SIEMENS

SINUMERIK

Safety Integrated

System Manual

Edition 07/2015

Answers for industry.

SIEMENS

SINUMERIK

SINUMERIK 840D sl / 828D
Safety technology with SINUMERIK Safety Integrated

System Manual

07/2015

A5E36262894B-AA

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E36262894B-AA
℗ 07/2015 Subject to change

Table of contents

Fundamental safety instructions for the software documentation (for all product families) 1

1.1 Fundamental safety instructions

1.1.1 General safety instructions

⚠WARNING

Risk of death if the safety instructions and remaining risks are not carefully observed

If the safety instructions and residual risks are not observed in the associated hardware documentation, accidents involving severe injuries or death can occur.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

⚠WARNING

Danger to life or malfunctions of the machine as a result of incorrect or changed parameterization

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization (parameter assignments) against unauthorized access.
- Respond to possible malfunctions by applying suitable measures (e.g. EMERGENCY STOP or EMERGENCY OFF).

1.1.2 Industrial security

Note

Industrial security

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit this address (http://www.siemens.com/industrialsecurity).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit this address (http://support.automation.siemens.com).

⚠ WARNING

Danger as a result of unsafe operating states resulting from software manipulation

Software manipulation (e.g. by viruses, Trojan horses, malware, worms) can cause unsafe operating states to develop in your installation which can result in death, severe injuries and/or material damage.

- Keep the software up to date.
  You will find relevant information and newsletters at this address (http://support.automation.siemens.com).
- Incorporate the automation and drive components into a holistic, state-of-the-art industrial security concept for the installation or machine.
  You will find further information at this address (http://www.siemens.com/industrialsecurity).
- Make sure that you include all installed products into the holistic industrial security concept.

Introduction

2

Manufacturers and operators of technical equipment and products are responsible in minimizing the risk from plants, machines and other technical equipment in accordance with state-of-the-art technology. Safety systems are designed to minimize potential hazards for both people and the environment by means of suitable technical equipment, without restricting industrial production and the use of machines more than necessary.

This document defines the safety functions and concepts that are available for the SINUMERIK control family in conjunction with the SINAMICS drive system.

Regulations and standards 3

3.1 Overview

There are guidelines, standards and regulations for nearly all areas of technology. These rules help ensure that the technical equipment provides an adequate level of protection for users and safety during operation.

The observance of standards is not a safety measure. This means that minimum requirements are satisfied and the current state-of-the-art technology and knowledge is observed. To ensure the functional safety of a machine or plant, the safety-related parts of the protection and control devices must function correctly. In addition, the systems must behave in such a way that either the plant remains in a safe state or it is brought into a safe state when a fault occurs. Functional safety means that all parts of machines function correctly and have sufficient equipment to minimize risks. In this case, it is necessary to use specially qualified technology that fulfills the requirements described in the relevant standards.

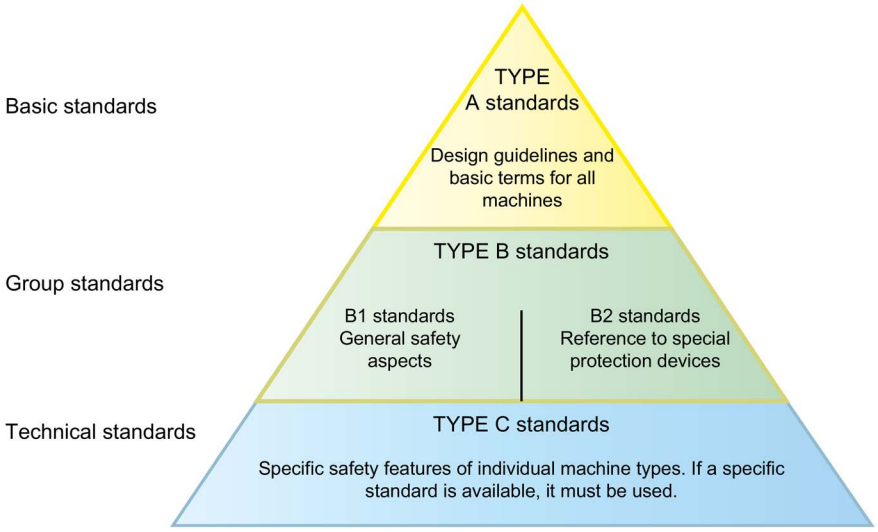
The requirements to achieve functional safety are based on the following basic goals:

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

The level of the functional safety achieved is expressed using different terms in the standards.

In IEC 61508, EN 62061, EN 61800-5-2 by the "Safety Integrity Level" (SIL) and in EN ISO 13849-1 by the "Performance Level" (PL).

The safety-related standards are subdivided into the types A, B and C.



Type A standards

IEC 61508	Functional safety
EN ISO 12100	Risk analysis
EN ISO 14121	Risk analysis

Type B standards

DIN EN 61800-5-2	Adjustable speed electrical power drive systems
IEC 62061	Safety of machinery
EN ISO 13849	Safety of machinery
IEC 60204	Electrical equipment of machines

Figure 3-1 Standards pyramid

3.2 Machinery directive (2006/42/EG)

The machinery directive is a European directive. Its range of validity therefore covers 28 member states (status February 2015) of the European Union. The machinery directive also applies in Switzerland, Liechtenstein, Norway, Iceland and Turkey. The machinery directive has no legal effect in all other countries.

In order that European directives, such as the machinery directive, take effect legally in the member states, they have to be transposed into national legislation in each member state.

The machinery directive is intended for manufacturers that produce machines in the European Union as well as manufacturers and importers that import machines into the European Union from non-European countries.

The manufacturer or importer of a machine **must** verify that the machine complies with the basic requirements of the machinery directive.

The following standards can be applied to satisfy the requirements of the machinery directive.

3.3 IEC 61508

Functional safety of electrical/electronic/programmable electronic safety-related systems

Description

IEC 61508 is an international standard for the development of electrical, electronic and programmable electronic systems (E/E/PES) that perform a safety function. The standard can be applied for all safety-related systems that contain such components (E/E/PES) and whose failure would mean a significant risk for people or the environment. IEC 61508 is not harmonized in line with any EU directives, which means that an automatic presumption of conformity for fulfilling the protective requirements of a directive is not implied. However, the manufacturer of a safety-related product can use IEC 61508 to fulfill basic requirements from the European directives according to the new concept.

3.4 EN ISO 13849

Safety of machinery – safety-related components of control systems, Part 1: General design guidelines, Part 2: Validation

Description

EN ISO 13849-1 is based on the previous standard EN 954-1, but also requires a quantitative consideration of the safety functions.

Its area of application covers safety-related components of control systems and all types of machines, regardless of the technology used (electrical, hydraulic, pneumatic, mechanical, etc.).

The following safety-related parameters are required for components/devices:

- Category (structural requirement)
- PL: Performance Level
- MTTFd: Mean Time To Dangerous Failure
- DC: Diagnostic Coverage
- CCF: Common Cause Failure

The standard describes how the Performance Level (PL) is calculated based on the PFH value (**P**robability of dangerous **f**ailure per **h**our) for safety-related components of control systems and complete safety functions based on designated architectures (categories B - 4). The five Performance Levels (a, b, c, d, e) represent the different probability values of a dangerous failure per hour.

With nonconformance, EN ISO 13849-1 refers to EN 61508.

As ISO 13849 considers all types of machines, irrespective of the technology used, this standard is preferred by the manufacturers of machine tools.

3.4.1 Performance Level

With EN ISO 13849, the result of a risk evaluation is indicated by the Performance Level for the respective safety function. Depending on the determined Performance Level, the safety function must be assigned a corresponding PFH value.

The following table shows the relationship between Performance Level and PFH value:

Performance Level	PFH value (Probability Of Dangerous Failure Per Hour)
a	≥ 10^{-05} to < 10^{-04}
b	≥ 3 x 10^{-06} to < 10^{-05}
c	≥ 10^{-06} to < 3 x 10^{-06}
d	≥ 10^{-07} to < 10^{-06}
e	≥ 10^{-08} to < 10^{-07}

3.4.2 Categories

The categories for the components/devices are described in the following.

Category B

Single-channel structure.

The occurrence of a fault can result in the loss of the safety function.

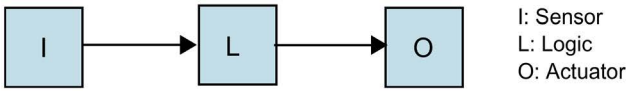


Figure 3-2 Sensor logic actuator

Category 1

Single-channel structure.

The occurrence of a fault can result in the loss of the safety function, but the probability of an occurrence is less than in Category B.

Well-proven components and well-proven safety principles must be implemented.

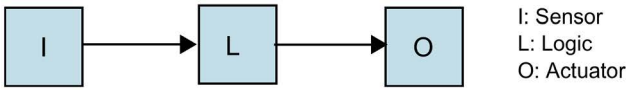


Figure 3-3 Sensor logic actuator

Category 2

Single-channel structure with test channel.

The safety function must be tested at regular intervals by the machine control system.

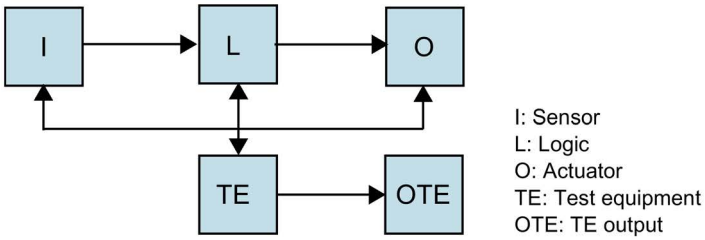


Figure 3-4 Sensor logic actuator test device output TE

Category 3

Two-channel structure.

