siemens A&D in Nuremberg .

The result was an elegant design that could be applied as standard to all six of the new cells and was able to eliminate a high percentage of relays and complex interconnecting cabling. Safety-related functions were also able to be used for the existing cells. Further, additional safety equipment and automatic tests were added that especially simplify maintenance and commissioning - for example, the extensive diagnostic functionality of the touch panels that makes trouble-shooting far simpler.

These cells are mainly used for the robot welding equipment. Pressed body parts are fed to the machining stations where they are spot-welded. In some cases, the metal parts are transferred by robots to other machines for further operations. Ford engineers have utilized the SIMATIC HMI systems and distributed I/O with Profibus to maximum advantage in the design of these cells. Robots are directly controlled through Profibus therefore permitting fast disturbance-free data transfer. Pneumatic components at the clamping units are connected to Profibus through Festo valve blocks.

Operator stations are equipped with PP17 Operator Panels for operator interaction and visualization. Further, the TP 27 Touch Panel used allows production data and diagnostic information to be accessed. On the larger cells, an MP 370 Touch Panel additionally supplies this data and information at a central location.

The high resolution graphics of these panels allows photographic images of clamping units to be displayed with the dynamic status of clamps and proximity switches superimposed. This is an excellent way of clearly presenting diagnostic information to technicians and operators.

Central safety systems with SIMATIC S7-400F

The automation functions of the cells are controlled by standard non-fail-safe ladder code in the SIMATIC S7-400F PLC. This interacts closely with the programs in the robots. Ford personnel programmed the robots according to the process requirements and to interface to the supervisory PLC. In most cases, ICT developed the standard PLC code in close cooperation with Ford. Ford personnel configured and engineered subsequent cells themselves in-house. It goes without saying that the safety systems are a critical component of these cells. Light grids are generally used for every cell. Light barriers protect operator stations where parts are manually loaded. Using the two-hand control console, a part can be clamped while the technician remains within the area protected by the light barriers. Position switches at the robot base monitor the orientation and therefore allow manual access to a machine while the robot is presently working at another. Light barriers also protect access points for forklift trucks when they fetch finished parts stacked on pallets.

Safety interlocking functions in the robots, sensors in the fixtures, drives for the servo-driven rotary table and in a higher-level fast release valve respond to signals from light barriers, access gates and Emergency Stop devices. All of these safety-related functions are implemented using a fail-safe SIMATIC S7-400F PLC. A safety PLC also controls the electrical interlocking at the access gate. The fact that these functions were implemented using software resulted in a drastic reduction of electrical cabinet cabling and represents an implementation of the required safety logic in-line with that required in the field.

New maintenance functions were able to be added that would have been impossible with the previous, conventionally wired system. Diagnostic functions on the SIMATIC TP 27 Touch Panels supply detailed information about the status of the safety system and the fault diagnostics. One of Ford's main requirements was to block access to programmed safety-related functions - but at the same time still allow free access to standard code. This is important as modifications are required from time-to-time and additional systems are installed at the lines while the safety-related functions typically remain constant. This requirement was easily achieved using the SIMATIC S7-400F. Now, it is possible to modify the standard code without influencing the fail-safe code.

Distributed safety in LAD

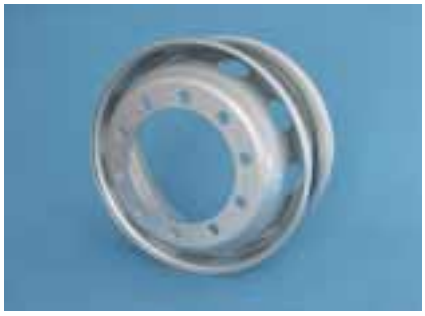
The latest installation of distributed safety-related technology is programmed in LAD and is based on “Distributed Safety”. This was well received by Ford personnel. The ability to program the fail-safe logic in LAD is considered to be a simpler alternative to CFC that was used in earlier S7-400F systems. Ford wants to use LAD in all of its future projects.

Ford has already announced that it also wishes to use the SIMATIC S7-315F for the safety I/O for smaller machines - that actually only require 1 or 2 safety relays. This PLC is extremely cost-efficient and with a high degree of performance. Just recently, engineering commenced work on 5 new cells. The distributed safety S7-315 PLC will also be used for all of the automation and safety-related functions for these cells.

(from move up 1-2/2003)

10.4 PLC-based safety concept in the manufacture of truck wheels for Michelin, Germany

Europe's leading manufacturer of steel truck wheels had to retrofit its proven rim profiling line to meet the standard of the highest safety Category 4 in compliance with DIN EN 954-1. Initially, this task appeared to be almost impossible as a result of the complexity of the system using conventional safety technology. However, this was able to be quickly handled using fail-safe PLC and fieldbus systems and at the same time with a high degree of flexibility.



Solingen is not only the address for razor sharp blades, but also the source of millions of wheels for automobiles and trucks all over the world. For the manufacturer, the wheel is what most automobile drivers would call a rim: A combination of the so-called disk fixed to the hub and the rim that carries the tire. Both parts are made separately from coils of sheet steel that are then formed, punched, joined, welded, tested and painted in several stages. Michelin with a market share of approximately 50 percent is leader in its branch for steel truck wheels in Europe. The "wheels" business unit of this company that originally invented the tire, manufactures well over two million units per year. It goes without saying that these wheels are crucial for the safety of all drivers. They are manufactured at Troyes (France), Aranda de Duero (Spain) and since 1997 also in Solingen. In this steel city, the Michelin Kronprinz Werke GmbH manufactures about 600,000 truck wheels per year on three dish lines and one rim line. This production capacity is to be doubled in the next three years when Solingen will advance to become a development center and will gradually absorb the manufacturing capacity of the Spanish daughter company.

Newly structured safety technology

For all its productivity, the mother company still places a great deal of significance on safety at work. The declared goal: Less than 5 accidents at work per factory and year. In order to achieve this value over the long term, Kronprinz carried-out a detailed risk analysis of the rim profiling line that had been producing rims for many years. Result: Safety Category 4 according to DIN EN 954-1 must be applied to the line comprised of 3 forming machines. From a safety-related perspective, this meant that the system had to be completely retrofitted.

Three protective areas were to be implemented and a total of 24 protective doors, 12 press safety modules and 30 motors were to be integrated into an integrated, seamless safety concept. The Europlan Systemtechnik from Kempen close to Krefeld - who had already handled several similar jobs - were entrusted with the implementation. However, up until now, they had always used conventional solutions, i.e. with hard wiring, safety control and proprietary safety bus – not an easy task with almost 60 safety relays.

In the pre-planning phase, Siemens presented its new fail-safe PLC controllers. "From the very start, I was convinced - especially as a result of the extensive fault diagnostic capability and the flexibility" recalled Dipl. Ing. Siegfried Schädlich, Head of Electrical Engineering of the Wheels Business Unit. "This is the reason that we took on the calculable risk and implemented our first PLC and fieldbus-based safety solution."

Distributed system for total safety

A fail-safe SIMATIC S7-300F is the core of the safety concept that was configured in parallel to the existing line control. This was done for reasons relating to time and costs. “Normal” and safety-related functions can be implemented together on one SIMATIC F-CPU; however, with Kronprinz, the F-CPU (S7-315F) exclusively processes safety-related field signals. When faults occur the F-CPU immediately switches the plant or the plant section into a safe state. Instead of a multiple number of single conductors, the safety equipment and devices are connected to the CPU via a safety-related Profibus connection. There are small local electrical enclosures close to the protective equipment and devices (protective doors, press safety modules). These local enclosures have fail-safe SIMATIC ET 200S Profisafe signal modules that transmit local signals to the central control station in the switchgear room using a conventional Profibus cable. The“Profisafe” protocol profile, developed by the PNO guarantees error-free communications. This protocol fulfills the highest safety requirements with SIL 3 (IEC 61508) and Category 4 of EN 954-1.

Mechanical interlocks at the protective doors and additional interrogation routines in the control program prevent production from being unintentionally interrupted. Europlan implemented the link to the (SIMATIC) line control required to coordinate the safety equipment devices and equipment with the production process using a bus coupling.

“One of the basic advantages of PLC-based solutions is naturally the high degree of flexibility” - explained Siegfried Schädlich - “this is because experience has shown that it is very difficult to precisely plan everything in advance - and often additional requirements are only received during the commissioning phase. Using SIMATIC F controllers, in the future, we will be able to quickly and flexibly respond to these late requirements.” With hard-wired safety relays, changes that are only considered to be small, always cost us a lot of valuable time - and additional requirements can often only be implemented with an over-proportional amount of time and costs. On the other hand, just the fact that the protective equipment and devices are connected through Profibus results in a high degree of flexibility when it comes to expanding the functionality. “What also plays a role is to visualize all of the states and components on one HMI device even when commissioning the equipment. This saves a lot of time” - explained Mario Stärz a programming engineer with Europlan. For conventional solutions, a lot of information can only be obtained in early project phases by measuring individual signals - a time-consuming affair.

Since the beginning of 2003, a SIMATIC TP270 Touch Panel in the local electrical cabinet continuously provides detailed information about the current status of the plant safety. The standardized Profibus diagnostics module from Siemens is integrated in the operator interface. This allows faults to be quickly localized and resolved. This makes diagnostics extremely simple, helps to keep downtimes short and therefore the degree of availability high.

Engineering as usual

PLC-based safety technology was a new area for Mario Stärz and he exclusively used the "Distributed Safety" software option package for Step7. This library includes block and application templates for safety-related tasks certified by the German Technical Inspectorate [TÜV]. It is embedded in the Step-7 environment so that even sophisticated safety-related tasks can be quickly and reliably solved in the standard languages F-LAD (ladder diagram) and F-FBD (function chart). "This meant that different functions for the setting-up and automatic modes were just as simple to implement as flexibly grouping certain plant parts for safe tool change or post machining (grinding) of tools in the line" explained the programmer. If, for some applications, the functional scope is not adequate, the possibilities of the open system can be fully utilized. This means that blocks can be modified or engineers can generate their own blocks from the instruction set of the option package.

Machine operators understand the benefits of a high degree of transparency and the straightforward, user-friendly operation of the new safety technology utilizing touch panels. Up until now, the diagnostics capability was not able to be proven in practice as there wasn't one single fault in the safety-related plant sections - such as wire breakage, short-circuit or cross-circuit fault.

Those responsible in Michelin Kronprinz for the effective implementation of safety requirements - both technically and from a cost-effective perspective - think that the PLC-based solution with SIMATIC F controllers also offers significant benefits in far smaller plants and systems: "Already with just two protective circuits within a system, the increase in performance in the application certainly makes the higher investment costs worthwhile" - explained Siegfried Schädlich. He and Europlan are already in the middle of detailed planning for several additional projects. These include, among others, a new complex welding line for automobile wheels with SIMATIC-controlled safety technology.

(excerpt from Blech Rohre Profile, Edition 8/03)

10.5 Exciting trip through Madame Tussauds

A safety system integrated in the standard automation

Modern amusement rides and production equipment have something in common: In both environments, high-speed drives execute automated motion. Not only this, downtimes are tabu - otherwise cost effectiveness goes out of the window. However, even when every attempt is made to maximize turnover, safety of persons has topmost priority.

A visit to Madame Tussauds in London includes, in addition to the obligatory exhibition of wax figures, also a trip on the so-called "Spirit of London". Visitors are sent on a trip through time where they can experience London from its early beginnings up to the present day. Passengers travel through the history of London in 87 London taxis. Siemens Automation and Drives (A&D) upgraded the safety and monitoring of this exciting trip to bring it in-line with the latest state of the art safety technology so that passengers can be guaranteed a safe trip.

In Madame Tussauds, state-of-the-art technology ensures a high degree of safety.

Interdisciplinary technology

The "Spirit of London" is extremely sophisticated and involves numerous mechanical and electrical drives, synchronized lighting, sound and special effects as well as a multi-language information system. A wide range of technologies - automated, driverless systems, industrial automation and theater workshops - were combined in order to create this unique indoor amusement ride. The safety systems have been designed so that safety can be guaranteed no matter what fault occurs – whether triggered by the system itself, the visitors or other events.

