SIEMENS

Ingenuity for life

Whitepaper

Five steps to safer machines

A primer on safety technology in standard automation

usa.siemens.com/motioncontrol

Competent support throughout the entire lifecycle provides protection for worker and line alike

Specific drive control requirements for test stands

With an innovative and comprehensive safety technology and product portfolio, as well as competent support services in application engineering and field operations, today's machine component suppliers must offer substantial advantages — throughout all phases of the product lifecycle. These advantages must apply to the machine builder and end-user of any industry, if there is to be seamless collaboration in this key area of plant operations. This whitepaper will cover how to help stay in compliance with applicable standards and regulations, maintenance and training protocols, as well as the other steps necessary to build and operate safe machines on the factory floors. Functional safety in machine building is a critical component in market success, while operational integrity of the motion control and automation safety systems represent practical necessities for all companies today. As the founder of our company, Werner von Siemens, observed in 1880, "The prevention of accidents must not be understood as a regulation required by law, but as a precept of human responsibility and economic reason."

Integrated Safety

Fast and easy implementation of functional safety in the design of any machine requires a comprehensive portfolio of control, drive and switching technology, which covers every requirement placed upon the functional safety of machines and systems in operation.

Integrated safety facilitates the seamless integration of safety technology in standard automation concepts. This entails decisive advantages, both for machine manufacturers and system operators. These advantages include reduced engineering expenditures, increased availability and system consistency. Overall, this means that an integrated safety approach in design significantly eases and accelerates the realization of safe and productive machines. With an integrated safety concept onboard, end-users receive reliable protection of people, machines and the environment, and all benefit from maximum and sustainable efficiency and flexibility.

The functional safety of machines and systems in the market today is subject to increasing requirements. On the one hand, this is the result of strict legal regulations for the protection of people to be met by machine builders and operations management. On the other hand, any potential risks posed by a machine should be largely eliminated from the start for economic reasons. Lastly, a safety system should minimize unnecessary trips, thereby maximizing uptime.

Here are five steps to consider, when planning a machine build:

STEP ONE
Risk assessment

The machine builder is required to implement risk assessment in order to identify all hazards associated with any proposed system; to assess and evaluate the respective risks; and to design and construct the system in consideration of such hazards. Risk assessment implementation is to be considered a design-accompanying process which is to be carried out by experts of various disciplines. In this context, the EN ISO 12100 standard offers support by description of an iterative procedure for risk assessment. Also, in the U.S., this is covered by the ANSI B11.0 standard.

STEP TWO
Risk reduction

Following risk assessment, a decision as to whether risk reduction measures must be initiated will be required. Such risk reduction comprises design measures and technical protective equipment, as well as training measures for users — and can be divided into three levels:

Level 1 — Safe design

Safe design can, for example, be ensured through the integration of safety in the machine (covers, fences etc.). These measures take top priority within the scope of risk reduction. They are to ensure the following:

- Avoidance of crushing points
- Avoidance of electric shock
- Concepts for machine shutdown in case of emergency
- Concepts for operation and maintenance

Level 2 — Technical protective measures

A safety function must be defined for each hazard which cannot be eliminated by means of design measures. As shown in the following example, such safety functions can be executed by a safety system:

"When the protective door is opened during normal operation, the motor has to be switched off."