When a single fault occurs, the safety function is always maintained.

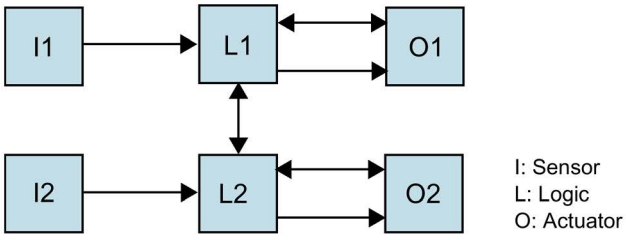


Figure 3-5 Sensor logic actuator Cat 3 and Cat 4

Category 4

Two-channel structure.

Single faults must be detected at or before the request for the safety function. If this is not possible, an accumulation of undetected faults must not result in the loss of the safety function.

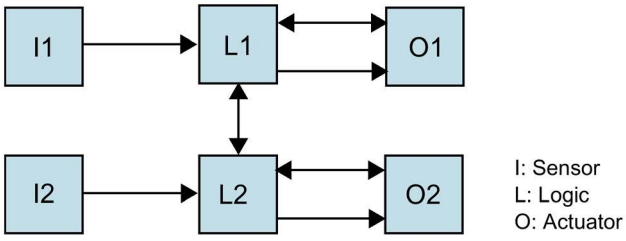


Figure 3-6 Sensor logic actuator Cat 3 and Cat 4

3.5 IEC 62061

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

Description

EN 62061 (identical to IEC 62061) is a sector-specific standard under IEC 61508. It describes the implementation of safety-related electrical control systems of machines and takes into account the complete lifecycle - from the conceptual phase to de-commissioning. The standard is based on the quantitative and qualitative analyses of safety functions.

Sector-specific standards should use the basic approaches of IEC 61508 and apply them for the respective area of application. For example, machine sector, power plant sector, medical sector, etc.

The IEC 62061 standard describes the risk to be minimized and the ability of the control system to minimize this risk in the sense of the SIL (Safety Integrity Level). Three SILs are used in the machine sector whereby SIL 1 is the lowest and SIL 3 is the highest safety integrity level.

3.5.1 Safety Integrity Level

The result of a risk evaluation for a safety function using IEC 62061 is the Safety Integrity Level (SIL). Depending on the determined SIL, the safety function must be assigned a corresponding PFH value.

The following table shows the relationship between the SIL and PFH value:

Safety Integrity Level	PFH value
SIL 1	≥ 10^{-06} to < 10^{-05}
SIL 2	≥ 10^{-07} to < 10^{-06}
SIL 3	≥ 10^{-08} to < 10^{-07}

3.6 Relationship between SIL, PL and PFH value

The following table shows the relationship between the Performance Level, PFH value and Safety Integrity Level:

Performance Level (PL) (EN ISO 13849)	PFH value (Probability of dangerous failure per hour)	Safety Integrity Level (SIL) (IEC 62061)
a	≥ 10^{-05} to < 10^{-04}	-
b	≥ 3 x 10^{-06} to < 10^{-05}	1
c	≥ 10^{-06} to < 3 x 10^{-06}	1
d	≥ 10^{-07} to < 10^{-06}	2
e	≥ 10^{-08} to < 10^{-07}	3

3.7 EN 61800-5-2

Adjustable-speed electrical power drive systems, Part 5-2: Safety requirements - Functional safety

Description

This standard defines requirements and gives recommendations for the design and development, integration and validation of safety-related power drive systems with adjustable speed (PDS(SR)) with regard to their functional safety.

3.8 EN 60204-1

Safety of machinery - Electrical equipment of machines - Part 1: General requirements

Description

As standard part of EN 60204, EN 60204-1 controls the general specifications and recommendations for the safety, correct functioning and maintenance of the electrical equipment of machines.

The purpose of the rules is to avoid dangerous situations and their risks and to take safety measures into account during the construction. It contains general requirements and recommendations for the electrical, electronic and programmable electronic equipment of machines.

The standard part:

- Promotes the safety of persons and property
- Maintains the correct functioning
- Simplifies service and maintenance

3.9 C standards

The C standards are specific technical machine safety standards that contain detailed safety requirements for a specific machine or group of machines of the same type.

If a C standard exists for the relevant machine type, it has preference over a B or A standard. If no special C standards exists for the machine to be planned, the risk reduction must be made in accordance with A and B standards.

Examples of C standards:

DIN EN 12417 Machine tools – safety – machining centers

DIN EN 12717 Safety of machine tools – drilling machines

DIN EN 13128 Safety of machine tools – milling machines (including drilling machines)

DIN EN 13218 Machine tools – safety – stationary grinding machines

DIN EN ISO 23125 Machine tools – safety – turning machines

Safety functions

4

SINUMERIK Safety Integrated provides integrated safety functions that support the implementation of highly effective personnel and machine protection.

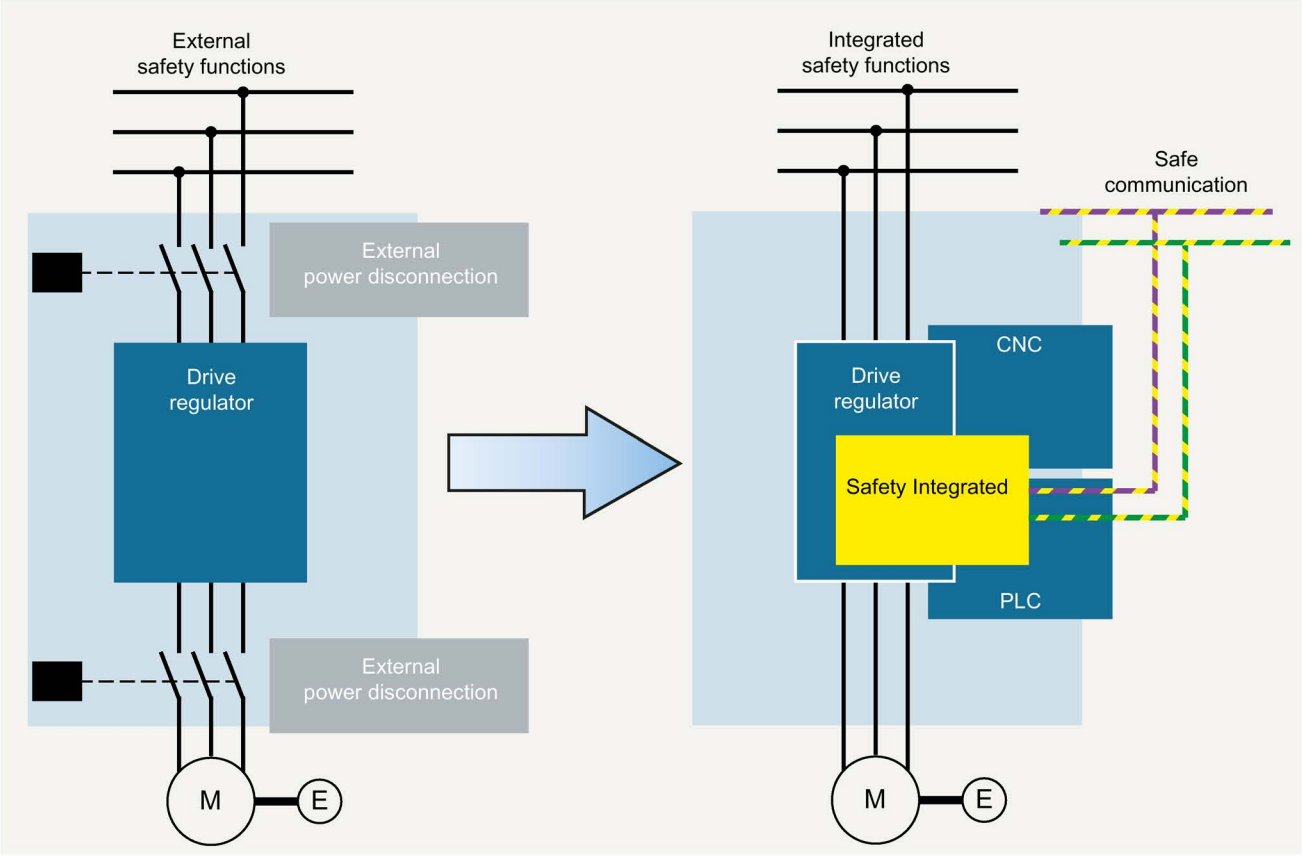


Figure 4-1 Comparison between external and integrated drive safety functions

The safety functions comply with the requirements of Category 3 as well as Performance Level d according to DIN EN ISO 13849-1 and Safety Integrity Level SIL 2 according to DIN EN 61508.

As a consequence, the essential requirements relating to functional safety can be simply and cost-effectively implemented.

The range of functions includes, for example:

- Functions for safety monitoring of velocity and standstill
- Functions for establishing safe boundaries in work spaces and protected spaces
- Direct connection of all safety-related signals and their internal logic combination

Note

Refer to the current Description of Functions for the relevant control family as to which of the current safety functions described in the following are available for the individual SINUMERIK control.