The company operating Madame Tussauds contracted the local D.B. Brooks consulting company - that specializes in amusement rides - to draw-up a detailed design for the required safety technology. A joint evaluation of the alternatives quickly indicated that the use of Siemens AS-Interface Safety at Work (safety technology integrated in the AS-Interface system) permitted the highest possible degree of safety and reliability but at the same time retaining operational flexibility. The introduction of the new International Standards EN 954-1 and IEC make this all possible. These standards now permit that all of the safety-related and standard operating control systems can be completely integrated into one another.

Certified safety

These technical prerequisites are fulfilled when using AS-Interface Safety at Work and also implemented in the field. As far as possible, safety-related functions are based on components that have proven themselves in standard operating automation over many years. In the case of AS-Interface, in addition to signals from the standard operating automation, safety-related signals are also transferred in parallel on communication links that have not changed from the hardware perspective. Safety-related components that have been specifically developed and certified for transmitting, receiving and evaluating safety-related signals are compatible with the existing communications concept. This has resulted in a decisive lead when it comes to cost-effectiveness by being able to reduce the amount of wiring and providing simpler diagnostics. The Madame Tussauds application is especially important as it is the first application of AS-Interface Safety at Work in England in the area of highly developed amusement rides.

A SIMATIC S7-300 controller, core of the new installation, can access all of the actuators and sensors via AS-Interface. It is also linked to six operator control devices that monitor every aspect of the amusement ride. The safety-related signals are continually evaluated in parallel using an independent safety monitor.

The Siemens OP7 operator devices provide access to all of the monitoring elements at each location – from standard operator control and maintenance steps through safety-related elements up to fire alarm and evacuation systems. Extensive diagnostic data is embedded in all of these systems.

SIGUARD light curtains - a Safety-Integrated product for applications up to EN 954-1 Category 4 - provide an optical protective field. This field reliably detects anybody that tries to leave the ride. If an emergency situation does arise, then it takes less than 2 seconds to stop the ride and to switch-on the lighting. The emergency evacuation is simul-taneously started together with the safety lighting system and announcements.

Integrated system increases the degree of safety

AS-Interface Safety at Work is a part of Safety Integrated - a Siemens concept that combines all aspects of sequential control and data management in order to provide the highest possible safety standards for man, machine and the environment. It is a safety system fully integrated in standard operating automation - Totally Integrated Automation. Users can enjoy many benefits regarding cost-effectiveness, flexibility and safety thanks to this innovative safety technology solution.

10.6 Seed production – a pump system for chemicals is controlled using ASIsafe

Recently, a fully automated pump control system went into operation in a large English seed production facility. This pump control for the chemicals used in the process is distributed throughout the plant. Together with a system integrator, all aspects of a fully-automated, high precision and safe process control were combined with the required data management functionality in compliance with international standards.

As agricultural areas dwindle, the yield from any piece of land becomes increasingly important and with it the quality of the seed used. Bayer Cropscience, part of the internationally active Wynnstay Group, produces chemicals to produce seeds and supplies a so-called "Twin Vanguard" seed production machine for Wynnstay Arable.

Wynnstay Arable is specialized in the production of seeds for the agricultural industry and places significant value on the safe distribution of chemical substances throughout the facility.

AS-Interface concept offers advantages

The system integrator DB Brooks that was awarded the complete automation has been successfully working with Safety Integrated products from Siemens AG for many years to implement solutions tailored to customers' specific requirements. The advantages of the AS-Interface concept were also used for the control of the seed production system and a special control unit was constructed: The "Bayer Cropscience Pump Transfer System".

In order that the"Twin Vanguard" machine manufactures the seed corresponding to the precise quality specifications, the chemicals must be pumped from the large containers at the ground level up to where the machines are located in the upper level. 36 liters of fluid must be precisely distributed to process 24 tons of seed per hour in batch operation at intervals of 15 seconds. The automation technology must have a high degree of safety especially in rugged industrial environments. The risk of permanent damage to the complete plant, e.g. if the pump system was to malfunction, is too high if a special safety system is not used. The effects of such a malfunction could have catastrophic effects on the environment.

Information is required to control the liquid flow. This information safely links all of the containers and precisely controls when and how much liquid should be pumped from the individual large containers to the processing machine.

All of the containers are connected through a single AS-Interface cable with its know "modular capability" - contrary to multiple cabling in a star configuration. This yellow, two-conductor cable also allows container levels to be graphically displayed on operator panels also connected to the cable.

This information is then sent to a SIMATIC S7-200 PLC that sends its control signals to the pump controls to either pump the liquid to the machines or fill the containers.

Simple, effective and highly reliable

Jim Donald, Head of Production for Bayer Cropscience explained: "In a large production facility it can be difficult to distribute chemicals precisely dosed. This is the reason that we are very serious when it comes to safety - which is reflected in the fact that we demand the highest possible standards. During the planning phase, we clearly recognized that the Siemens AS-Interface would provide us with many benefits. Apart from the fact that this is a simple, effective and highly reliable solution, the danger of making mistakes when installing the system is extremely low as only a single cable is used. Cost-saving was an additional reason to use this system - not only were the wiring and installation costs reduced, but also the risk of mistakes when installing the system for the first time and when making subsequent modifications."

Hardly any production downtime

All of this became reality: The production interruptions at the Wynnstay facility while installing the new automation system were minimal. The development engineers of the DB Brooks system integrator tested the AS-Interface without any significant additional expense because they were able to set it up in their own facility before it was actually installed on-site. The simple network configuration and installation drastically reduced production downtimes in comparison to conventional cabling techniques.

(excerpt from VERFAHRENSTECHNIK 38 (2004) No.1-2)

10.7 AS-Interface simplifies safety at work for UPS

120 employees at the UPS Center in Aachen sort and handle up to 20,000 parcels every day.

For the staff's safety, Emergency Stop command devices are located at the unloading stations and many other points along the 700 meter sorting plant. ASIsafe is the name of the control technology that was installed and which is now ensuring safety at the workplace.

The parcel sorting plant in Eschweiler/ Weissweiler, Germany comes to life when the clock in the UPS center in Aachen strikes 4:30 a.m.

By 8:00 a.m. the parcels are sorted on an apparently endless belt where workers load all of the parcels as quickly as possible for the 50 deliverers with their characteristic brown trucks. Trouble-free, smooth sorting is crucial. But because UPS's company philosophy not only focuses on speed and precision but also on the safety of its personnel, those responsible in Eschweiler rely on safety switching elements from the Siemens ASIsafe program to additionally increase safety. Instead of the previous, conventional industrial controls that were used, UPS decided to install Emergency Stop command devices with AS-Interface. AS-Interface always provides advantages when simple I/O devices are to be addressed by the machine control.

50 delivery personnel start their tour with their typical brown trucks from the UPS headquarters in Eschweiler close to Aachen.

Up to 62 slaves can be operated on one network with the new AS-Interface Version 2.1. This type of configuration is of particular interest to logistic experts because the necessary safety circuits have recently been implemented with safety monitors as are specified in sorting centers. Emergency Stop command devices are located wherever personnel come close to moving parts and equipment. There are 26 Emergency Stop command devices in Eschweiler.

The UPS specialists quickly realized the advantages of the AS-i safety technology and therefore rejected a solution involving a special safety bus system plus additional costs for components, installation and maintenance. The 3RK1105 safety monitors are directly connected to the SIMATIC S7-300 controller used in Eschweiler for the UPS solution. It took about two weeks to retrofit the plant and this was carried-out in parallel to the old system without

26 Siemens Emergency Stop command devices mounted at key locations in the parcel sorting system and connected with one another through AS-Interface

affecting the daily sorting routines. The new safety network was completely commissioned in one day – between two shifts. Like all signal transmission systems, AS-Interface must comply with certain basic values. A repeater must be installed after not more than 100 meters. A maximum of two repeaters may be connected to each AS-Interface line.

The system engineers in the UPS center in Aachen generated their own solution for locating the signal amplifiers. Since the supervisory computer is positioned very centrally in the sorting plant, a completely untypical order of slave numbering was selected. The trick: The typical yellow AS-Interface cables can be branched-out in a star configuration from the four safety monitors for the 26 Emergency Stop command devices. This ensures that there are no problems associated with the distances - even in an enormous parcel sorting plant that extends over 700 meters. This example shows that a single AS-Interface ring cable does not always have to be routed directly from the control system, but that AS-Interface can be flexibly used in an existing plant layout.

Faults simply detected

The interesting feature about the circuit used is that it is immediately obvious to which Emergency Stop command device has been pressed. The control has an additional optical indicator precisely for this purpose. This makes it easier for technicians in the logistics center to localize faults. Further, the UPS technicians have integrated a monitor module in the electrical cabinet. The SIMATIC C7 621 AS-Interface unites the AS-Interface master CP 342-2, an S7-300 SIMATIC-CPU and an OP3 operator panel in one housing.

Safety up to Category 4

The complete sorting plant shuts down as soon as an Emergency Stop command device is actuated. The initial plan in Eschweiler was to only shut down those conveyors within a range of 15 meters – the distance specified in the relevant safety regulations. However, the planners immediately realized that almost all of the belts would be stopped as a result. It was therefore agreed that it must be possible to shut down the entire plant within several milliseconds.

Applications up to Category 4 according to EN 954-1 can be equipped with AS-i Safety from Siemens. The required safety-related communications between the safety slaves and the safety monitor is provided by an additional signal transmission route. The safety monitor "expects" a 4 bit telegram cyclically from every safety slave which changes continuously according to a defined algorithm. If, due to a fault, the expected telegram fails to arrive or the telegram reserved for an alarm 0-0-0-0 is received, the safety monitor shuts down the safety-related outputs with its dual-channel enable circuit after a maximum of 40 ms.

In addition to the newly installed Emergency Stop command devices in the UPS center in Aachen, all other typical I/Os such as magnetically-operated switches, pushbuttons, laser scanners or light barriers, grids and curtains can also be equipped and implemented using the safety-related AS-Interface system.

Siemens offers their full range of safety devices from the "Safety Integrated" portfolio. These devices are assigned to the safety monitors using simple-to-use AS-Interface configuration software.

Can be flexibly expanded

With the objective of gradually modernizing plant, the in-house technicians have clearly noted "AS-i safety" in their requirement specifications for their next conversions.

The reason for this is that they all state system flexibility is incredibly important. Especially since not only single signals but complete data packets can now be transmitted. This closes an important diagnostics gap in AS-Interface.

Logistic centers profit from the AS-Interface technology in two ways. This is because all of the industrial controls can be quickly connected and disconnected as a result of the insulation displacement system used to establish connections. The technician no longer requires a screwdriver to connect-up the cables. Before an AS-Interface device is removed, the technician simply puts it into the service mode by pressing a button. The new device is then simply inserted without having to be programmed. This is because the individual "slot numbers" in an AS-Interface line-up are saved in the system itself. The technician then logs-on the new device with the host by pressing the button again. No specifically trained personnel is required to do this. This is particularly important because logistic centers are usually expansive and distances are long.

The technology is otherwise also very user-friendly. The experience of those responsible at UPS is that faults can be quickly eliminated and commissioning is extremely fast. Every employee soon became familiar with the AS-Interface devices. This saves valuable time – a major issue when it comes to logistical solutions.

Stefan Höfer (right) Manager of the UPS Center Aachen and Heinz Czichy, Siemens consultant are very happy about the new and simple safety solution using AS-i Safety. As a result of the centrally located electrical cabinet, special AS-Interface cabling was able to be implemented

10.8 CROWN Vourles – safety in the packaging industry with Safety Motor Starter Solution PROFIsafe

After production line 22 belonging to "Crown Speciality Packaging France" – as the name suggests, a packaging company – was adapted and modified in-line with the appropriate standards, it is now running with PROFIsafe. The 416F central processor of the S7-400 simultaneously manages the standard and safety-related inputs and outputs. The control functions are supported using touch screens that are connected to the MPI bus. The technology used allows testing and processing times to be halved when using Safety Motorstarter Solution PROFIsafe.