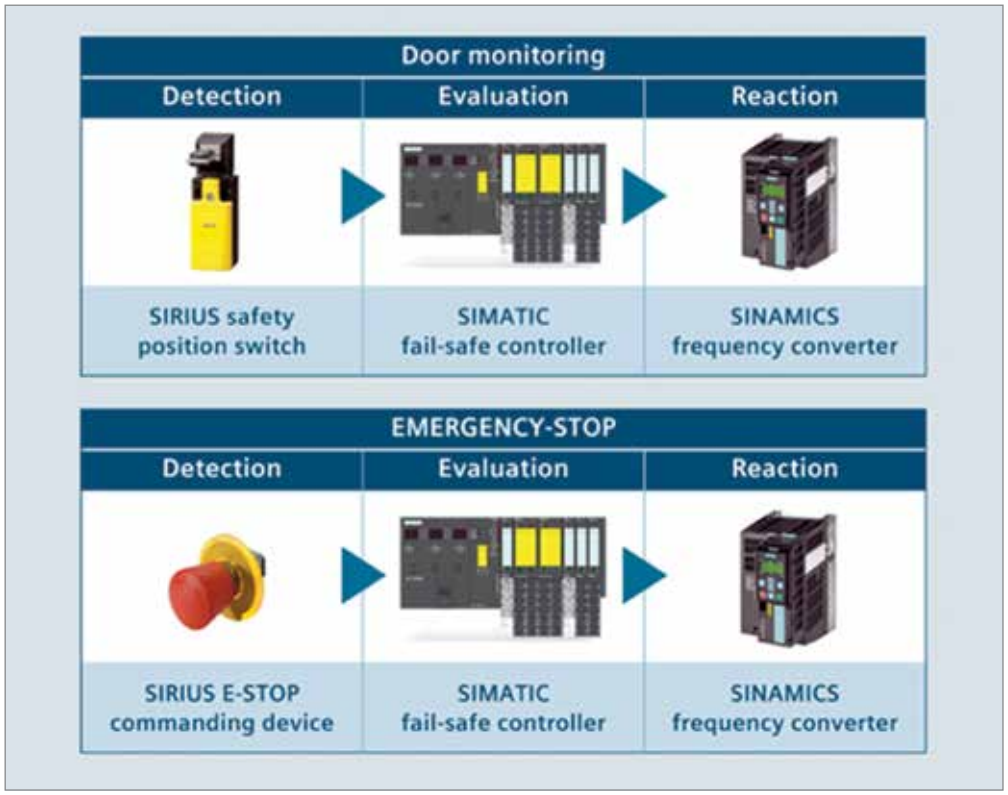


Figure 1:
Safety function example

A safety system executes safety functions and comprises these sub-systems:

- Detecting (position switch, E-STOP, light curtain etc.)
- Evaluating (fail-safe controller, safety relay etc.)
- Reacting (contactor, drives etc.)

Level 3 — User information on residual risks

As a matter of law, users must be informed of any possible residual risks. However, such information does not replace the request for safe design and technical protective measures, but is merely intended to supplement such measures. User information might typically comprise:

- Warnings in the operating instructions
- Special work instructions
- Notes on the use of personal protective equipment
- Pictograms

Machine builders can ensure compliance with the new machinery directives and resulting export capability and liability by the application of the EN ISO 13849-1 and IEC 62061 standards. Besides qualitative considerations, also quantitative aspects are introduced by these standards. Protective measures for risk reduction which are described by means of safety functions can be derived from the process of risk assessment. The solution of the safety function is then verified and evaluated with the help of hardware and, if required, software components, until the safety integrity as required in the risk assessment is achieved.

IEC 62061 standard

Functional safety of safety-related, electrical, electronic and programmable control systems

The IEC 62061 standard specifies requirements and provides recommendations for the design, integration and validation of safety-related, electrical, electronic and programmable electronic control systems (SRECS). A system designed in accordance with IEC 62061 complies with all relevant requirements of IEC 61508. The IEC 62061 standard does not define any requirements for the capacity of non-electrical (e.g. hydraulic, pneumatic, electromechanical) safety-related control elements for machines.

Application of IEC 62061

The IEC 62061 (EN 62061) standard can be applied for the evaluation of all electrical and electronic systems, independent of their category. The requirements can also be applied to non-electrical controls, given they comply with ISO 13849. Sub-systems (SRP/CS) assessed in accordance with EN ISO 13849-1 can be used comparably.

A comparison table with Safety Integrity Level (SIL) and Performance Level (PL) values, based upon PFHD values, is available for this purpose.

ISO 13849-1 standard

Safety-related parts of control systems

The ISO 13849-1 standard may be applied to safety-related parts of control systems (SRP/CS) and all types of machines — regardless of the technology and energy used (electrical, hydraulic, pneumatic, mechanical etc.). It also specifies special requirements for SRP/CS with programmable electronic systems.