Basic differentiation of the safety functions for the SINUMERIK controls:

- SINAMICS Safety Integrated basic functions
- SINAMICS Safety Integrated extended functions
- SINUMERIK Safety Integrated safety functions integrated in the system

The following table shows a comparison of the safety functions for SINAMICS and SINUMERIK:

SINAMICS Safety Integrated basic functions	SINAMICS Safety Integrated extended functions	SINUMERIK Safety Integrated safety functions integrated in the system
Safe Torque Off (STO)	Safe Torque Off (STO)	Safe Torque Off (STO)
Safe Stop 1 (SS1)	Safe Stop 1 (SS1)	Stop A
Safe Brake Control (SBC)	Safe Brake Control (SBC)	Stop B
Stop A	Stop A	Stop C
Stop F	Stop F	Stop D
-	Safe Operating Stop (SOS)	Stop E
-	Safe Stop 2 (SS2)	Stop F
-	Safe Speed Monitor (SSM)	Safe Operating Stop (SOS)
-	Safely-Limited Speed (SLS)	Safe Brake Control (SBC)
-	Safe Acceleration Monitor (SAM)	Safe Speed Monitor (SSM)
-	Safely-Limited Position (SLP)	Safely-Limited Speed (SLS)
-	Safe Position (SP)	SLS Override
-	Safe Direction (SDI)	Safe Acceleration Monitor (SAM)
-	-	Safe Cam (SCA)
-	-	Safely-Limited Position (SLP)
-	-	Safe Programmable Logic (SPL)

The SINAMICS Safety Integrated basic functions are included as standard in the basic scope of SINAMICS.

Software licenses are required for the SINAMICS Safety Integrated extended functions and for the SINUMERIK Safety Integrated safety functions integrated in the system.

4.1 Safe Torque Off (safe standstill)

Safe Torque Off (STO) electronically safely disconnects the energy supply to the motor in the event of a fault or in conjunction with a machine function. This is performed axis-specifically and is contactless. The motor is not electrically isolated from the drive module.

Applications:

- Always active after emergency stop
- Turning a spindle by hand when protective doors are open

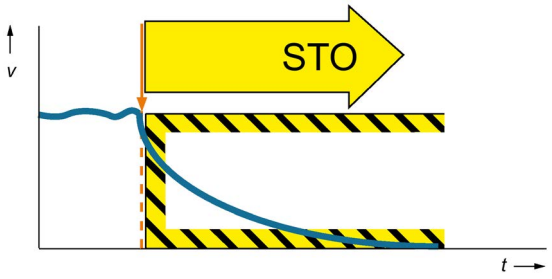


Figure 4-2 Safe Torque Off

4.2 Safe Stop 1

With the Safe Stop 1 (SS1) function, stopping of the drive according to EN 60204-1: 2006, Stop Category 1 can be implemented. The drive decelerates along a ramp once Safe Stop 1 has been selected, and goes into the Safe Torque Off (STO) state once the delay time has expired.

Application:

- Shutdown for emergency stop

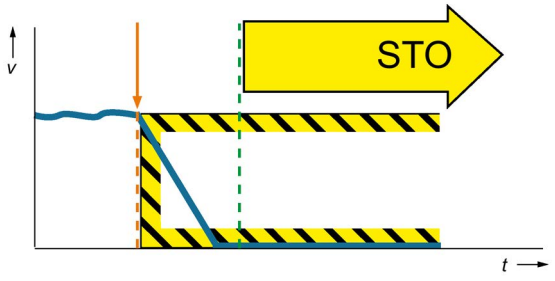


Figure 4-3 Safe Stop 1

4.3 Safe Brake Control

The Safe Brake Control (SBC) function is used to control holding brakes that function according to the closed-circuit principle (e.g. motor holding brake).

The brake is controlled via a two-channel output of the SINAMICS Motor Module.

SBC (if configured) is always triggered together with STO.

Application:

- Control of a holding brake for axes subject to gravity

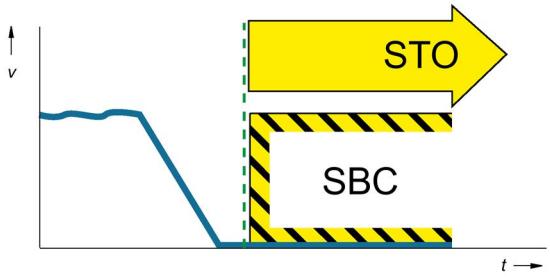


Figure 4-4 Safe Brake Control

4.4 Safe Operating Stop

This Safe Operating Stop (SOS) function serves for fail-safe monitoring of the standstill position of an axis or spindle. The drives remain fully functional in position or speed control and are monitored for position.

Applications:

- Working in a hazard area with protective doors open
- Axes with asymmetrical workpieces are held in position
- Vertical axes are held in position

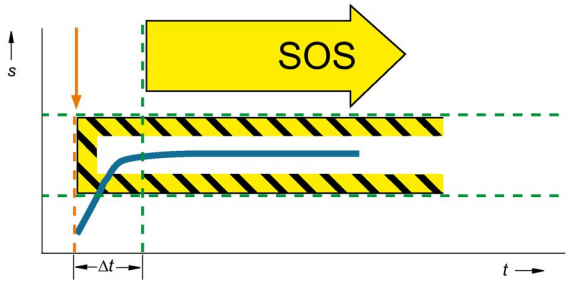


Figure 4-5 Safe Operating Stop

4.5 Safe Stop 2

With the Safe Stop 2 (SS2) function, stopping of the drive according to EN 60204-1: 2006, Stop Category 2 can be implemented. The drive decelerates along a ramp once Safe Stop 2 has been selected, and goes into the Safe Operating Stop (SOS) state once the delay time has expired or when a configured speed limit is exceeded.

Application:

- Operator protection

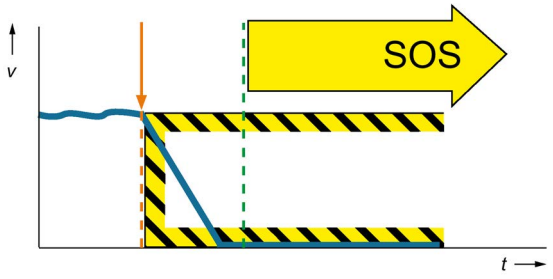


Figure 4-6 Safe Stop 2

4.6 Safe Speed Monitor (n < nx)

The Safe Speed Monitor (SSM) function supplies a safe output signal when the motor speed (n) is below a specified limit value (n_x).

This safe signal unlocks a protective door, for example.

Application:

- Release of the protective door only when all drives are stationary

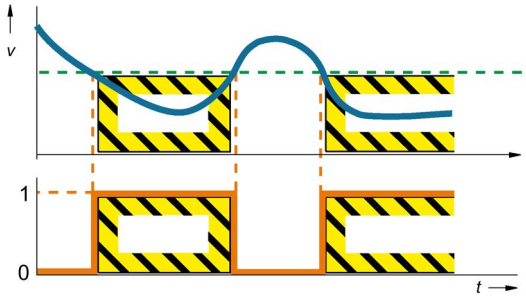


Figure 4-7 Safe Speed Monitor

4.7 Safely-Limited Speed

The Safely-Limited Speed (SLS) function serves for fail-safe monitoring of the load-side speed of an axis or spindle.

Four different speeds (SLS1, SLS2, SLS3, SLS4) can be parameterized for each axis or spindle.

For the SINUMERIK 840D sl, the safely-limited speeds SLS2 and SLS4 can be calculated with 16 different percentage values (SLS Override) so that there are up to 34 different speed values available for each axis.

Applications:

- Traversing the axes or spindles with open protective door → operator protection
- Burst protection, e.g. for grinding wheels or lathe chuck → machine protection

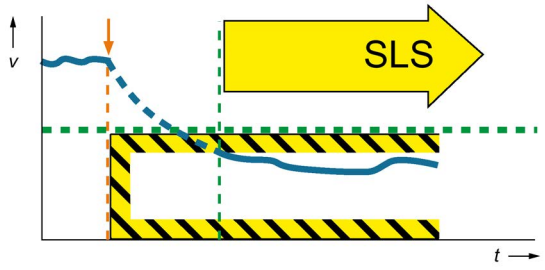


Figure 4-8 Safely-Limited Speed

4.8 Safe Acceleration Monitor

For STOPs B and C or for SS1 and SS2, the Safe Acceleration Monitor (SAM) function monitors whether the drive speed increases.

If the speed increases during a braking operation, an STO is triggered immediately and the relevant drive coasts to a standstill. Further acceleration is therefore excluded.

Application:

- Monitoring of the braking operation

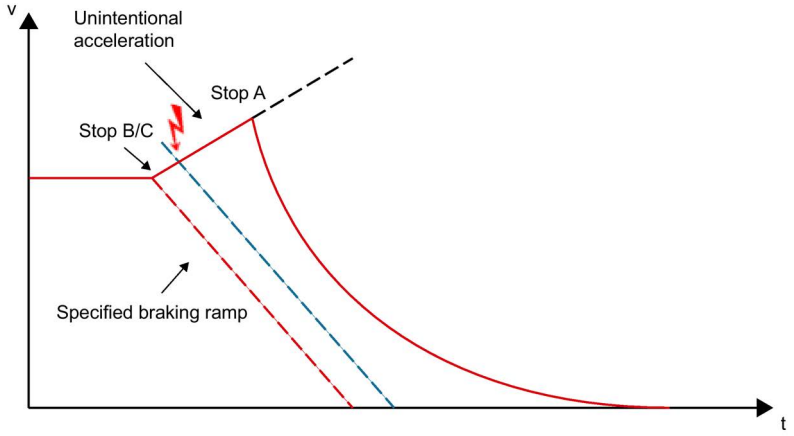


Figure 4-9 Safe Acceleration Monitor

4.9 Safe Cam

30 Safe Cam (SCA) are available for the SINUMERIK 840D sl? When a cam position is approached, a safe signal is generated which can be processed further.

Different working or protection areas can be defined with the Safe Cam function or safety functions switched.