CROWN Holdings in Vourles/Lyon in France is one of the market leaders in the packaging industry. The company manufactures special metal packaging. This includes cans for beverages and other products and special packaging for large brand names (e.g. Bonduelle, Coca-Cola and others) in "small quantities" - this means a maximum of million cans per production line and year.

"Especially so-called 3-section cans" are produced - explained Gilles Guerrin, responsible for engineering at the facility: "Each can comprises a rounded or welded body, a drawn cover where the opening is located and also a drawn base element."

Industrial buckets with a diameter of 220 mm and a capacity of either 5 or 6 liters are produced on line 22. "The hourly production rate exceeds 2500 buckets - this therefore meant that the line had to be adapted to be compliant with Dekret 9340 - the French Standard for safety of machinery. The goal was also to increase the productivity by correctly adjusting the line and in turn requiring fewer personnel to operate the line."

Not only this, the automated production of the "funnel bucket" also included installing a new machine to locate the rings therefore replacing two manual machines that up until then required four operators.

Fourteen machines in series

Line 22 comprises 14 machines in series that are supplied with steel sheets:

- The welding machine rolls the flat metal sheet before the cylinder that is formed is welded together.
- The hydraulic expander tapers the tubes.

- The forming machine forms the upper part of this taper so that it can accept the upper sections.
- The ring machine completes this operation. At the same time, a ring is inserted in the main body in order to avoid deep nesting of the buckets. This allows them to be easily separated later on.
- Every bucket is turned-over before it runs-through the following machines: The bordering machine, then the capping machine. The diameter is reduced while the edge is bent so that the base can be welded to the main body.
- The bucket is turned-over again before the seamer prepares the upper section of the bucket.
- The welding machine locates disks at both sides of the main body for handles. The handles are distributed using gravity using a centrifugal drum and positioned precisely at the weld seam.
- The painting machine ensures that the welded elements are protected.
- The tunnel is used to dry the paint that has been applied.
- The double ring capping machines was renewed in the Lycée Lamache.
- The bar installation device attaches the handle to the disks.
- The buckets are then automatically stacked.

The bucket production line was adapted in compliance with the Standard

This meant that fourteen machines had to be adapted. Extremely short intervention times were required in order to keep downtimes to a minimum and in turn minimize supply delays to customers.

Preliminary work was started in May 2003. The first machine was adapted in compliance with the appropriate Standard the following September. All of the line components were incorporated after three additional modifications.

This modification work affected the safety in the following ways:

1. Machine protection: Non-controlled grids were replaced by light curtains and fixed protective grids were installed at the rear.

2. The conventional control panels were replaced by SIMATIC Touch Panels with two Emergency Stop command devices: One of these is an Emergency Stop device to locally stop the machine and the other to stop the complete line.

3. In order to implement the pneumatic distribution in compliance with the Standard, the distributors and the valve supply blocks had first to be changed as well as the control of the pneumatic supply.

Further, the following modifications were made:

1. Sensors were installed at the housings with the mechanical cam controllers that are extremely difficult to adjust; the settings of the sensors can be modified directly at the OP with a far higher accuracy (to an accuracy of 1 degree).

2. Finally, the electrical cabinets were renewed, the connected safety relays were replaced by an automated SIMATIC safety system: A central cabinet with S7-416F control is connected to other electrical cabinets using the ET 200S I/O.

"With Siemens and our installation company, we started to investigate the automation architecture required", recalled Gilles Guerrin. "We have been working for 25 years with SNEF (a company specializing in automating industrial operations) both in France as well internationally". Gilles Guerrin: "Siemens was the only manufacturer of automation technology that implemented a safety PLC with standard fieldbus communications."

Today, the line has three networks that connect the various machines:

1. A power network runs through the complete line. The central cabinet is connected to every distribution cabinet close to the machine.

2. 10 TP170B panels are connected to the MPI network (196 kbaud). They replace all of the conventional knobs with the exception of the Emergency Stop command devices.

3. The PROFIBUS DP network with PROFIsafe profile connects the production systems with the SIMATIC S7-416F control. Safety-related telegrams are exchanged between standard devices via this network. The PLC is connected to 19 DP slaves and more precisely with 13 ET 200S I/O stations, 5 frequency inverters and 2 pneumatic blocks.

Further, there are a total of 248 inputs and 124 outputs, 64 safety inputs, 64 safety outputs, 43 safety fail-safe motor starters and 7 SSI modules to connect the position sensors.

When it comes to the safety network, emphasized Gilles Guerrin, “PROFIsafe has the advantage that it permits safety-related communications on a standard PROFIBUS DP”. And this means the highest communications standard according to the IEC 61508 safety standard. Standard communications and safety-related communications can run on one and the same cable.

The ET 200S I/O system clearly established itself thanks to its modularity and the ability to support the safety-related functions - and at the same time reduce the amount of wiring. “We were able to install the fail-safe motor starters at the ET 200S stations. They allow selective safety trips to be simply executed and correspond to the safety requirements, Category 4 in compliance with EN 954-1. An additional benefit was the fact that there was a redundant line contactor without any additional wiring”.

Twice the speed - half the price

“While previously we had a type of hardware intelligence that was coupled with a type of software intelligence, today, everything is software - embedded in the PLC”

For Gilles Guerrin, this transition had some wide-ranging consequences. When compared to conventional solutions where the terminal and the safety relay had to be wired-up, now, thanks to the electronic management of classic inputs and outputs as well as the safety inputs and outputs and connecting the motor starter to the line supply, the testing time was halved. The wiring time itself was also halved, as the safety functions no longer have to be connected-up and the motor starters communicate via PROFIsafe. Finally, it allowed the system intelligence to be re-grouped and all of the information to be arranged at the same location of the PLC in order to simplify commissioning the line.

10.9 More safety in the automobile industry

The new flexible production line in the Renault plant in Cleon in the North of France has been operational since the end of 1998. Working around the clock, 40 machines in the plant produce 5000 cylinder heads every week. Each of the machines is equipped with a SINUMERIK 840D with Safety Integrated. We asked the head of the production line, Patrick Renault, about his experience with integrated safety technology from Siemens.

Mr. Renault, the new production line has been operational since September 1998.
What does the line consist of and what is it producing?

Patrick Renault: In addition to a total of 40 machines, there are also 13 loading gantries, entry and exit areas as well as assembly units, measuring stations and the labeling units. The line operates around the clock – the only exception is six hours on Sunday morning. This line produces various cylinder heads for our 1.4 to 2.2 liter engines.

All of the 40 machines are equipped with Safety Integrated in conjunction with a SINUMERIK 840D. What made you decide to use Safety Integrated?

Patrick Renault: It was the machine OEM (Grob) who first recommended and implemented Safety Integrated. In the meantime we are extremely happy about this decision. This is because the

GROB machining center in the production line

machines operate with an extremely high speed – 60 to 70 meters per minute at the machining centers and 120 meters per minute at the loading gantries – which means that it is absolutely mandatory to provide a maximum of safety – and we can achieve this with Safety Integrated.

What additional advantages does integrated safety have in comparison to conventional safety technology?

Patrick Renault: To start-off with, it has a significantly shorter response time as it is integrated in the SINUMERIK 840D numerical control.

Further, safely reduced speed is possible using Safety Integrated. This means that we can intervene with the protective doors open and the machine still running – and with 100% safety. Not only this, but the drives no longer have to be disconnected from the power source. In turn, this extends the drive lifetime – as you know, the lifetime is reduced by frequently powering-up and powering-down the DC link.

Patrick Renault - head of the production line

Which criteria initiated you to use integrated safety as standard on all of your production lines?

Patrick Renault: Renault's goals are quite clear: We only want to use machines that fulfill Category 3 of the EN 954-1 safety Standard and we want to achieve a high degree of safety using fast response times. Safety Integrated fulfills these requirements.

Are the operating personnel satisfied with integrated safety?

Patrick Renault: The possibility of manually intervening in the machine with the door open for service or when setting-up the gantries creates a lot of confidence. Furthermore, the use of Safety Integrated is quite transparent; this means that there are no problems during production. Operating personnel have clearly understood that Safety Integrated offers them more safety and security although the speed of these production lines is significantly higher.

Mr. Renault, thank you for the interview.

10.10 New standard for machine tools

For some time now, Alfing Kessler Sondermaschinen GmbH, at home in Aalen, Germany, has used flexible production systems. The latest alloy-machining module is the ALFING 2-Spindler, which is also being used by VW Saxony in Chemnitz. One of the special features of these machines is the integrated safety technology from Siemens.

Instead of rigid transfer lines, flexible production systems and instead of special machines, standard units – which reflects the demand for modular systems for state-of-the-art production equipment. Standard modular units not only simplify service and maintenance but also increase the availability. They also allow existing systems to be expanded and modified – also for the new machine modules, for example, the two-spindle machine from Alfing Kessler. This is used in flexible production environments to machine alloy parts and components.

Especially in vehicle construction, low-weight designs are increasingly demanding the use of alloys. It is not surprising that the ALFING 2-Spindler will be used by VW Saxony to machine cast aluminum cylinder head covers (aluminum die-case components).

Minimum idle times

For the ALFING 2-Spindler, the separately driven spindles operate independently of one another. While one of the spindles machines the workpiece, the second spindle picks up the next tool from the magazine allocated to each spindle (with a 48-tool capacity). The second spindle is then immediately accelerated up to its rated speed. This means that the tool that has just been inserted is already rotating and can quickly start to machine. All of this is realized in a maximum of 1 second after the spindle is ready and the tool has been changed in the magazine. The extremely fast tool transfer with both spindles operational reduces the idle times. This drastically increases the productivity: A cylinder head cover is completely machined in just approx. 165 seconds. The 2-spindle design uses lightweight moving masses and heavy stationary masses. Only then can the required dynamic response and stability be achieved. The axis movements are distributed: The tool executes movements in the Y and Z axes, while the workpiece moves along the X axis. The operating range extends over 880 x 630 x 500 mm (X, Y, Z).

For the first time with SINUMERIK Safety Integrated

The machine is controlled from a SINUMERIK 840D and SIMODRIVE 611D. The machine is equipped with Safety Integrated, including safe programmable logic (SPL) – which is a first for a production facility of VW Saxony.

"For these types of high-speed machines, with acceleration rates of over 10 m/s2, in our opinion, it would be irresponsible not to use safety functions", explained Willi Diemer, the Head of the Electrical Design Department, regarding his decision to use SINUMERIK with Safety Integrated. And why integrated safety? Diemer: "Reduced speed can only be safely monitored using integrated safety technology. If it is not done this way, the software reduces the speed, but as soon as the machine develops a fault without safety function, it would simply start. And everybody knows what that can mean."

Operator concept with SINUMERIK Safety Integrated

Fewer relays mean fewer failures

Safety technology is also required in order to move the drives with safely reduced speed even with the protective door open, for example, when the machine is being set-up. Conventional safety technology can only disconnect the power. When a fault develops, Safety Integrated can shut down the machine faster and more safely. It is no longer absolutely necessary to disconnect the power. Only drives that really have become uncontrollable are automatically disconnected from the power supply. This provides more safety for the operator at the decisive instant and also reduces the mechanical stress on the machine and process. "For Alfing, safe programmable logic triggered us to use this technology", reported Willi Diemer. "This is because this logic allows conventional switching devices to be eliminated - which has a positive impact - and not only on the price."
A machine equipped with Safety Integrated and SPL can be offered at almost the same price as conventional technology (however, one option is that the machine can be operated using the enable button). Furthermore, fewer relays also mean fewer failures and therefore a higher degree of safety and higher machine availability. For instance, if an important relay, for example the relay that enables the pulses or controller for the drive, fails, then the machine can no longer brake in a controlled fashion. The motor coasts down and there is a chance that the machine could be badly damaged.

Convincing concept

For the customers from VW Saxony, Safety Integrated with SPL was a new technology that they first wanted to carefully check out. Alfing Kessler was able to convincingly present the machine, configured according to the Siemens specifications together with the safety functions, to those responsible at VW Saxony, VW production planning and representatives from the appropriate German Regulatory Body. The two-channel configuration for all of the safety components in compliance with the Siemens specifications was especially impressive. These safety components included, for example, the protective doors and Emergency Stop function. For this machine, even the cross-circuit monitoring of the two safety channels was implemented using the "4-terminal concept".