Most important changes in the standard include:

- Performance level (beyond the exclusive consideration of categories)
- Incorporation of development and application of programmable electronic systems with safety function (PES) in safety-related parts of control systems
- Extended consideration of the control and avoidance of systematic failures and faults

Application of ISO 13849-1

Application of the ISO 13849-1 standard is recommended when the safety function is mainly realized on the basis of fluid power (hydraulic, pneumatic).

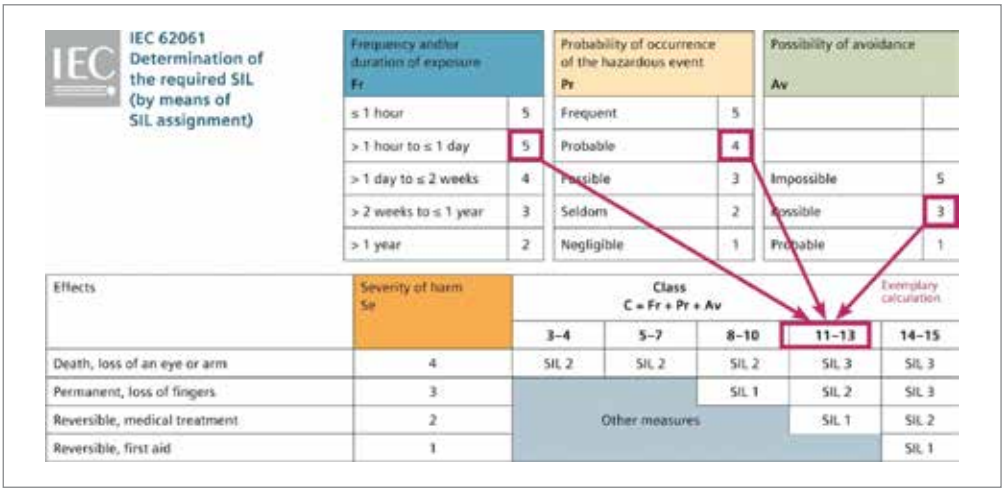
Both standards

The risk of each hazard is estimated on the basis of the risk element determination.

This determination is based upon:

- Severity of the harm involved
- Frequency and duration of a person's exposure to the hazard
- Probability of occurrence of a hazardous event
- Possibilities of avoiding or limiting the harm

The required Safety Integrity Level (SIL in accordance with IEC 62061) or Performance Level (PL in accordance with ISO 13849-1) is determined on the basis of these criteria.



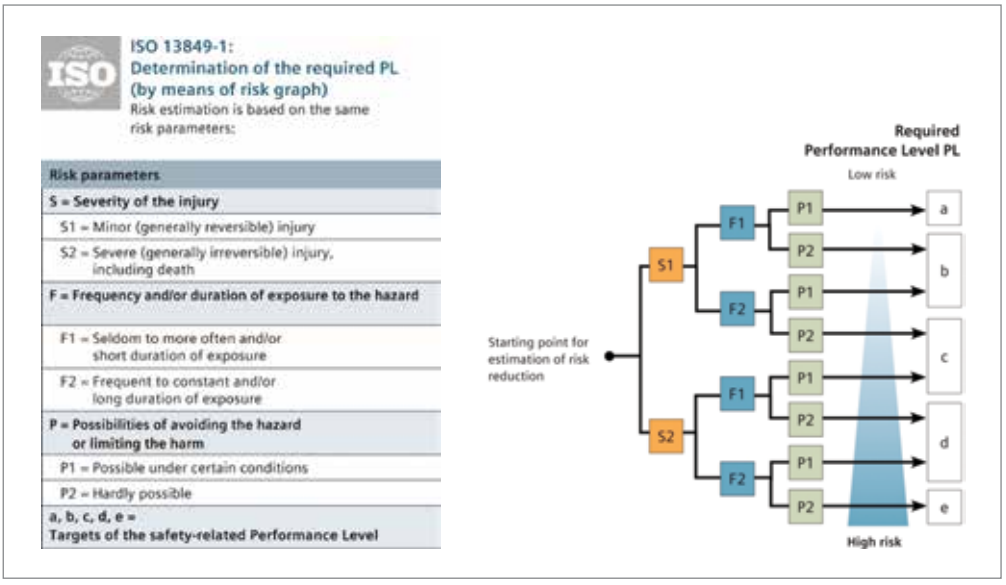
IEC 62061
Determination of the required SIL (by means of SIL assignment)