Application:

- Definition of working or protection areas
- Safe switchover of safety functions (e.g. switching of SLS levels)

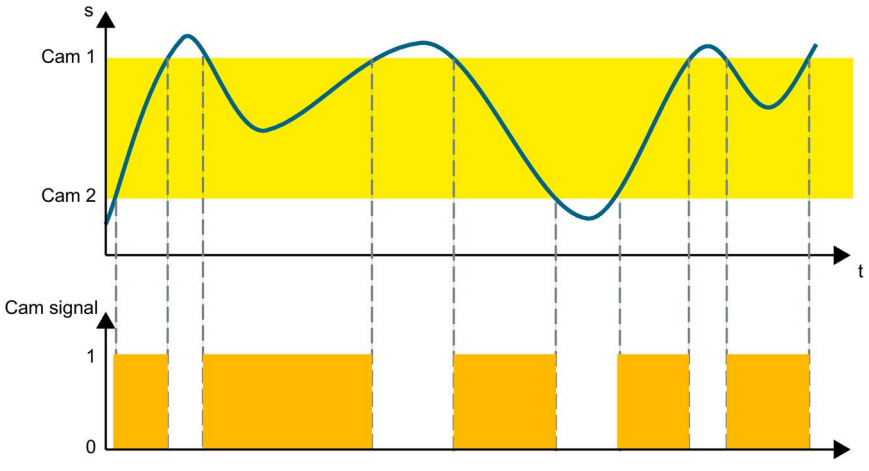


Figure 4-10 Safe Cam

4.10 Safely-Limited Position (safe software limit switch)

An axis-specific traversing range limitation can be implemented with the Safely-Limited Position (SLP) safety function. Hardware limit switches that are subject to faults and expensive can therefore be omitted.

It is possible to switch between two different software limit switch pairs.

If a software limit switch is crossed, Safety Integrated triggers a stop function parameterized by the machine manufacturer.

Application:

- Traversing range limitation for axes

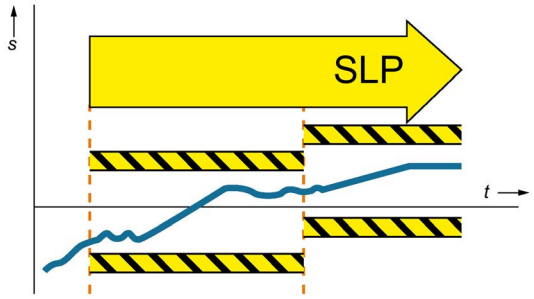


Figure 4-11 Safely-Limited Position

4.11 Safe Programmable Logic

The Safe Programmable Logic (SPL) enables the direct connection of all safety-related sensors and actuators and their internal logic combination.

The Safe Programmable Logic is structured redundantly and comprises a subprogram in the SINUMERIK 840D sl (NCK) and a standard STEP 7 program in the integrated PLC. There is a crosswise data and result comparison between these two programs.

Applications:

- Safe logic operation of fail-safe sensors and actuators without additional hardware
- Selection of the safety functions
- Processing of the status signals from the axis monitoring channels

4.12 Safe Direction (safe direction of rotation)

The Safe Direction (SDI) safety function is a SINAMICS Safety Integrated extended function. The direction of rotation of an axis or spindle is monitored safely with this safety function.

The safety function is available in conjunction with the SINUMERIK 828.

Applications:

- Retraction after violation of the safe software limit switch
- Monitoring of a milling spindle for tools that can only work in one direction

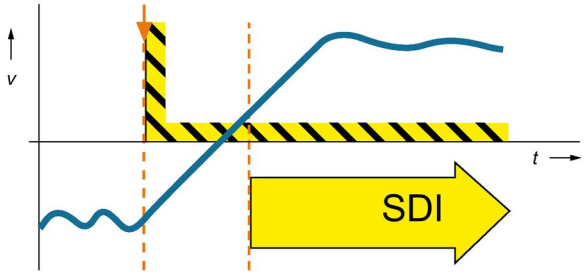


Figure 4-12 Safe Direction

4.13 Stop variants

Safe stops are used to stop a drive in motion and bring it to a standstill. The type of stop response that occurs in the event of errors can either be permanently specified by the system or configured by the machine manufacturer.

In this way, the shutdown of the machine can be optimally adapted to the respective situation.

In the following list, the Stop B can be compared to an SS1 and the Stop C to an SS2.

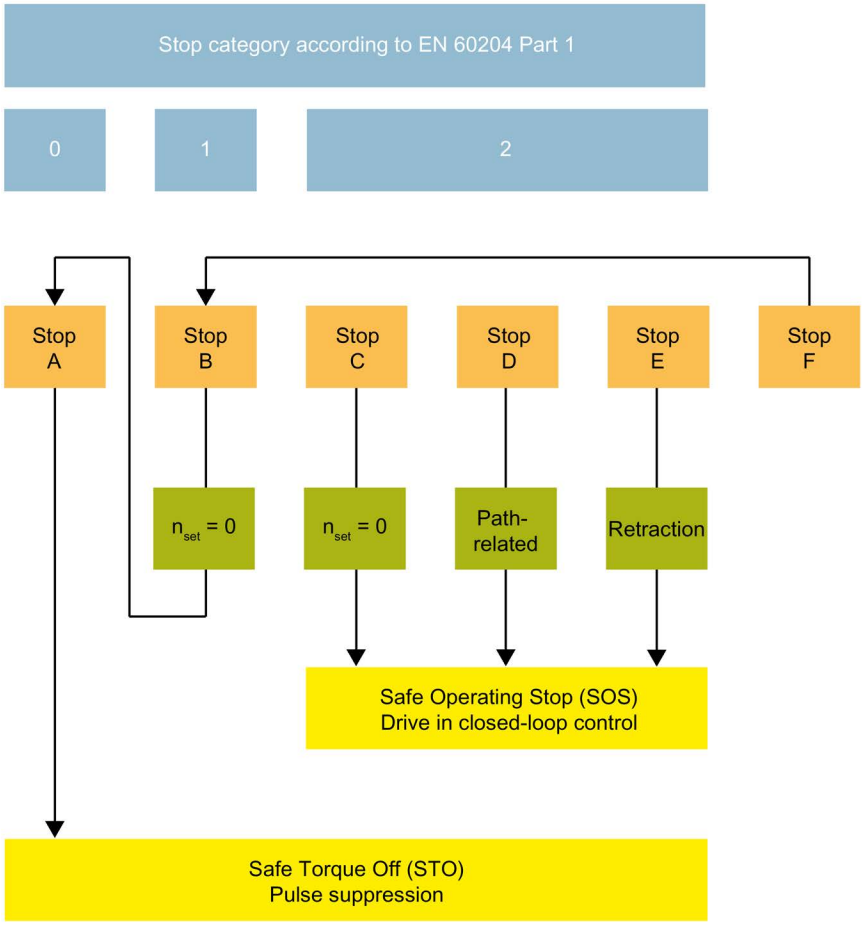


Figure 4-13 Overview of the stop variants

4.13.1 Stop A

With Stop A (corresponds to Stop Category 0 according to EN 60204-1, without electrical isolation), the drive is switched directly to zero torque via the Safe Torque Off function. A drive that is still running coasts to a standstill. A drive at standstill cannot be started again accidentally.

Application:

- E.g. for safety faults

4.13.2 Stop B

The drive is braked at the current limit under speed control and brought to a safe standstill (corresponds to Stop Category 1 according to EN 60204-1, without electrical isolation).

Application

- E.g. when SOS responds

4.13.3 Stop C

The drive is braked at the current limit under speed control and brought to a safe standstill (corresponds to Stop Category 2 according to EN 60204-1).

A Stop C followed by a Stop A is normally selected in the case of an emergency stop because this is the quickest way of stopping a drive.

Application:

- Operator protection

4.13.4 Stop D

The drives are braked together path-related (interpolatory) on the contour and brought to a safe operating stop.

Application:

- Protection for tool and workpiece (machine protection)

4.13.5 Stop E

The drives are braked together, including a jerk motion during which the tool and workpiece are separated from one another, path-related and brought to a safe operating stop.

Application:

- Machine protection

4.13.6 Stop F

The Stop F is permanently assigned to the crosswise result and data comparison (CDC) and cannot be changed by the user.

If a discrepancy is determined in the monitoring channels of Safety Integrated, a Stop F is triggered.

Depending on the parameter assignment, a Stop A or Stop B response is triggered.

Applications:

- Detection of errors during the crosswise data and result comparison
- Detection of communication errors between SINUMERIK and the drive
- Detection of encoder errors

4.14 Safe Brake Management

Axes and mechanical systems can drop due to gravity when the drives are switched off. Dangerous motion can result for vertical axes or for rotary axes or spindles with asymmetric weight distribution.

For this reason, a drive must be held safely in position in a de-energized state. This is usually implemented through a holding brake. The reliability of this holding brake is an essential part of the protection against falling on vertical axes.

Safe Brake Management consists of the Safe Brake Control and the Safe Brake Test.

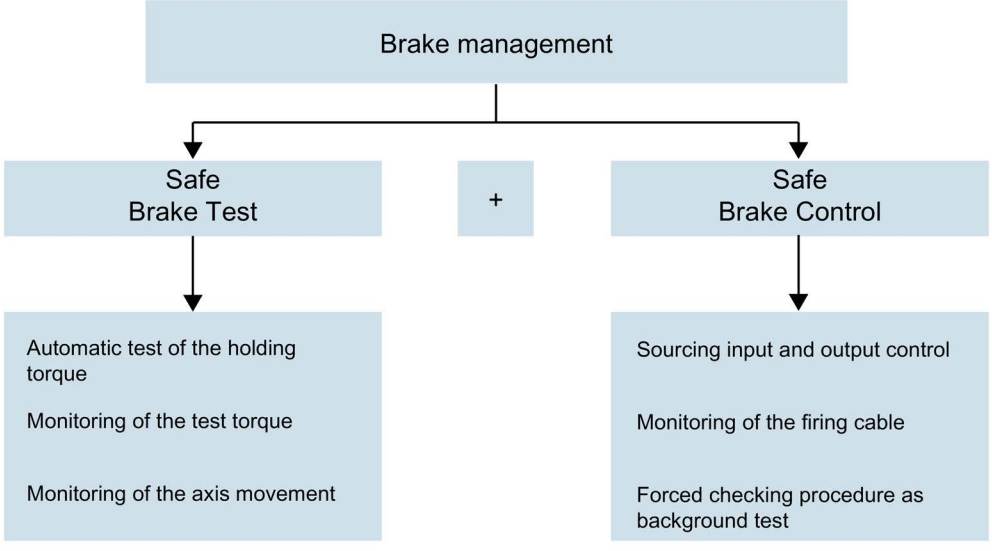


Figure 4-14 Safe Brake Management components

4.14.1 Safe Brake Control

The Safe Brake Control function (SBC) is used to control holding brakes that function according to the closed-circuit principle (e.g. motor holding brake).