For VW, it was also important that the machine could be operated with the protective doors open. Using Safety Integrated, the machine operator concept can be optimally harmonized to the requirements of the operating personnel and the process itself. This makes it far easier to set-up the machine. Tampering, which unfortunately still occurs today, is prevented by the basic concept itself. Additional machines utilizing the same concept will now be built for VW Kassel, SKODA Auto and DaimlerChrysler.

Willi Diemer is clear about one thing: "For our high-speed machines, we will always use integrated safety technology from Siemens."

10.11 Safety when testing products used for safety at work

State-of-the-art safety when working at machines is a good example for how new technologies are establishing themselves in today's industrial environment. They not only ensure that man and machine can safety interact with one another, but also provide high economic benefits - earlier, this would have been a contradiction in terms.

Summary

Increasingly, safety products such as laser scanners and cameras - that are "electro-sensitive protective equipment" are being increasingly used in and on machines to protect persons in hazardous areas. In order to investigate and test these devices, the BG Institute for Occupational Safety & Health has, for some time now, been using a test system with linear axes in an open type of construction. In order to be able to carry-out the time-consuming series of tests even faster, more simply and therefore more efficiently, the test system has now been upgraded with "latest state-of-the-art technology". This includes the integrated safety functions of the Siemens SINUMERIK 840D CNC control, a network of all of the safety-related system sections via the Profibus fieldbus with PROFIsafe profile and four new Siguard LS-4 PROFIsafe laser scanners to secure the protective fields.

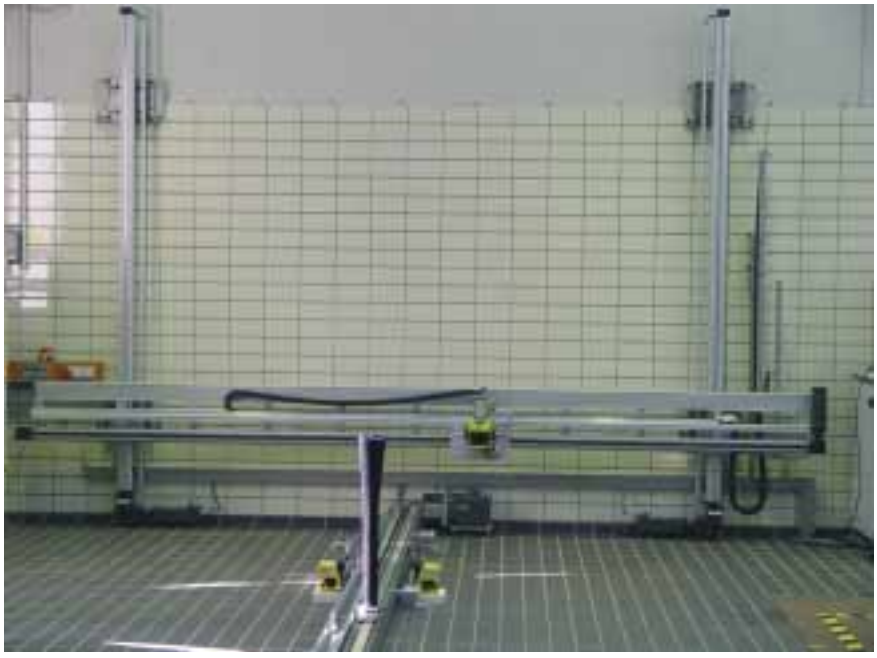


Fig. 10/1
The modernized and automated test system of the BG Institute for Occupational Safety & Health for and with the latest generation of safety technology makes the product tests specified by law more efficient – and offers testers themselves "all encompassing safety"

Product testing and certification with the BG Institute for Occupational Safety & Health

The BG Institute for Occupational Safety & Health is a research and testing institute for a German Regulatory Body (BG). The BG Institute mainly supports the various trade organizations and their institutions when it comes to scientific technical issues in the area of health and safety at work by providing the following

- Research, development and investigation
- Checking/testing products and material samples
- Carrying-out measurements in operation and providing support
- Participating in the Standards Associations and drawing-up regulations
- Providing specialist information and expert know-how.

Further, the BG Institute is active throughout Europe for manufacturers and companies providing the following services:

- Product testing and certification
- Certifying quality management systems.

The BG Institute for Occupational Safety & Health carries-out basic investigation/ research work for new types of protective equipment and devices. Not only this, it develops testing techniques and works in the Standards Associations, provides consultation in the product development process and in actual use and as certified testing body, tests and certifies products. Presently, it is mandatory that these safety-related products are tested.

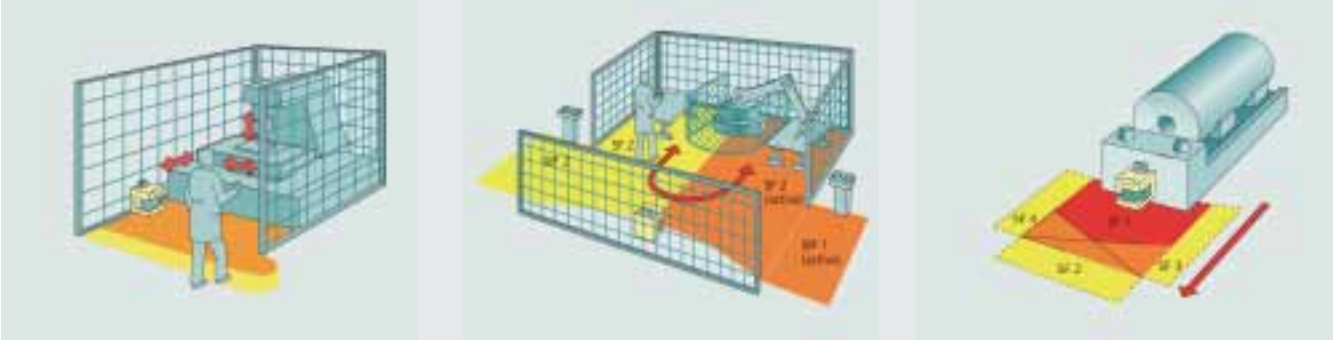


Fig. 10/2
The many and diverse applications of laser scanners

Partially automated product testing – e.g. for laser scanners

Laser scanners are optical distance-measuring sensors and are used in various applications as personnel protective systems:

- Protecting hazardous areas at stationary machines and robots
- Monitoring routes taken by driverless transport systems

In this case, persons must be detected directly from a driverless vehicle - e.g. directly in the hazardous area in front of the vehicle. An appropriate safety-related signal must then be output that stops the potentially hazardous movement. For instance, the driverless vehicle is braked down to standstill using its drive and brake and is kept in this condition as long as somebody is in the hazardous area.

The ability to safely detect a person – under all application conditions and even if its optical, mechanical or electronics system develops a fault – is a decisive feature of the laser scanner. As part of the product certification by the BG Institute for Occupational Safety & Health, the testing of all sensor characteristics and measuring the monitoring areas - the so-called protective fields - is an important component. Individual tests regarding the detection capability, the protective field geometry, measuring and mapping accuracy, resolution, response time and the ability to function under different ambient effects such as external light sources make this test extremely complicated and time consuming. However, using a test system, these tasks are essentially automated and what is especially important can be carried-out with a high degree of precision and reproducibility.

Automated test system

The greatest degree of "support" that a system can provide when testing electro-sensitive protective equipment is to precisely move and position reference targets - so-called test bodies. These are used to emulate parts of the human body with precisely defined characteristics. Here, neither specimen bodies nor showcase models are used. This is because test bodies achieve a far higher degree of reproducibility of the measured results and must have features to represent "poor condition" characteristics for detecting persons. The test system in the BG Institute for Occupational Safety & Health is a 3-dimensional coordinate system using linear axes between the test object – i.e. the protective equipment to be evaluated – and the test body.
In Figs. 1 and 3, the test object is identified as a yellow "box" on the slider of the X/Y portal and the test body as cylinder on the slider of the Z axis.

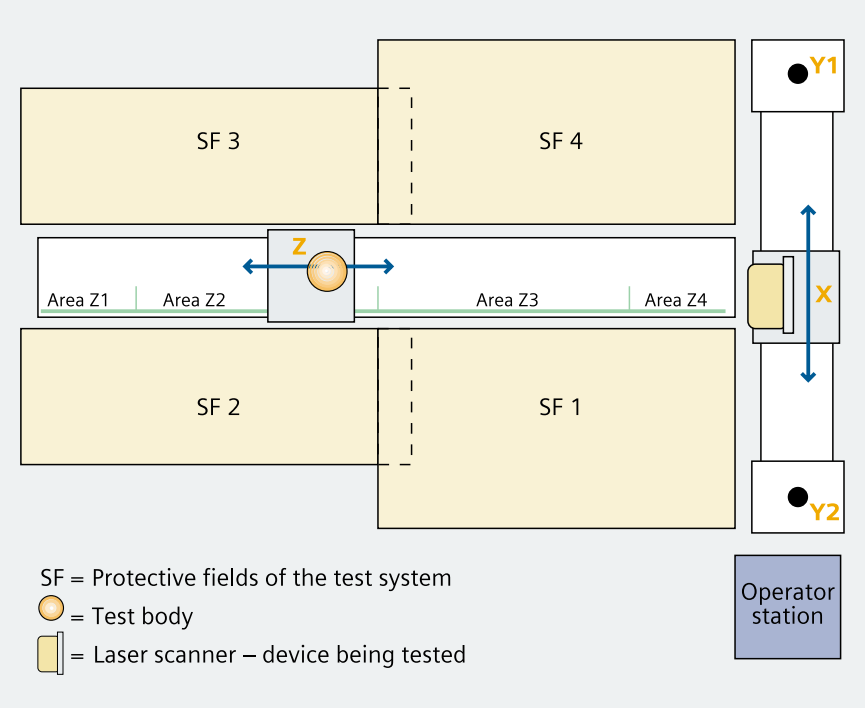


Fig. 10/3
Schematic representation of the axis protective field (view from the top)

When dimensioning the protective fields, the test system has the task of positioning the test body in extremely fine grid steps. The device being tested is then interrogated as to whether it detects the test body. The many yes/no results allow a 2 or 3-dimensional image regarding the protective field geometry to be created therefore identifying possible gaps. If a response time of a protective device is to be measured, then the test system moves the test body with a variable velocity in the protective field of the device being tested. It then evaluates the delay up to its output switching signals. This also simulates, e.g. a vehicle actually approaching a person. In addition to the (four) axes, an "intelligent" control is required that "handles" all of these test scenarios in a coordinated fashion, contains an operator interface for a test program, which can be used to configure the test task, test sequence and equipment data. It also provides a program area in which all of this collected measuring data of the equipment/ device being tested can be displayed and/or evaluated.

This is complemented by the fact that the test system is designed so that it is open and accessible. And what looks completely harmless for positioning motion to accuracies of millimeters, changes when dynamic test programs are used. In this case, either the test body or the euipment/ device being tested "flies" through the (test) area at a high speed. *Comment: Another reason why "live" test objects should not be used!* Of course for the BG Institute for Occupational Safety & Health, safety always comes first. A hazard analysis was carried-out just the same as for securing areas at machines industry, and the areas of the axes that could cause injury were carefully protected and secured. And it should be of no surprise - using laser scanners.

The latest generation of laser scanners

In the test system, four Siguard LS-4 PROFIsafe laser scanners with protective fields SF1 to SF4 (shown in a simplified fashion in Fig. 10/3) provide perfect personnel protection in the axis traversing ranges. The laser scanners are directly connected to Profibus with the PROFIsafe profile via an integrated interface. By the way, the BG Institute for Occupational Health & Safety also certified the laser scanner that is suitable for applications up to Category 3 according to EN 954-1. This means that what was previously a device being tested, is now operational in the test system providing the optimum degree of safety.