Frequency and/or duration of exposure Fr		Probability of occurrence of the hazardous event Pr		Possibility of avoidance Av	
≤ 1 hour	5	Frequent	5		
> 1 hour to ≤ 1 day	5	Probable	4		
> 1 day to ≤ 2 weeks	4	Possible	3	Impossible	5
> 2 weeks to ≤ 1 year	3	Seldom	2	Possible	3
> 1 year	2	Negligible	1	Probable	1

Effects	Severity of harm Se	Class C = Fr + Pr + Av				
		3–4	5–7	8–10	11–13	14–15
Death, loss of an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, loss of fingers	3			SIL 1	SIL 2	SIL 3
Reversible, medical treatment	2	Other measures			SIL 1	SIL 2
Reversible, first aid	1					SIL 1

Exemplary calculation

Figure 2:
Safety Integrity Level (SIL)



ISO 13849-1:
Determination of the required PL (by means of risk graph)
Risk estimation is based on the same risk parameters:

Risk parameters
S = Severity of the injury
S1 = Minor (generally reversible) injury
S2 = Severe (generally irreversible) injury, including death
F = Frequency and/or duration of exposure to the hazard
F1 = Seldom to more often and/or short duration of exposure
F2 = Frequent to constant and/or long duration of exposure
P = Possibilities of avoiding the hazard or limiting the harm
P1 = Possible under certain conditions
P2 = Hardly possible
a, b, c, d, e = Targets of the safety-related Performance Level

Figure 3:
Performance Level (PL)

STEP THREE
Implementation of technical protective measures and validation

Validation is important in the development of safety-related components for control systems. A validation plan should include all documents of the validation procedure, the relevant operating and environmental conditions and the analysis and test methods applied. For this purpose, a test plan must first be drawn up with the relevant test specification, including a detailed description of the tests, the test setup, the test environment, the test programs and error simulations. The test plan must also include the expected results of the individual tests. The validation can start in any phase of the machine life, but must be completed before delivery and acceptance by the customer.

Validation target

Assurance of compliance with requirements

- Specified in European directives
- Resulting from the customer's specification documents, the machine's application and any further country-specific requirements applicable to the machine
- The purpose of the validation procedure is to ensure that the implemented safety functions make the required contribution to risk reduction to ensure that the machine is safe and remains so.

STEP FOUR
Market availability with documentation

All machine-relevant information must be available with full documentation when the machine is made available to the market. This comprises: customer specification documents, technical documentation, certificate of conformity, acceptance report (if applicable), transport documents, etc.

STEP FIVE
Product monitoring in the field

Every manufacturer is required to monitor their product by means of a survey for any hidden defects after it has been placed on the market. For example, information as to whether the product is actually used as originally intended, as well as information regarding its behavior over the course of its lifecycle is to be collected. In particular, dangerous defects as well as misuse or incorrect product handling are to be rectified by means of corresponding measures. The user must be informed of any discovered hidden defects.

Added value for machine builders and system operators

Consistent integration of safety technology in standard automation

The integration of safety technology in standard automation concepts entails considerable and sustainable user benefits for enhanced competitiveness. Machine builders benefit from reduced hardware and significantly simplified engineering. The result: considerably faster realization of machines and systems, as well as easier adjustability to new requirements. The advantages for system operators: they are provided with safe and more productive machines and systems. A single integrated system of safety technology and standard automation reduces downtimes thanks to improved diagnostics, which also increases the system availability for production. Retrofits and modernization are simplified — due to flexible, modular, expandable concepts, machines and systems can be upgraded to state-of-the-art technology even faster and more efficiently.