The brake is controlled via a two-channel output of the SINAMICS Motor Module.

SBC (if configured) is always triggered together with STO.

4.14.2 Brake test (diagnostics function)

The brake test checks whether the expected holding torque is still available. The drive moves specifically against the closed brake and applies the test torque – there should be no axis movement. However, if an axis movement is detected, it must be assumed that the brake holding torque is no longer sufficient to hold the axis in position. In this case, the relevant axis must be traversed to a safe position and the brake checked and repaired, if required.

4.15 SLS-specific setpoint limitation

The SG (SLS) specific setpoint limitation is implemented in a single channel in the SINUMERIK 840D sl and therefore not a safety function. This function limits the speed setpoint depending on the safe speed which is currently active.

This prevents a violation of the selected safe speed level and the associated stop response.

The safety of the operator is ensured through the selected SLS level and the possible use of an acknowledgment button.

Application:

- Testing of new programs with open protective door with reduced speed without exceeding the SLS level

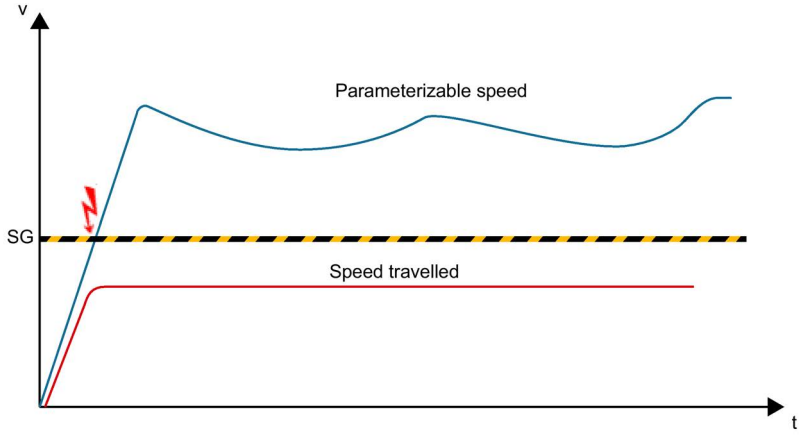


Figure 4-15 Method of operation of the SLS-specific setpoint limitation

Control safety concepts

5

The individual safety concepts of the SINUMERIK control families are described below.

5.1 SINUMERIK 808

For a SINUMERIK 808 with a SINAMICS V70 for the feed drives and, e.g. a SINAMICS G120 for the main spindle, a Safe Torque Off can be implemented for the drives with an appropriate external hardware circuit.

See application example:

STO for SINUMERIK 808 (https://support.industry.siemens.com/cs/ww/en/view/79170136) (Intranet)

Example of implementation of Safe Torque Off (STO) for a SINUMERIK 808:

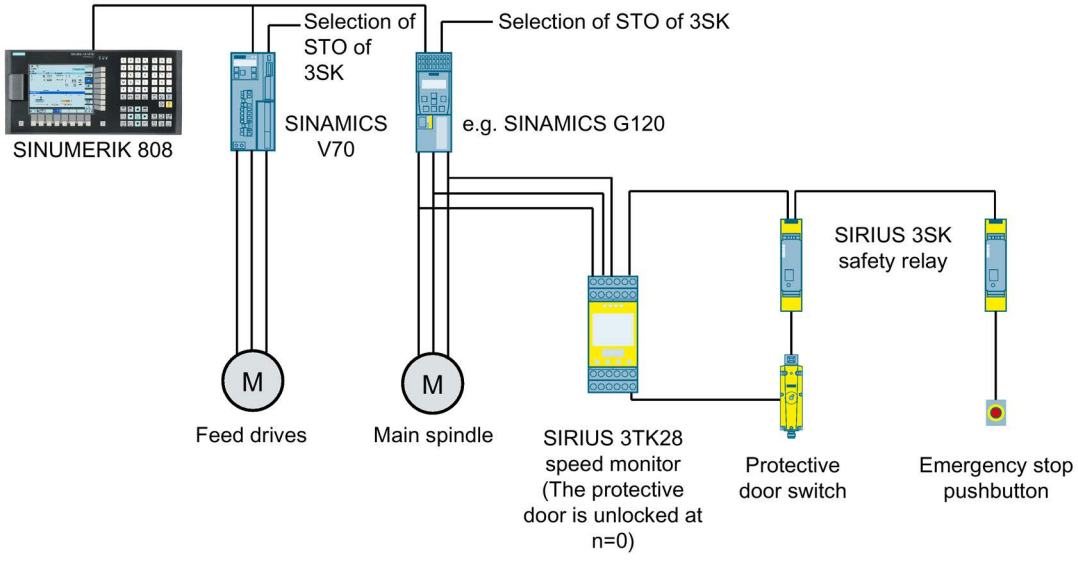


Figure 5-1 Schematic circuit diagram for the implementation of STO

5.1.1 Emergency stop

If the emergency stop pushbutton is actuated, the drives are braked in a single channel in the SINAMICS V70 and SINAMICS G120. After a set time, Safe Torque Off is selected via the two STO terminals of the feed and main spindle drives.

5.1.2 Protective door

In most cases, a protective door is equipped with a locking solenoid. Before the protective door can be opened, the locking solenoid must be unlocked. This is performed, for example, via the Request protective door button on the operator panel.

If the protective door is requested, the drives are braked via a single channel. After a set time, Safe Torque Off is selected via the two STO terminals of the SINAMICS V70 and SINAMICS G120. The protective door is not unlocked until the feed axes signal STO active and the speed monitor signals spindle speed n = 0.

5.2 SINUMERIK 828

With the SINUMERIK 828 / SINAMICS S120, the drive-based safety functions are used in the SINAMICS.

The Safety Integrated basic functions, STO (Safe Torque Off) and SS1 (Safe Stop 1), can be selected via terminals. The Safety Integrated basic functions also contain the SBC (Safe Brake Control). If it has been parameterized, this safety function is activated automatically with an STO.

In addition to the Safety Integrated basic functions, the Safety Integrated extended functions can also be used and are selected using the TM54F Terminal Module.

The following table shows the safety functions that are available:

Safety function	Safety Integrated basic functions	Safety Integrated extended functions
Safe Operating Stop	x	x
Safe Stop 1	x	x
Safe Brake Control	x	x
Safe Stop 2	-	x
Safe Operating Stop	-	x
Safely-Limited Speed	-	x
Safe Speed Monitor	-	x
Safe Acceleration Monitor	-	x
Safely-Limited Position	-	x
Safe Direction	-	x

The TM54F Terminal Module is a terminal expansion module with fail-safe digital inputs and digital outputs via which the safety functions can be selected.

The fail-safe inputs of the TM54F can be controlled either via external safety relays, e.g. SIRIUS 3SK1, or via the SIRIUS 3RK3 modular safety system.

The safety functions are selected via the TM54F fail-safe inputs.

Each Control Unit (PPU, NX) of the SINUMERIK 828 can be assigned exactly one TM54F, which is connected via DRIVE-CLiQ.

Further axes can be connected to the SINUMERIK 828 via PROFINET and, for example, a CU320. The SINAMICS Safety Integrated basic functions can be selected for these axes via terminals.

As of SINUMERIK software version 4.7, the status information is transferred to the control via the Safety Info Channel. The status information displays which safety function has been selected in the SINAMICS.

Signals can be communicated from the control to the drive via the Safety Control Channel, e.g. "Start of the brake test".

5.2.1 Controlling the safety functions via the TM54F and SIRIUS 3SK

When controlling the safety functions via the SIRIUS 3SK safety relay, the hardware linking of the fail-safe sensors and actuators is via the relay. Via K1 and K2 in the following example.

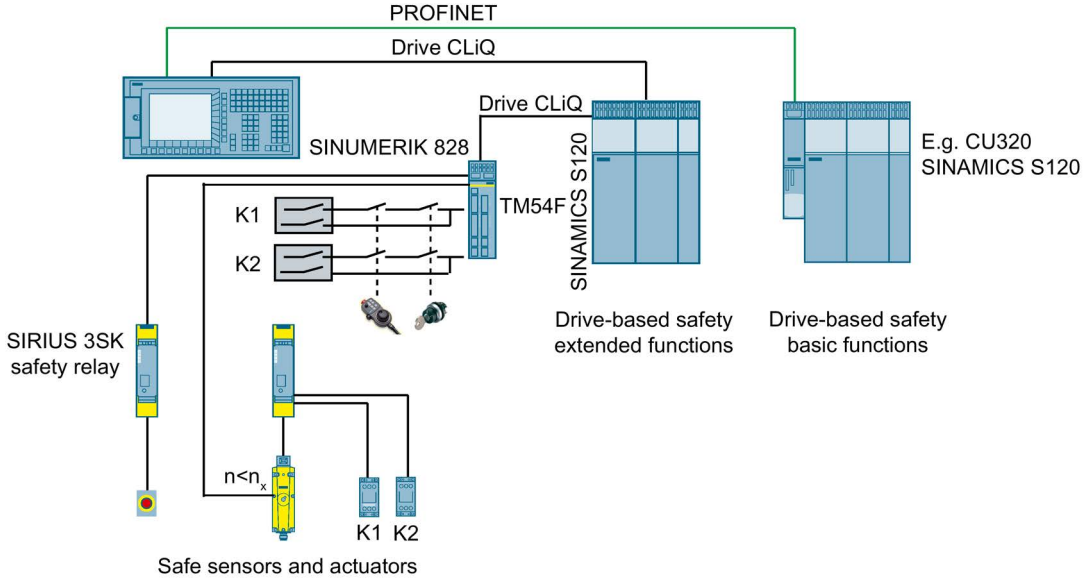


Figure 5-2 Schematic circuit diagram for the implementation of the safety functions with safety relay

5.2.2 Controlling the safety functions via the TM54F and the modular 3RK3 safety system

The 3RK3 Modular Safety System (MSS) is a freely parameterizable modular safety relay. The fail-safe inputs and outputs of the MSS can be parameterized and linked via the associated graphic engineering tool.