Fig. 10/4
New SIGUARD LS-4 PROFIsafe laser scanners – simple, reliable installation using the integrated Profibus interface

Simple installation using a direct connection to Profibus

Profibus with the PROFIsafe profile was selected to establish the connection between the laser scanners and the safety-related system control – the SINUMERIK 840D. It establishes the direct connection to the laser scanners as well as to all of the other safety-related plant sections. These include, for example, the Emergency Stop command devices, operating mode key-operated switches and holding brakes. These are directly connected to the fail-safe SIMATIC ET 200S input/output modules without requiring any additional devices therefore minimizing costs. Of course all of this has the positive spin-off that engineering and installation costs are also significantly reduced.

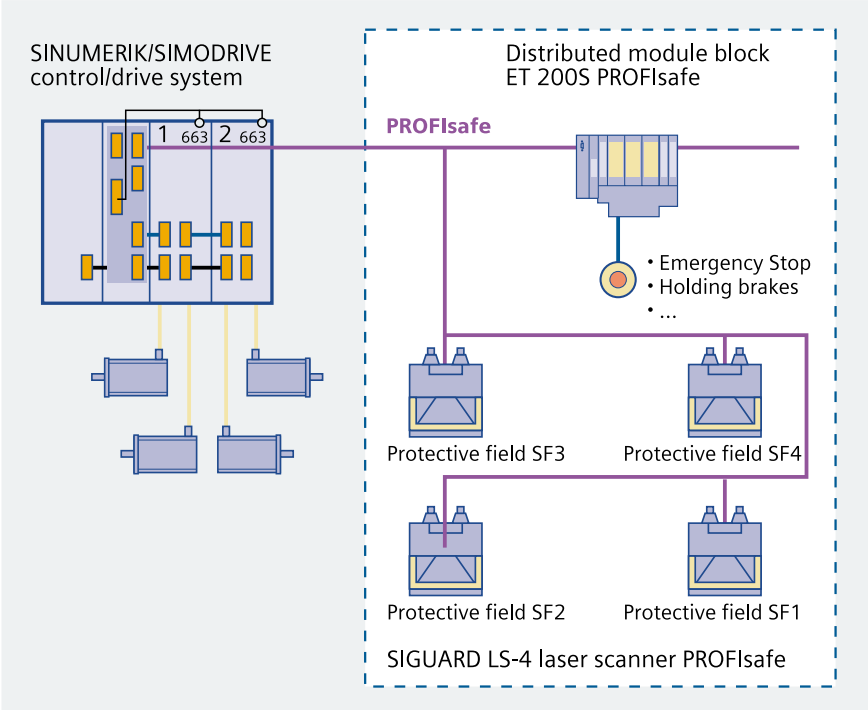


Fig. 10/5
Profibus with PROFIsafe profile to network all the safety components results in a simple system installation

Additional safety integrated in the control/drive system

The test system was automated with a CNC control already back in 1996. Even then, the SINUMERIK 840D used had integrated safety functions. The functional scope included (just the same as today) standstill, velocity and position and endstop monitoring that could be parameterized (!) Additional, functions are used on and in the test system in the form of the current SINUMERIK Safety Integrated safety package; these are as follows:

- **Safe programmable logic (SPL)**

All of the safety-related sensors and actuators are directly connected to the I/O of the control without using any external evaluation devices. They are evaluated in the software. This safety-related functionality realized in the software results in a high degree of flexibility when implementing plant operator control philosophies in line with those required in practice. Further, high cost-saving benefits are obtained by substituting conventional hardware components.

- **Expanded stop functions**

With the introduction of the “external stop” function, it has been possible to operate parts of the test system without any interruption or to simply continue operation even when safety signals have responded. For example, if a person (generally accidentally and unintentionally) or the test engineer himself enters the protective field during the test - as example, one of the protective fields 2 or 3 (SF2/SF3 in Fig. 10/3) then the velocity of the portal slider (axes X/Y) is reduced to a “safely-reduced speed”; however, it doesn't remain stationary - that would disturb production - and does not result in the program being interrupted. This means that the test engineer doesn't have to wait for the program to start again before continuing the test - however, safety is still absolutely provided in every situation. The reason for this is that also for the Z slider, depending on its particular position at any time, an intelligent decision is made as to whether it must stopped to a standstill or the safely reduced speed activated.

- **Expanded status and diagnostics display**

In order to provide fast and basic diagnostic functionality, the required information about the status of the safety functions in the system can be directly displayed using a softkey bar. Further, graphic, application-specific diagnostic status screens are integrated in the operator control panels.

Afterwards **Beforehand**

Fig. 10/6
Software replaces hardware components, electrical cabinets become smaller

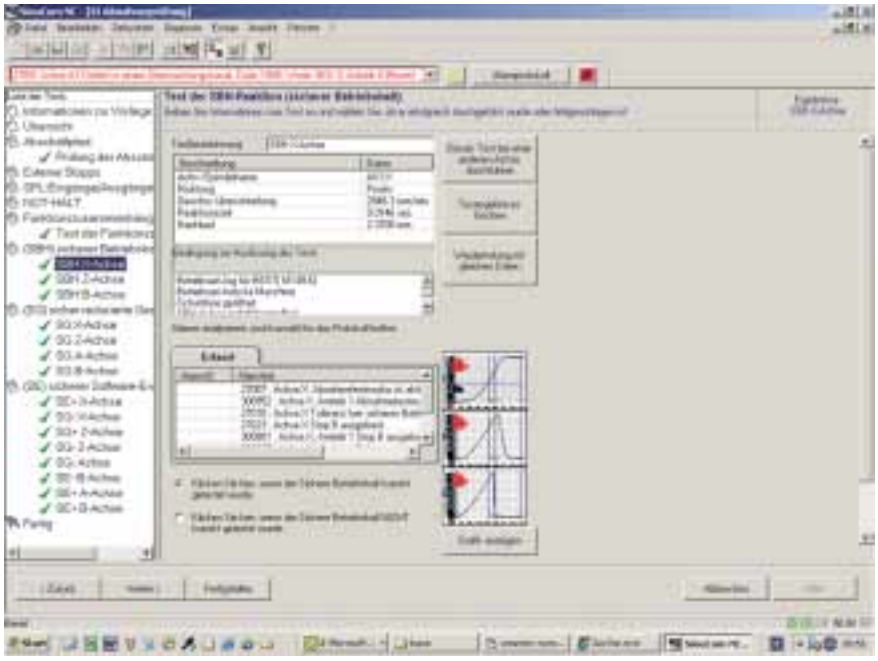


Fig. 10/7
Integrated acceptance test with operator prompting and plain text display as proof for machinery construction companies and end users

• **Integrated acceptance test**
The safety functions of electric drives are to be tested when commissioning using an acceptance test according to the specifications of the applicable standards. A "tool" has been integrated into the control/drive system to allow users to carry-out this test as simply and quickly as possible. This significantly reduces the acceptance times as, e.g. relevant machine data can be automatically transferred. The prompted tested sequence with plain text display also simplifies operator control. Even the acceptance report required is automatically generated.

Operating experience: The highest degree of flexibility, availability and safety

When operating a (test) machine that behaves, depending on the situation, in a specific, safety-related fashion "gives a good impression" from the perspective of a test engineer. This means that he is not confronted with tedious interruptions, or has to start from the very beginning when, as a result of the new stop functions, he inadvertently or deliberately enters the hazardous area when testing a piece of protective equipment. The requirement for simple handling and fast (test) sequences was therefore fulfilled. This means that this state-of-the-art safety technology really provides the highest degree of flexibility and availability and at the same time, the best possible personnel protection – "Safety (really is) integrated"!

Torsten Borowski
BG Institute for Occupational Health & Safety; Saint Augustin
Group 5 "Accident Protection"
Peter Keil
Siemens AG, Erlangen – A&D MC, Automation and Drives, Motion Control

10.12 A synthesis of speed & safety

Safety Integrated for complex, special machine tools

Time is money. If you want to stay in the black when producing parts or you wish to reduce costs then speed is of essence. The sophisticated machine concepts from August Wenzler GmbH in Spaichingen permit cycle times to be achieved for their rotary transfer machines for machining large batches which some can only dream about. Innovative solutions are also in demand when it comes to safety technology. With the three large rotary cycle machines that Opel ordered from the Wenzler company, "Safety Integrated' celebrated a successful entry.

Using its technology, the Wenzler company produces complex, precision workpieces, for example, automobile chassis components. For the case being considered, wheel hub carriers and pivot axes are machined from aluminum with a unit machining time of only 17 seconds. This time is a real benchmark. This is complemented by other features such as a favorable price-performance ratio, the fact that the machines can be flexibly set-up and the experience which Wenzler has already gained in other projects in the automobile industry. All of these facts together convinced Opel to award Wenzler the three large rotary cycle machines to machine their chassis components. Not only this, each machine has 72 NC axes which also isn't an everyday occurrence - even for the high-tech Wenzler company.

The machine, in its present version, was developed in various phases over the last 20 years.

From 1983 onwards, the machine was equipped with a CNC control system which Wenzler themselves had developed. At the end of the nineties, Wenzler changed-over to using Siemens control systems.

Today, Wenzler has about 70 employees and constructs between 8 and 10 machines per year. Most of these machines are supplied to the automobile industry. The value of such large machines can easily reach between 1.5 and 2.5 million Euro, depending on the actual version.

High degree of productivity in the tightest space

The Wenzler MSC-8 B (multi-spindle center) is an 8-station machine. The 8 workpieces can be simultaneously machined by up to 14 tools.

The workpieces are mounted on satellite tables that can be swiveled so that 5-side machining - or by automatically turning-over - 6-side machining is also possible. Thanks to its rigid modularity, this flexible cell has the character of a standardized rotary interlinked machine with the performance of a special-purpose machine. Each movement is CNC controlled so that the full flexibility of the machine can be utilized in a machining cube of 400 x 400 x 400 mm. The central element is the 8-corner drum. This is suspended and supports the workpiece - is suspended. This guarantees optimum chip flow and good accessibility of the drum bearing and clamping equipment.

On the electrical side, the MSC-8B is equipped with the Siemens Sinumerik 840D machine control, and the matching Simodrive 611D digital drives, 1FT6 permanent-magnetic synchronous motors and the Profibus fieldbus. This is complemented by a series of distributed units. Just recently, Wenzler has also started to use the integrated safety functions “SINUMERIK Safety Integrated”.

Integrated safety technology

About five years ago, Siemens was the first drive manufacturer worldwide with integrated safety functions for personnel and machinery protection.

By integrating the safety functions, the drive system and the CNC control also handle the safety functions in addition to the control itself. The sa-fety functions include safely monitoring the speed, standstill and position as well as functions to logically combine signals in a safety-related fashion.

The logical operations and responses are realized within the system. All safety-related faults in the system always result in the potentially hazardous motion being safely shut down and the power to the motor being contactlessly interrupted. Motion is always stopped, optimally adapted to the state of the machine. When setting-up, this means a high degree of protection for personnel and additional protection for the machine, tool and workpiece in the automatic mode.
Safety Integrated is already in use in over 13.500 machines with over 80.000 drives. Machinery manufacturers can access a considerable amount of know-how when it comes to engineering new safety concepts.

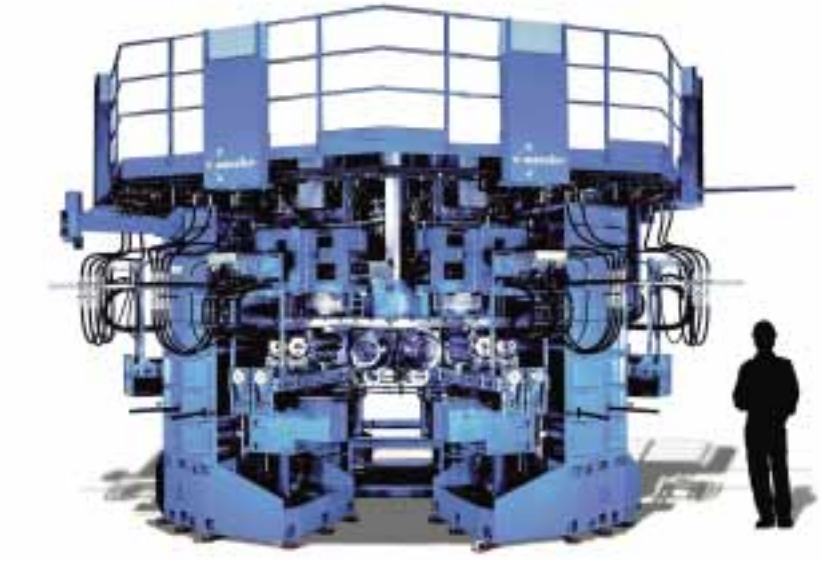
For the Opel machines from Wenzler, this involved 72 CNC axes and a total of 99 drives per machine. This presented both Wenzler as well as Siemens with new challenges - especially because almost all of the Safety Integrated functions, including the safe brake management as protection against vertical axes falling were to be implemented on these machines.