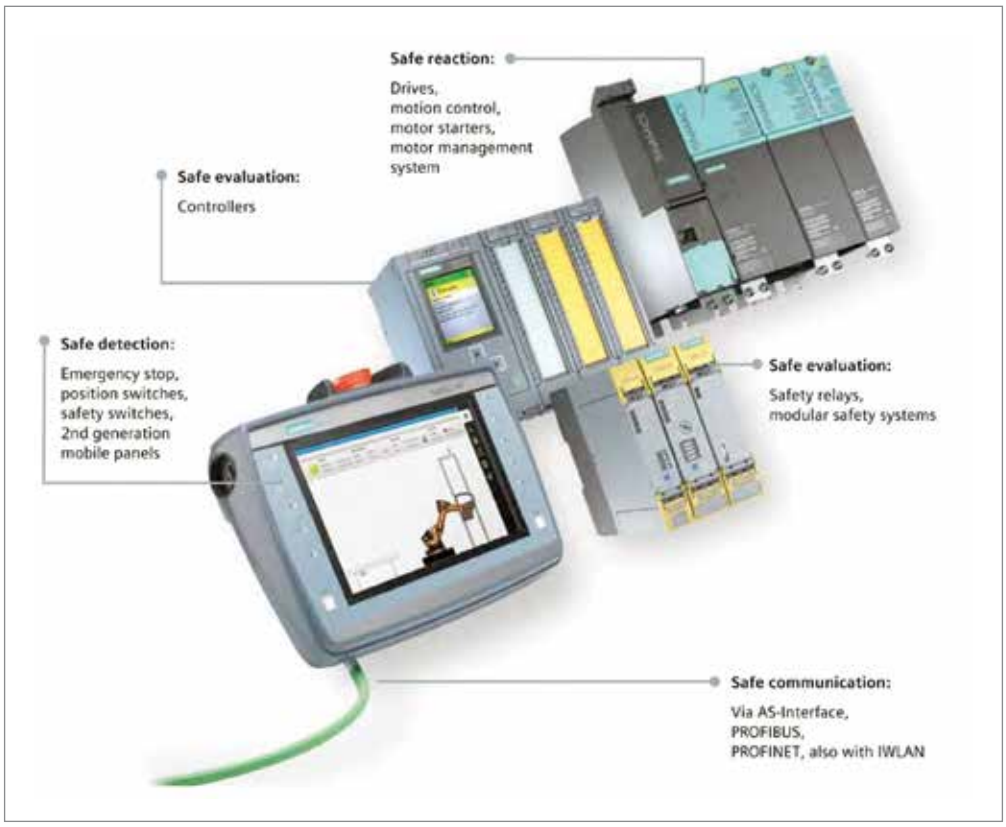


Figure 4

Drives with integrated safety functions

Electrically-driven power units and machine components frequently bear enormous risk potential. Rotating units such as saws, rollers and spindles may lead to severe or even fatal injuries. The same applies to linear motion machine units such as handling axes and machine slides.

Easier and faster realization of standard-compliant, powerful safety concepts

Drives with integrated safety functions facilitate the easy realization of safety concepts. Previously required electromechanical components and corresponding wiring are eliminated. The transfer of safety-relevant signals can be realized via standard field buses, which additionally minimizes wiring complexity and expenditures. Furthermore, drives with integrated safety functions support the implementation of much more powerful safety concepts — both in terms of functionality and response times. In many cases, this often results in increased productivity.

Five steps to safer machines

A primer on safety technology in standard automation

Prepared by
John Krasnokutsky

Marketing Director
Siemens Industry, Inc.
Digital Factory — Motion Control

john.krasnokutsky@siemens.com

Published by
Siemens Industry, Inc.

5300 Triangle Parkway, Suite 100
Norcross, GA 30092

(770) 871-3800

Order No. DRWP-5STSM-1117

Printed in USA

usa.siemens.com/motioncontrol