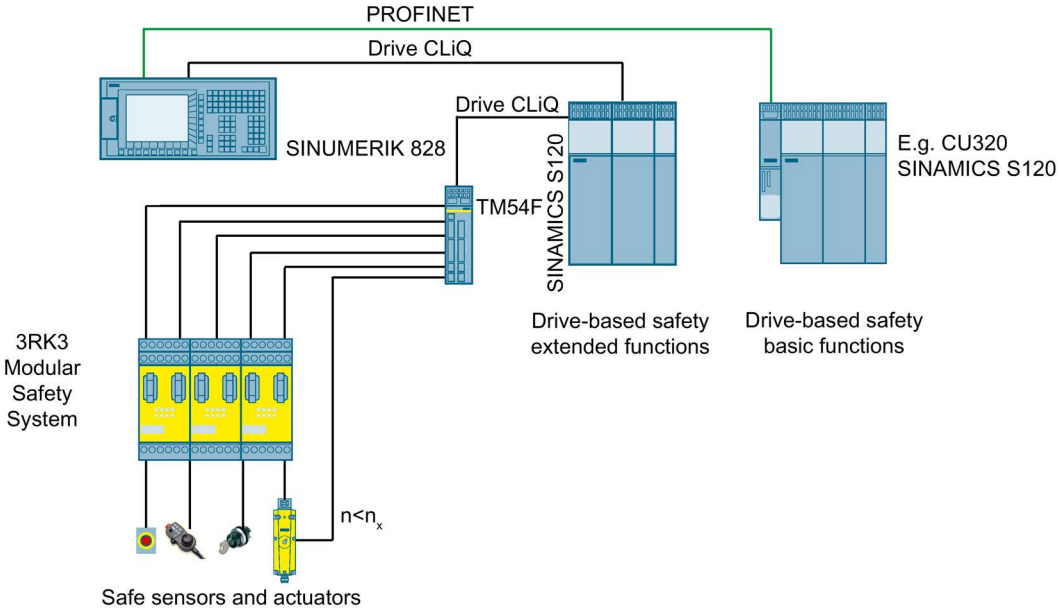


Figure 5-3 Schematic circuit diagram for the implementation of the safety functions with the modular 3RK3 safety system

5.3 SINUMERIK 840D sl

For the SINUMERIK 840D sl in conjunction with SINAMICS S120, the Safety Integrated basic functions of the SINAMICS as well as the safety functions integrated in the system can be used for the axes assigned directly to the SINUMERIK NCU.

The Safety Integrated basic functions of the SINAMICS include the STO (Safe Torque Off) and the SS1 (Safe Stop 1). These safety functions can be controlled via terminals. The Safety Integrated basic functions also contain the SBC (Safe Brake Control). This safety function is activated automatically with an STO.

The safety functions integrated in the system are controlled via the safe programmable logic and are implemented in the SINUMERIK and in the SINAMICS.

The following table shows the safety functions that are available:

Safety function	Safety Integrated basic functions	System-integrated safety functions
Safe Torque Off	x	x
Safe Stop 1	x	x
Safe Brake Control	x	x
Safe Stop 2	-	x
Safe Operating Stop	-	x
Safely-Limited Speed	-	x
Safe Speed Monitor	-	x
Safe Acceleration Monitor	-	x
Safely-Limited Position	-	x
Safe Cam	-	x
Safe Programmable Logic	-	x

The safety functions integrated in the system are controlled via the Safe Programmable Logic (SPL). The Safe Programmable Logic is structured redundantly and comprises a subprogram in the SINUMERIK 840D sl (NCK) and a standard STEP 7 program in the integrated PLC of the SINUMERIK 840D sl. There is a crosswise data and result comparison between these two programs.

The interface to the machine is formed by fail-safe inputs and outputs (F-DI, F-DO). The safety-related sensors and actuators are connected directly to these inputs and outputs without an additional hardware circuit.

The communication between the control and the fail-safe I/O is via PROFIBUS or PROFINET with the aid of the PROFIsafe protocol. The signals of the safety-related sensors are transferred to the NCK SPL and to the PLC SPL. In the reverse direction, the safe actuators are addressed via the NCK SPL and the PLC SPL.

External drives can be connected via PROFIBUS or PROFINET and, for example, with the CU320 Control Unit. The axis can be either an NC or a PLC axis. The drive-based safety functions of the SINAMICS can be used for these external drives. These safety functions are controlled by the SPL with the PROFIsafe protocol.

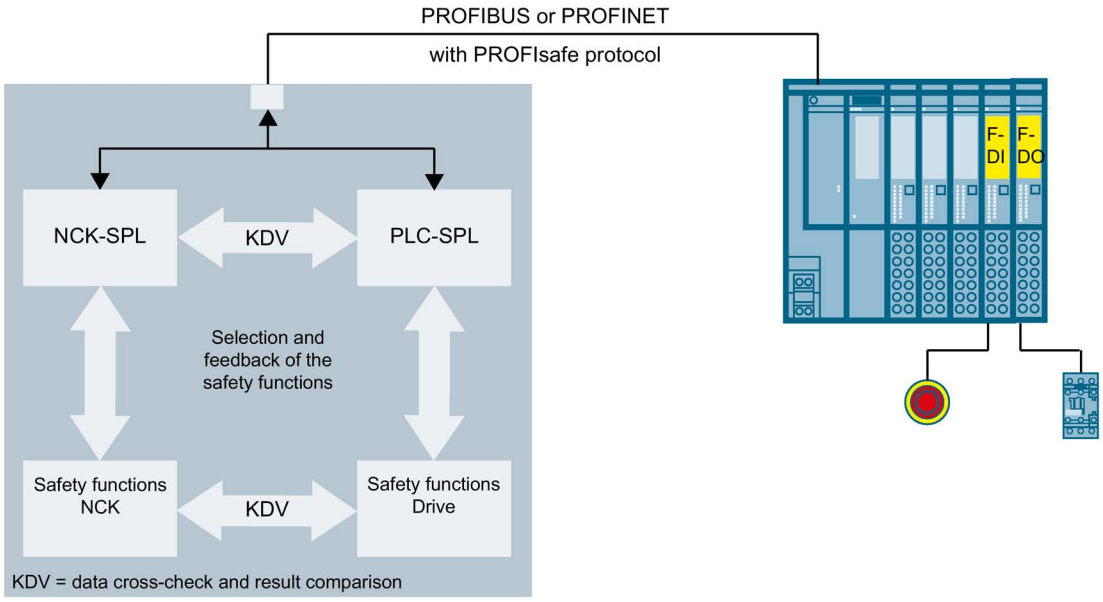


Figure 5-4 Structure of the Safe Programmable Logic

5.3.1 Controlling the safety functions

The following figure shows an example of the control of the safety functions:

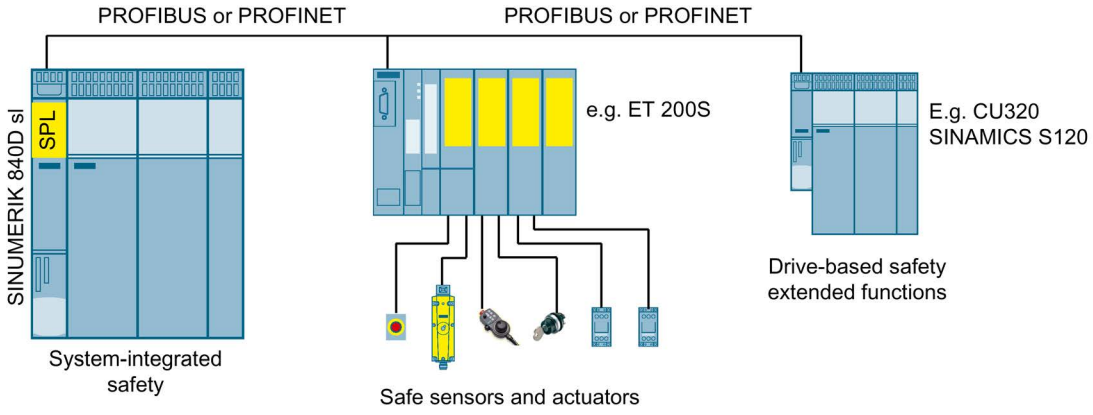


Figure 5-5 Schematic circuit diagram for the implementation of the safety functions

Sensor and actuator integration 6

6.1 SINUMERIK 808

With the SINUMERIK 808, the safety-related sensors and actuators are linked to the control, for example, via a safety relay of the SIRIUS 3SK series.

The signals are linked via the wiring.