The Opel project

The Wenzler machines were used in the Opel project to produce aluminum hub carriers and pivot axes. Each type in the left/right versions is simultaneously machined so that after 4 workpieces, the components required for 1 automobile have been produced. Aluminum hub carriers and pivot axes are relatively new in chassis construction. Previously, Opel manufactured these parts out of gray cast iron. The performance and ride comfort of vehicles are improved by reducing the weight, especially the unsprung masses. The new aluminum version was able to reduce the weight by 6.6 kg. "The project was kicked-off in late Autumn 2000. In cooperation with Wenzler, a rough concept was initially drawn-up which indicated as to how such extensive safety integrated applications could be even approached", explained Ingrid Hölzer who was responsible on the Siemens side for this task. This concept used the control structure defined by the Wenzler company, which comprised eight NCUs. NCU1 was defined as master for the Safety Integrated functionality. The specialists from Wenzler - namely Ralf Rottler - wrote the software for the NC and the PLC sections of the control. "This was extremely successful" explained Ingrid Hölzer. Communications down to the level of the setting-up technicians was fantastic".

Higher degree of protection and flexibility

The advantages which Wenzler now sees, explained Jürgen Ruffieux, head of the electronics development department, "primarily in a higher degree of protection during the setting-up operation as well as in the higher flexibility for the setting-up personnel." Previously, safety devices and equipment had to be bypassed when setting-up the machine – this is now a thing of the past. The setting-up technicians are always protected.
Using Safety Integrated, Opel expected lower costs when installing the machine, shorter response times and a higher degree of safety due to automatic self-diagnostics and the crosswise monitoring using the PLC and NC. The new machines went into series production in the first quarter of 2002.



The MSC- 8B - a modular, rotary cycle machine that for Opel is equipped with 72 NC axes. The "naked" machine shows the design comprising individual and similar basic elements

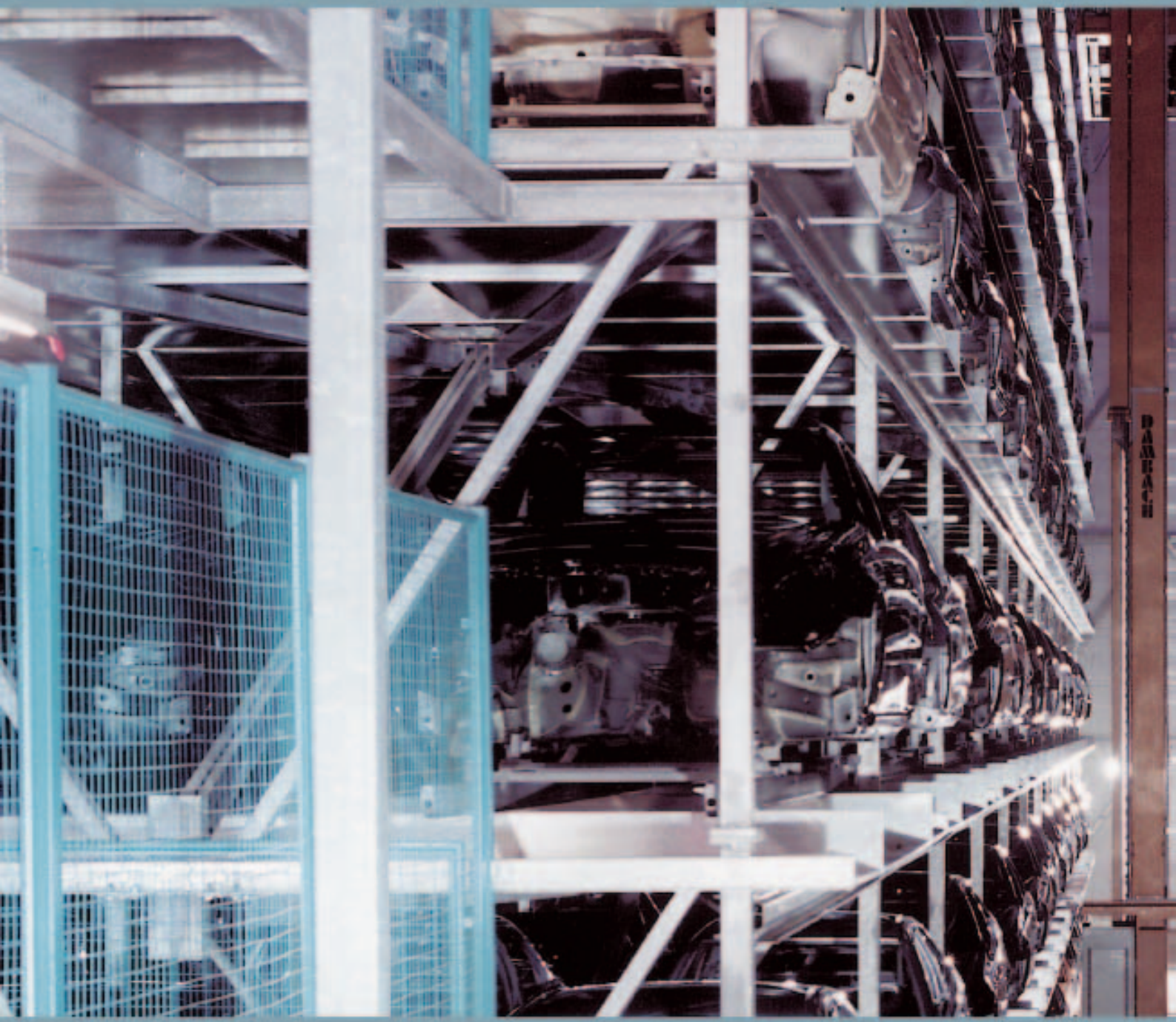
Aluminum reduces the weight of an automobile. In this particular case with Opel, these aluminum wheel hub carriers and pivot axes reduce the weight by 6.6 kg with respect to cast iron parts

10.13 Safe standstill in the printing industry

Increasing productivity and a high degree of cost consciousness in the printing machine industry is resulting in the fact that classic mechanical solutions (for example, line shafts) are being replaced by electric drives (mechatronics). On the other hand, this places higher demands on the safety technology which is used to monitor the drive. Previously, only a few drives had to be monitored from the safety aspect, whereas today, new concepts mean that many drives have to be incorporated in the monitoring system.

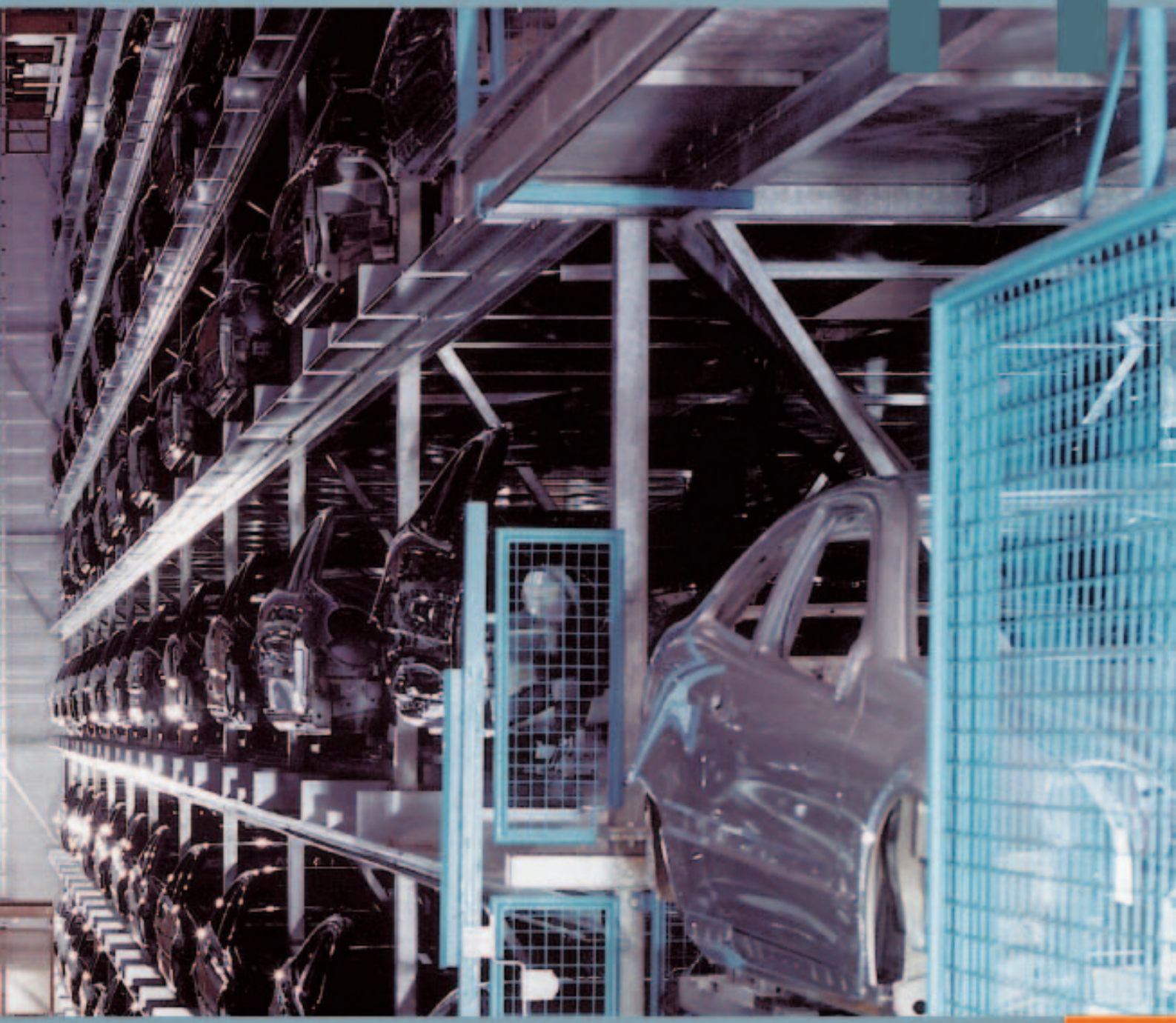
An especially high potential hazard is when operating personnel have to work on a printing machine with the protective devices open. Here, legislation demands that personnel must be protected against the drives undesirably starting by using suitable devices.

SIMOVERT MASTERDRIVES drives support this protective function. This prevents drives undesirably starting using an integrated safety relay. This means that the contactor on the motor side that was previously used can be eliminated. In the printing machine industry, systems with well over 100 drives are no longer a seldom occurrence. Significant time and cost savings were achieved by eliminating material and installation costs and due to the less space required in the control cabinet.



11

Appendix



11 Appendix

11.1 Terminology and abbreviations

Terminology

Actuator

An actuator converts electrical signals into mechanical or other non-electrical quantities.

Blanking

Using blanking, a specified section or area is suppressed from a protective field, e.g. a light curtain or light grid, i.e. it is disabled. There are two types of blanking: Fixed and floating blanking.

Fixed blanking

For fixed blanking, the selected area or range is fixed. This function is used, for example, if fixed objects protrude into the protective field.

Floating blanking

Floating blanking permits that normally one or two light beams in a protective field are interrupted without a stop signal being output from a light curtain. This function is required if the "permissible" interruption of the light beams does not refer to a fixed position in the protective field, e.g. if a moving cable enters the protective field.

Category

In EN 954-1 (prEN ISO 13849-1) this is used to "classify the safety-related parts of a control with reference to their immunity to faults and their behavior under fault conditions which is achieved as a result of the structural arrangement of the parts and/or their reliability."

Channel

Element or group of elements that executes a function independently.