6.2 SINUMERIK 828

With the SINUMERIK 828, the safety-related sensors and actuators are linked to the control, for example, via a safety relay of the SIRIUS 3SK series or via the 3RK3 modular safety system (MSS).

When linking the hardware signals with the modular safety system (MSS), the safety-related sensors and actuators are connected directly with additional hardware. The fail-safe signals are linked via a graphic parameter assignment.

6.3 SINUMERIK 840D sl

The safety-related distributed I/O is connected to the control via fail-safe input and output signals and via PROFIBUS or PROFINET with the PROFIsafe protocol. The safety-related sensors and actuators are connected directly to the fail-safe input and output modules without additional hardware.

The fail-safe modules of the ET 200S, ET 200eco, ET 200M and ET 200SP or the DP-/ASi F-Link can be used as I/O modules.

System requirements and software licenses 7

7.1 SINUMERIK 808

The SINUMERIK 808 in conjunction with the SINAMICS V70 provides the Safe Torque Off safety function as standard.

No further requirements are necessary from SINUMERIK or the drive for this safety function.

7.2 SINUMERIK 828

The drive-based safety functions of the SINAMICS S120 can be used for the SINUMERIK 828, in conjunction with the SINAMICS S120.

The Safety Integrated basic functions (STO Safe Torque Off, SS1 Safe Stop 1, SBC Safe Brake Control) are always included as standard.

The following requirements must be satisfied in order to be able to use the Safety Integrated extended functions:

- "Safety Integrated Drive-Based" software license

  6FC5800-0AC50-0YB0 (for each axis)
- TM54F Terminal Module

  6SL3055-0AA00-3BA0 (for each Control Unit)

7.3 SINUMERIK 840D sl

For the SINUMERIK 840D sl in conjunction with SINAMICS S120, the Safety Integrated basic functions of the SINAMICS as well as the safety functions integrated in the system can be used.

The Safety Integrated basic functions of the SINAMICS (STO Safe Torque Off, SS1 Safe Stop 1, SBC Safe Brake Control) are always included as standard and require no further hardware or software license.

The following software licenses are available for the safety functions integrated in the system:

- SINUMERIK SI Basic (4 SPL inputs / 4 SPL outputs, incl. one axis)

  6FC5800-0AM63-0YB0
- SINUMERIK SI Comfort (64 SPL inputs / 64 SPL outputs, incl. one axis)

  6FC5800-0AM64-0YB0
- SINUMERIK SI High-Feature (192 SPL inputs / 192 SPL outputs, incl. one axis)

  6FC5800-0AS68-0YB0

- SINUMERIK SI Axis (additionally for each further axis/spindle)

  6FC5800-0AC70-0YB0
- SINUMERIK SI Axis/Spindle Package (further additional 15 axes/spindles)

  6FC5800-0AC60-0YB0
- SINUMERIK SI Connect (16 safe connections)

  6FC5800-0AS67-0YB0

No special hardware for Safety Integrated is required for the SINUMERIK 840D sl.

External axes can be connected via PROFIBUS or PROFINET, for example, via a CU320.

If the Safety Integrated extended functions of the SINAMICS are to be used for these external axes, the following license is required for each relevant:

- Safety Integrated extended functions

  6SL3074-0AA10-0AA0

Acceptance test

8

The requirements associated with an acceptance test of the safety functions are derived from the EU Machinery Directive. According to the Directive, the machine manufacturer (OEM) has an obligation to carry out acceptance testing for safety-related functions and machine components and to produce an acceptance certificate from which the results of the tests can be derived.

When using the Safety Integrated function, the acceptance test is used to check the correct configuring of the Safety Integrated monitoring functions used in the NCK, PLC and drive.

The test objective is to verify the correct implementation of the defined safety functions, to check the implemented test mechanisms and to examine the response of individual monitoring functions by explicitly violating tolerance limits. This must be performed for all safety functions.

A distinction is made between a complete and a partial acceptance test. For a complete acceptance test, all the intended safety functions have to be checked. During this test, the entire fault response chain from the sensor over the control to the actuator is run through and the correct funtioning of the safety function checked.

For a partial acceptance test, only the safety-relevant parameters that have been changed compared to the complete acceptance test or have been added need to be tested.

8.1 SINUMERIK 808

For the SINUMERIK 808, the correct functioning of the emergency stop function must be tested and documented by the machine manufacturer.

8.2 SINUMERIK 828

For the SINUMERIK 828 with SINAMICS S120, the acceptance test for all the safety-related functions can be performed with the STARTER commissioning tool.

In addition, as of SINUMERIK software version 4.7 SP2, the acceptance test for all safety functions can be performed partly automatically and operator-controlled with SINUMERIK Operate.

8.3 SINUMERIK 840D sl

The SinuComNC tool is available for the acceptance test for a SINUMERIK 840D sl / SINAMICS S120. The acceptance test can be performed partly automatically and operator-controlled with this tool. The trace functions are configured automatically here. The automatically generated acceptance protocol is proof of the tested functional safety of the machine for the machine manufacturer.

Safety functions on machines according to ISO 13849 or IEC 62061

9

Safety Integrated functions play an essential role in achieving functional safety of plants and machines. Functional safety means that all parts of machines function correctly and have sufficient equipment to minimize risks. In addition to functional risks, plants and machines have a whole series of other potential hazards.

Using risk analysis, risk assessment and the appropriate measures to minimize risk, the machine manufacturer can achieve a safe plant or machine.

9.1 Risk analysis

The primary task of a risk analysis is to detect and evaluate hazards as well as to control these hazards by means of protective measures to ensure that they will not cause any damage.

The following iterative process is recommended in EN ISO 12100:

1. Determination of physical and temporal machine limits
2. Identification of hazards, risk estimation and evaluation
3. Estimation of the risk for every identified hazard and hazardous situation
4. Evaluation of the risk and determination of decisions for risk reduction
5. Elimination of hazards or reduction of the risk associated with the hazard

The safety requirements to be satisfied are derived from the determined risks. For every identified hazard, a safety function has to be specified.

The risk analysis must be performed by the machine manufacturer.

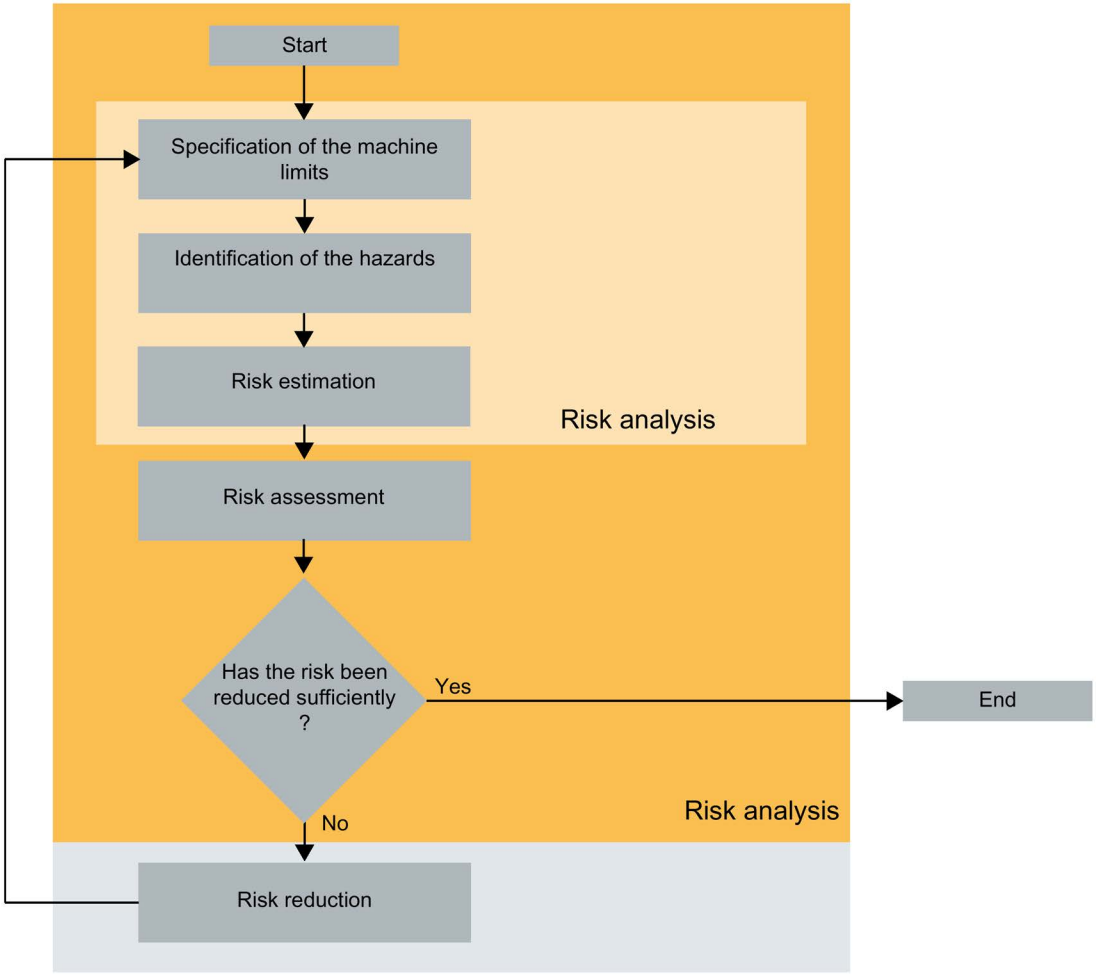


Figure 9-1 Process actions for the risk assessment and risk reduction

9.2 Risk assessment

The objective of the risk assessment is to quantitively determine the risk, i.e. the probability of an injury. This risk assessment must be performed for every identified safety function.

Processes are described in IEC 62061 and in EN ISO 13849 how an assessment of the risk is to be performed for a safety function.