2-channel structure

Structure that is used to achieve fault tolerance.

For example, a 2-channel contactor control can be achieved if at least two enable circuits are available and the main current can be redundantly switched-off or a sensor (e.g. Emergency Stop switch) is interrogated using two contacts that are then separately connected to evaluation unit.

Danger

Potential source of damage.
(from EN 292-1 or ISO 12100-1)

e.g. danger due to electric shock, danger due to crushing, ...

Emergency Stop

An operation in an emergency that is designed to stop a process or movement that is potentially dangerous (from EN 60204-1 Annex D).

EMERGENCY SWITCHING-OFF

Emergency Switching-off equipment

Arrangement of components that are intended to implement an Emergency Stop function (EN 418 or ISO 13850). (Note: Today, a differentiation is made between "Stopping in an emergency" and "Power off in an emergency".

Stopping in an emergency

A function which either avoids or minimizes impending or existing danger for persons, damage to the machine or when carrying out work;

– initiated by a single action of a person.
(EN 291-1 or ISO 12100-1)

Power off in an emergency

Power off in an emergency is achieved by disconnecting the machine from the supply subsequent to a Category 0 stop (EN 60204 1997). Power off in an emergency should be provided, in compliance with EN 60204-1 1997, where there is the possibility of danger due to electricity (electric shock).

Enabling device

Additional manually actuated control device that permits a specific function of a machine if it is continually actuated.

Fail-safe

The capability of a control to maintain a safe condition of the controlled equipment (e.g. machine, process), or to bring this into a safe condition when faults occur (failures).

Failure/fault

Failure

When a piece of equipment or a device is no longer capable of executing a specific function.

Fault

Unintentional status of a piece of equipment or device which is characterized by the fact that it is not capable of executing a specified function.

Note: “Failure” is an event and “Fault” is a condition.

Fault

Refer to “Failure / fault”.

Fault tolerance

Fault tolerance N means that a piece of equipment or device can still execute the specified task even when N faults are present. For N+1 faults, the piece of equipment or device fails when executing the specified function.

Feedback circuit

Circuit to monitor controlled contactors.

The function of contactors can be monitored by reading back the positively driven auxiliary contacts by an evaluation unit. If the contactor contacts are welded, the evaluation unit prevents a restart.

Functional safety

Part of the safety of a piece of equipment or device (e.g. machine, plant, which depends on the correct function.

Load group

A group of motor starters that is supplied through a power bus. A load group can be located within a potential group or can include parts of two potential groups.

Motor starter (MS)

Motor starters include direct and reversing starters. Starting and direction of rotation are determined using a motor starter.

Direct starter

A direct starter is a motor starter for one direction of rotation, which directly powers up or powers down a motor. It comprises a circuit-breaker and a contactor.

Reversing starter

A reversing starter is a motor starter for two directions of rotation. It comprises a circuit-breaker and two contactors.

Muting

Muting disables one or several safety functions for a limited time in line with specifications

Partial potential group

A partial potential group exists if within a potential group, the auxiliary voltage can be partially switched out.

Potential group

A group of motor starter and/or electronic modules which is supplied from a power module.

Redundancy

Availability of resources or equipment more than is actually required for its execution.

Requirement Class (AK)

Measure of the safety-related performance of control equipment. Defined in DIN V 19250 and DIN V VDE 0801.

Risk

Combination of the probability of the occurrence of damage and the extent of the damage.

Safety

Freedom from unacceptable risk.

Safety function

Function (e.g. of a machine or a control) whose failure (or breakdown) can increase the risk(s).

Safety functions of controls (EN 954 or prEN ISO 13849-1)

"A function, initiated by an input signal and processed by safety-related parts of controls that allows the machine to achieve a safe condition (as system)."

Safety goal

To keep the potential hazards for man and the environment as low as possible without restricting industrial production, the use of machines or the production of chemicals as far as absolutely necessary.

Safety Integrity Level (SIL)

In IEC 61508, this is defined as the measure for the safety performance of electrical or electronic control equipment. (-> Section 1)

Safety-related control function (IEC 62061)

Control function that is executed by a safety-related control system in order that a system goes into a safe condition (e.g. machine) or to avoid hazardous conditions occurring.

Safety-related control function

Slightly differing definitions are provided in the various Standards.

Stop

This is a function that is intended to avoid or minimize hazards to personnel, damage to the machine or the execution of operational processes. It has priority over every other operating mode.

Stop Category

A term which is used in EN 60204-1 to designate three different stopping functions.

Two-hand circuit

Control device, which requires that it is simultaneously actuated by both hands in order to activate hazardous machine functions and also maintain them.

Abbreviations

ANSI	American National Standards Institute
BGIA	German Technical Inspectorante
BWS	Electro-sensitive protective devices
CNC	Computerized Numerical Control
CPU	Central Processing Unit
DMS	Direct measuring system
FTS	Driverless transportation system
HMI	Human Machine Interface
IBS	Commissioning
IMS	Indirect Measuring System
KDV	Cross-checking
MRPD	Machine Readable Product Designation: Order No. of Siemens components
NC	Numerical Control
NCK	Numerical Control Kernel
NCU	Numerical Control Unit
NFPA	National Fire Protection Association
OP	Operator Panel
OSHA	Occupational Safety and Health Administration
PLC	Programmable Logic Control
PM	Positive-ground switching
PP	Positive-positive switching
S5	SIMATIC S5
S7	SIMATIC S7

11.2 References

[1] Position paper DKE 226.0.3: Safety-related functions electric drive systems in machines. Status 1/98.

[2] Schaefer, M.; Umbreit, M.: Drive systems and CNC controls with integrated safety. BIA Report No. 4/97

[3] Categories for safety-related controls acc. to EN 954-1. BIA Report 6/97.

[4] ZH1/419. Testing and certification regulations of the testing and certification bodies in BG-Prüfzert. Edition 10/1997.

[5] Reinert, D.;Schaefer, M.; Umbreit, M.: Drives and CNC controls with integrated safety. In: ETZ-Heft 11/98

[6] Safety-related data transfer; requirements as well as deterministic and probabilistic techniques; 1998, Uwe Jesgarzewski, Rainer Faller – TÜV Product Service

11.3 Contact – Internet Hotlines

Internet address:

General information

http://www.siemens.de/safety
http://www.siemens.de/automation

AS-Interface

http://www.siemens.de/as-interface

SIRIUS

http://www.siemens.de/sirius

SIGUARD

http://www.siemens.de/siguard

SIMATIC

http://www.siemens.de/simatic-controller
http://www.siemens.de/simatic-dp

SIMODRIVE 611, SIMODRIVE POSMO, SIMOVERT MASTERDRIVES

http://www.siemens.de/simodrive

SINUMERIK

http://www.siemens.de/sinumerik

Hotlines:

SIMATIC
++49(0)911-895-7000

SIRIUS
++49(0)911-895-5900

SINUMERIK
++49(0)180-5258008

11.4 Seminars available for safety technology, Standards and Directives

Because training is decisive for your success

SITRAIN® - the Siemens Training for Automation and Industrial Solutions - is there to support you in mastering all of your tasks.

With training from the market leader in automation, plant erection and support, you can certainly win when it comes to feeling comfortable in making the right decision. Especially when it involves optimally using products and efficiently using plants and systems. You can eliminate performance issues and problems in existing plants and systems and reliably exclude expensive planning mistakes from the very start.

When all is said and done, this signifies enormous benefits for your operation: Shortened start-up times, optimized plant and system sections, fast troubleshooting, lower downtimes. The result - a higher degree of profitability and lower costs.

Top trainers

Our trainers have in-depth experience in the field and also extensive didactic experience. Personnel that develop these training courses have a direct link to our product development groups and they directly pass on their knowledge to the trainers.

In-line with that required in practice

Because our trainers are very much in touch with what is required in practice, means that they can really communicate theoretical knowledge. But as everyone knows, theory can be somewhat dull, and this is why we place the highest significance on practical training - that represents up to halve of the course time. This means that you can immediately implement what you have learned in your day-to-day business. The training courses use training equipment that has been specifically developed for this purpose so that you feel absolutely confident in our training courses.

Wide variety of courses

We have a total of approximately 300 courses and provide training for the complete range of A&D products and to a large extent, plant solutions from I&S. Off-site training courses, self-learning software and moderated seminars in the web complement our classic range of courses.

Close to the customer

We are never far away. We are represented approximately 60 times in Germany and worldwide in 62 countries. Would you like personalized training instead of participating in our 300 courses? Our solution: We can tailor the training to your personal requirements.

We provide training courses in our training centers or also in your facility.

The right combination: Blended Learning

Blended Learning means a combination of various learning/training media and sequence of courses. For instance, a course in a training-center can be optimally supplemented by self-learning programs to prepare for a course or after a course. As a supplement, SITRAIN utilizes moderated online training in order to provide courses at scheduled times live in the Internet.

The combination is the clue. This is the reason that Blended Learning can provide know-how on complex subjects and train networked thought processes.
Spin-off:
Lower travel costs and non-productive times using training sequences that are independent of the training location and time.

The international learning portal

www.siemens.de/sitrain

All of the training possibilities at a glance! You can comfortably scan our global portfolio of training courses, you can call-up all of the course dates online, and courses where there is still space available are listed, updated on a daily basis. This means that you can directly register for the course you wish to participate in.

Subjects	Target group	Duration	Code
Safety Integrated Overview for planners	Decision-makers, sales personnel, project managers, project team members	2 days	ST-SIUEBP
Safety Integrated for developers	Programmers	3 days	ST-SIUEBE
Safety Integrated overview in the production industry	Decision makers, sales personnel, project managers, project team members, programmers, application engineers, commissioning engineers,	2 days	ST-SIUEBF
Engineering and programming with Distributed Safety	Programmers, commissioning engineers, application engineers	3 days	ST-PPDS
Engineering and programming with F systems in STEP7/ PCS7 environment	Programmers, commissioning engineers, application engineers	3 days	ST-PPFS
SIMATIC S7, S7-400 H system course	Programmers, commissioning engineers, application engineers	3 days	ST-7H400H
Product and application training for contact-less protective devices - SIGUARD	Decision-makers, sales personnel, commissioning engineers, application engineers, service personnel, operators, users	2 days	MP-BWS
SINUMERIK 840D, Safety Integrated service course	Service personnel, maintenance personnel	3 days	NC-84DSIS
SINUMERIK 840D, Safety Integrated engineering and commissioning	Commissioning engineers, application engineers, service personnel	5 days	NC-84DSIW
Electromagnetic compatibility in the field	Programmers, commissioning engineers, application engineers, service personnel, maintenance personnel	3 days	MP-EMVPRA
Explosion protection, basics	Decision makers, sales personnel, commissioning engineers, application engineers, service personnel, maintenance personnel	1 day	MP-EX-GRU
Explosion protection intrinsic safety	Decision makers, sales personnel, commissioning engineers, application engineers, service personnel, maintenance personnel	1 day	MP-EX-EIG

Safety Integrated Overview for Planners (ST-SIUEBP)

In this overview course, you will learn about everything that is required to plan a safe plant or system. You will get to know the appropriate legislation and Standards and understand how to transfer the resulting contents into you plant or system planning.

Contents

- Overview, legislation/standards
- Risk analysis, SIL Categories, Performance Levels, Safety Category
- Functional safety MM
- Application software development, V model
- Tasks of somebody that is responsible for functional safety
- Documents that must be requested or must be supplied, revision procedures
- Fault evaluation
- Probability of failure
- Qualifying the complete system - application examples with exercises
- Common Cause faults
- State-of-the-art safety-relevant systems
- Siemens solutions for machinery and process control

Target groups

Decision makers, sales personnel, project managers, project team members

Duration

2 days

Course fee

On request

Course location

Mannheim

Safety Integrated Overview for Development Engineers (ST-SIUEBE)

In this course, in addition to the contents of the overview course (ST-SIUEBP) you will obtain additional information regarding calculations required when planning a safe plant or system. The knowledge that is theoretically taught will be gone into more depth in examples and exercises that are in line with what is encountered in the field.

Contents

- Overview, legislation/standards
- Risk analysis, SIL Categories, Performance Levels, Safety Category
- Functional safety MM
- Application software development, V model
- Tasks of somebody that is responsible for functional safety
- Documents that must be requested or must be supplied, change requests
- Fault evaluation
- Probability of failure
- Qualifying the complete system
- Application examples with exercises
- Common Cause faults
- State-of-the-art safety-relevant systems
- Siemens solutions for machinery and process control
- FMEDA (Failure Modes, Effects and Diagnostic Analysis)
- ULM for safety technology
- Qualification, Common Cause
- Markov models
- Basic system structures
- Examples and exercises

Target group

Programmers

Duration

3 days

Course fee

On request

Course location

Mannheim

Safety Integrated, Overview in Production Technology (ST-SIUEBF)

This course provides you with the current situation as far as standards are concerned in production technology. You will also get to know how to correctly apply it in practice using selected examples. The objective of this course is to merge theory and practice. You will secure a high production quality and achieve competitive advantages by competently implementing this knowledge in your own operation.

Contents

- EC Machinery Directive
  - Basics, definitions, requirements, implementation, application on new machines and new machine equipment
  - Use when making modifications and upgrading
  - Evaluating conformity
- EC Directive
  - Basic, definitions, requirements, implementation
- Overview of the Standards
  - EN ISO 12 100 (EN 292), EN 1050 (ISO 14121)
  - EN 60204-1
  - EN 954-1, (prEN ISO 13849-1), EN ISO 13849-2, (EN 954-2)
  - EN 62061, IEC 61508
- Example from the field - automobile industry (paint shop, subsequent handling with transport using a rail-based system)
  - Standards and use
  - Applications
  - Configuration/design and implementation of the risk analysis using conventional wiring and bus-based solutions.

Target group

Decision makers, sales personnel, project managers, project team members, programmers, commissioning engineers, users

Duration

2 days

Course fee

On request

Course location

Nuremberg, Mannheim

Engineering and programming with Distributed Safety (ST-PPDS)

Participants learn how to handle, engineer, program, commission, diagnose and troubleshoot distributed safety systems. This includes the fail-safe CPUs 315F-2DP, CPU 317F-2DP, CPU 416F DP and the IM151-F CPU. The F-FBD and/or F-LAD programming languages are used for the fail-safe program generation.

Contents

Overview, Standards and Directives

- AS S7-300F (principle, system design and I/O)
- Engineering fail-safe I/O with distributed safety
- Programming a safety-related user program
- Fail-safe communications PROFIsafe (CPU-CPU communications, Master-slave communications)
- Diagnostic capability (CPU diagnostics, I/O diagnostics, other diagnostic tools)
- Exercises on configuring the I/O, communications, troubleshooting
- Examples for programming (Emergency Stop, protective door, safety-related shutdown, passivation, special programming issues)

Target groups

Programmers, commissioning engineers, application engineers

Duration

3 days

Course fee

On request

Course location

Essen, Hanover, Mannheim, Nuremberg

Engineering and programming F systems in the STEP7 / PCS7 environment (ST-PPFS)

Course participants learn how to handle, engineer, program, commission, diagnose and troubleshoot F systems. These include fail-safe CPUs 414-4 H and CPU 417-4 H that are optionally available as high availability versions. The CFC programming language is used to program the safety-related applications that these CPUs control.

Contents

- Overview, redundant systems (H/F difference, availability redundant systems, regulations)
- AS S7-400F (principle, system configuration and I/O)
- Engineering fail-safe I/O with F system
- Configuring a safety-related user program using CFC
- Profisafe fail-safe communications
- Exercises to configure I/O communications, troubleshooting
- Example for programming, special program issues

Target group

Programmers, commissioning engineers, application engineers

Duration

3 days

Course fee

On request

Course location

Essen, Mannheim, Nuremberg

SIMATIC S7, S7-400 H system course (ST-7H400H)

The course participants learn how to handle, engineer, commission and diagnose and troubleshoot the fault-tolerant SIMATIC S7-400H automation systems.

Contents

- Overview, redundant systems (H/F difference, availability, redundant systems)
- AS S7-400H (principle, system configuration and I/O, synchronization, coupling and updating the reserve, self-test, principle mode of operation, fault/error processing)
- Configuring with STEP7/HSys (system parameterization, system handling, fault diagnostics, documentation)
- Exercises to configure the I/O, troubleshooting, programming examples

Target groups

Programmers, commissioning engineers, application engineers

Duration

3 days

Course fee

On request

Course location

Essen, Nuremberg

Product and application training for contactless protective devices - SIGUARD (MP-BWS)

In this workshop you will learn how to handle and use electro-sensitive protective devices (light curtains, light grids and laser scanners) belonging to the SIGUARD series.

Contents

- European Directives
- Safety-related parts of controls acc. to EN 945-1
- SIGUARD safety light curtains
- SIGUARD safety laser scanners
- Calculating safety distances and clearances acc. to EN 999
- Evaluation units
- Testing electro-sensitive protective devices
- Diagnostics

Target group

Decision makers, sales personnel, commissioning engineers, application engineers, service personnel, operating personnel, users

Duration

2 days

Course fee

On request

Course location

Mannheim, Nuremberg-Moorenbrunn

SINUMERIK 841D, Safety Integrated Service&Maintenance course (NC-84DSIS)

This course provides participants with knowledge and skill sets that are required to service and maintain a machine equipped with SINUMERIK 840D and Safety Integrated. After participating in the course, course participants can troubleshoot and resolve faults. After repair/software upgrades, course participants can check the safety-related functions and accept them.

Contents

- General information on safety-related systems
- System prerequisites
- Description of the basic safety-related functions
- Safe programmable logic
- Connecting sensors/actuators
- Test stop
- Description of the machine data and interface signals
- Procedure when commissioning and troubleshooting
- Evaluating diagnostic and alarm displays
- Circuit examples for Safety Integrated
- Acceptance report
- Practical training exercises on fault finding and service at training models equipped with digital feed and main spindle drives

Target groups

Service personnel, maintenance personnel

Duration

3 days

Course fee

On request

Course location

Chemnitz, Düsseldorf, Nuremberg-Moorenbrunn

SINUMERIK 840D, Safety Integrated Engineering and Commissioning (NC-840DSIW)

This course shows participants how to engineer and commission the Safety Integrated functionality with a SINUMERIK 840D. After the course, participants can engineer, test and commission the Safety Integrated function and a SINUMERIK 840D special system configuration with safety-related functions.

Contents

- General information on safety-related systems
- System prerequisites
- Description of the basic relevant function
- Safe programmable logic
- Connecting sensors/actuators
- Test stop
- Safety-related communications with PROFIsafe
- Safe brake management
- Description of the machine data and interface signals
- Procedure when commissioning and troubleshooting
- Evaluation of diagnostic and alarm displays
- Circuit examples for Safety Integrated
- Acceptance report
- Practical exercises to engineer, commission and service equipment on training models equipped with digital feed and main spindle drives

Target groups

Commissioning engineers, application engineers, service personnel

Duration

5 days

Course fee

On request

Course location

Nuremberg-Moorenbrunn

Electromagnetic compatibility in the field (MP-EMVPRA)

This course addresses all personnel in development, mechanical design, production and service that require practical know-how and skill sets regarding EMC for their day-to-day work. Video films on the individual subjects show the effects of EMC phenomena in practice with the appropriate measures to prevent them or resolve them. The objective of this training course is to learn how to avoid or resolve EMC faults.

Contents

- What you have to especially observe when planning plants
- What an EMC correct electrical cabinet looks like, especially with variable-speed drives, background information on the individual cabinet design rule and regulations
- How a differentiation can be made between software, hardware and EMC faults and disturbances
- Which test equipment makes sense when troubleshooting and how it is used
- Tips and tricks when troubleshooting - how you can subsequently increase the noise immunity
- Causes, effects and countermeasures relating to static discharge
- The disadvantages and advantages of different grounding techniques, what are the causes of potential differences, how is potential bonding implemented
- What causes harmonics, their effects and how they can be avoided, line resonance effects, reactor circuits, blocking circuits etc.
- When can filters be used and how
- Everything about connecting cable shields
- Motor bearing currents, what causes them, effects, counter-measures
- Aspects relating to lightning protection, from identifying the hazard up to using protective elements
- Introduction into the various Standards, CE, caution, new EMC Directive!

Target groups

Programmers, commissioning engineers, application engineers, service personnel, maintenance personnel

Duration

3 days

Course fee

On request

Course location

Refer to the Internet

Explosion protection, basics (MP-EX-GRU)

This course provides manufacturers and users of electrical equipment for hazardous zones theoretical and practical know-how relating to electrical explosion protection. This includes basic physical data, information on the appropriate legislation, possible protective measures for electrical equipment and information on how they can be used. A background to explosions and interrelationships and hazards are highlighted using a presentation and video film clips.

Contents

- Explosion, prerequisites for explosion
- Ignition sources
- Primary and secondary explosion protection
- Safety-related parameters
- Temperature classes, explosion groups Zone classification
- Basic legislation relating to explosion protection
- Class of protection for electrical equipment
- Building regulations for equipment according to EN 50 014-50 028
- Designating and tagging electrical equipment
- The special explosion protective measures for a specific piece of equipment are discussed

Target groups

Decision makers, sales personnel, commissioning engineers, application engineers, service personnel, maintenance personnel

Duration

1 day

Course fee

On request

Course location

Mannheim

Explosion protection, intrinsic safety (MP-EX-EIG)

This course provides participants that develop, construct and support explosion-protected electrical equipment and intrinsically safe plants in depth perspectives of the class of protection, intrinsic safety and the design of operating equipment with intrinsically safe circuits. The use of intrinsically safe equipment is explained using application examples. Further, the required proof of intrinsic safety when combining intrinsically safe and associated equipment is explained using examples.

Contents

- Building regulations for equipment according to DIN EN 50 014 and 50 020
- Basics information on the class of protection, intrinsic safety
- Ignition limiting characteristics
- Intrinsically safe and associated electrical equipment
- Characteristics of special intrinsically safe equipment, tagging/designation
- Requirements on erecting equipment in the individual zones acc. to DIN 0165
- Combining equipment to form intrinsically safe plants/systems (DIN EN 50 039)
- Constructing intrinsically safe plants/systems acc. to VDE 0165
- Operation, service & maintenance, testing equipment

Target group

Decision makers, sales personnel, commissioning engineers, application engineers, service personnel, maintenance personnel

Duration

1 day

Course fee

On request

Course location

Mannheim

For actual dates, course locations and prices, please refer to the Internet under:

www.siemens.de/sitrain

11.5 List of contents

Impressum:

Safety Integrated:
System Manual Safety Technology, 5th Edition

Published by:
Siemens AG
Automation and Drives Group
Postfach 4848, D-90327 Erlangen

Authors responsible for the contents:
Georg Becker (A&D PT7)
Robert Gassner (A&D CD)
Maximilian Korff (A&D CD)
Hartmut von Krosigk (A&D ATS)
Jürgen Lange (A&D MC)
Stefan Lechner (A&D PT7)
Peter Maurer (A&D MC)
Guillaume Maigret (A&D CD)
Bernard Mysliwiec (A&D AS)
Uwe Schade (A&D CD)
Carsten Schmidt (A&D CD)
Jürgen Strässer (A&D MC)
Lutz Teschke (I&S IS)
Bernhard Wöll (A&D AS)

Concept, Support, Coordination and Editors:
Wolfgang Kotitschke (A&D SE)
Johanna Gebhardt (A&D CD)
Sybill von Hofen (A&D GC)

Layout:
NEW ORANGE DESIGN, Obernzenn

Printing:
Farbendruck Hofmann, Langenzenn

Subject to change without prior notice

Siemens Aktiengesellschaft

Automation and Drives
Low Voltage Controls and Distribution
P.O. Box 3240, D-91050 Erlangen

Automation and Drives
Industrial Automation Systems
P.O. Box 4848, D-90327 Nürnberg

Automation and Drives
Motion Control Systems
P.O. Box 3180, D-91050 Erlangen

www.siemens.de/safety

Order No. 6ZB5 000-0AA02-0BA1
Printed in Germany
Dispostelle 06 345 / SEK 30 296