The result of a risk assessment with IEC 62061 is the Safety Integrity Level (SIL), and the result from EN ISO 13849 is described by the Performance Level (PL).

Although the two standards use different assessment methods for a safety function, the results are transferable.

The machine tool industry only uses EN ISO 13849 because this standard also considers pneumatic, hydraulic and mechanical systems in addition to electrical and electronic systems.

The risk assessment must also be performed by the machine manufacturer.

9.2.1 Determination of the Safety Integrity Level (IEC 62061)

A process to estimate the qualitative risk and to determine the required Safety Integrity Level (SIL) is shown in Appendix A of EN 62061. This process must be performed for every identified safety function and is based on the method described in EN ISO 12100.

The following risk parameters must be considered:

- S → Severity of the possible damage or injury
- F → Frequency and duration of the exposure to danger
- W → Probability of the occurrence of a dangerous event
- P → Possibility of avoidance or limitation of the damage

The individual risk parameters must be considered for each safety function and weighted with an appropriate number depending on the characteristic.

The probability class of the damage (K) results from the addition of the risk parameters F, W and P (K = F + W + P).

The parameters S and K are then applied in a matrix to determine the SIL (Safety Integrity Level).

Effects	Degree of damage S	Class K=F+W+P					Frequency F (duration < 10 min)		Probability of occurrence W		Possibility of avoidance P	
		3-4	5-7	8-10	11-13	14-15						
Death, loss of eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 h	5	Frequent	5		
Permanent, loss of fingers	(3)		OM	SIL 1	SIL 2	SIL 3	>= 1 h to <= 1 day	(5)	Probable	4		
Reversible, medical treatment	2			OM	SIL 1	SIL 2	<= 1 day to <= 2 weeks	4	Possible	(3)	Impossible	5
Reversible, first aid	1				OM	SIL 1	>= 2 weeks to <= 1 year	3	Rarely	2	Possible	(3)
							>= 1 year	2	Negligible	1	Probable	1

Serial number	Hazard number	Hazard	S	F	W	P	K	Safety measures	Safe
		Axis movements	3	5	3	3	11	Emergency stop	

Figure 9-2 Determination of the SIL according to IEC 62061

9.2.2 Determination of the Performance Level (EN ISO 13849)

EN ISO 13849 describes how to determine the Performance Level (PL) for safety-relevant parts of control systems based on specific structures (categories) for the intended service life (usually 20 years). When combining several safety-related parts to form a complete system, the standard explains how to determine the resulting PL.

The assessment of the Performance Level of a safety function can be determined using a risk assessment flowchart.

The following risk parameters are considered:

- S → Severity of the injury
  - S1 = slight (usually reversible) injury
  - S2 = serious (usually irreversible) injury, including death
- F → Frequency and/or duration of the exposure to danger
  - F1 = seldom to frequent and/or short exposure to danger
  - F2 = frequent to continuous and/or long exposure to danger
- P → Possibility of avoiding the hazard or limiting the damage
  - P1 = possible under certain conditions
  - P2 = hardly possible

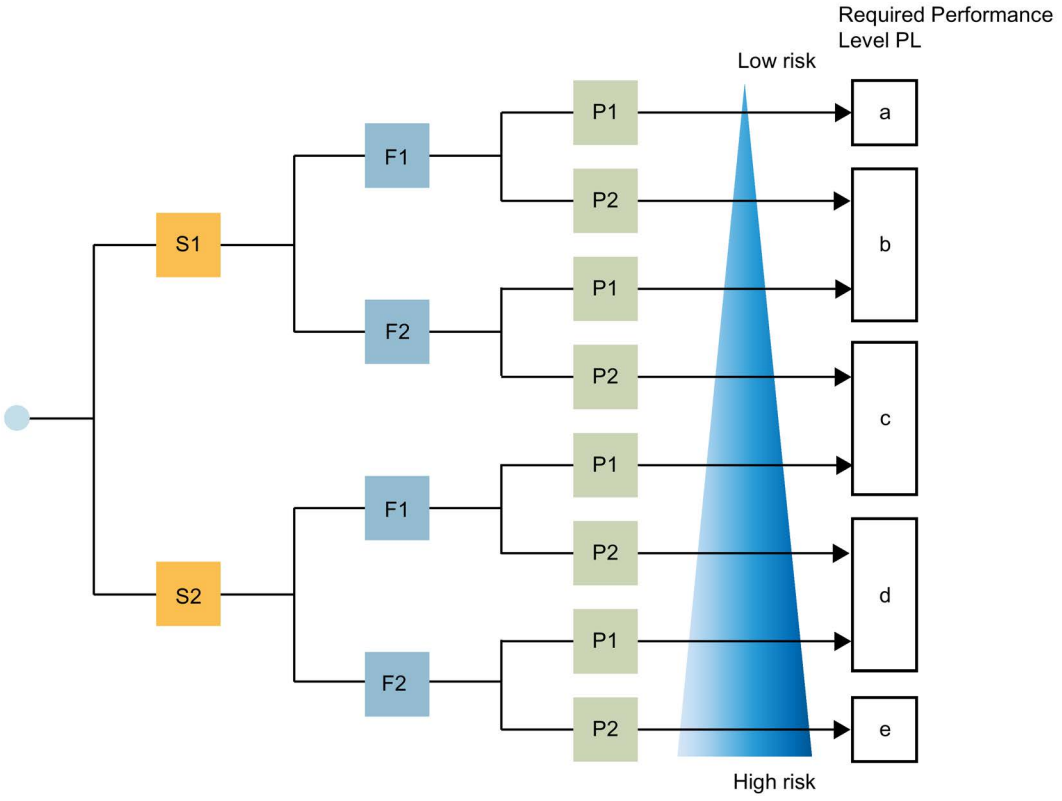


Figure 9-3 Risk assessment flowchart according to EN ISO 13849

9.3 Structure of a safety function

A safety function consists of the three subsystems detecting, evaluating and reacting.

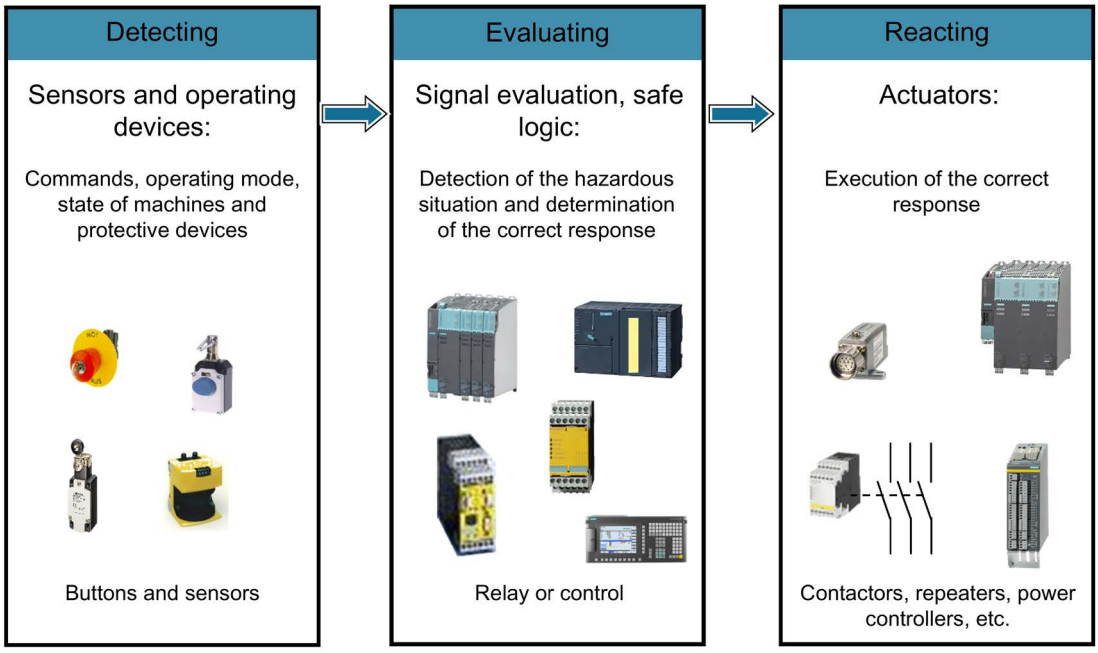


Figure 9-4 Structure of a safety function

The components involved in the safety function must be specified for each of these subsystems and the probability of failure calculated in the form of a PFH value (**P**robability of dangerous **f**ailure per **h**our). The sum of the individual PFH values results in the total PFH value and consequently the Performance Level (PL) or Safety Integrity Level (SIL) for the complete safety function.

SIEMENS provides the Safety Evaluation Tool (SET) for the calculation of the safety functions.

Some machine manufacturer use the SISTEMA tool from the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA).

9.4 Safety Evaluation Tool

The TÜV-tested free-of-charge online tool - Safety Evaluation Tool (SET) from Siemens - for the IEC 62061 and ISO 13849-1 standards, guides the user step-by-step from defining the structure of the safety system, through the selection of components, to the calculation of the achieved safety integrity (SIL/PL). The result is a report in conformance with the standards that you can integrate as proof of safety into the documentation.

Figure 9-5 Safety Evaluation Tool

See also

Safety Evaluation Tool (http://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/safety-evaluation-tool/Pages/default.aspx)

9.5 SISTEMA

The SISTEMA software wizard (safety of controls on machines) of the IFA (Institute for Occupational Safety and Health of the German Social Accident Insurance) provides support for the assessment of the safety of controls within the framework of the DIN EN ISO 13849-1. The free-of-charge Windows tool simulates the structure of the safety-related control components (SRP/CS, Safety-Related Parts of a Control System) based on the so-called intended architectures and calculates reliability values on various detail levels including the achieved Performance Level (PL).

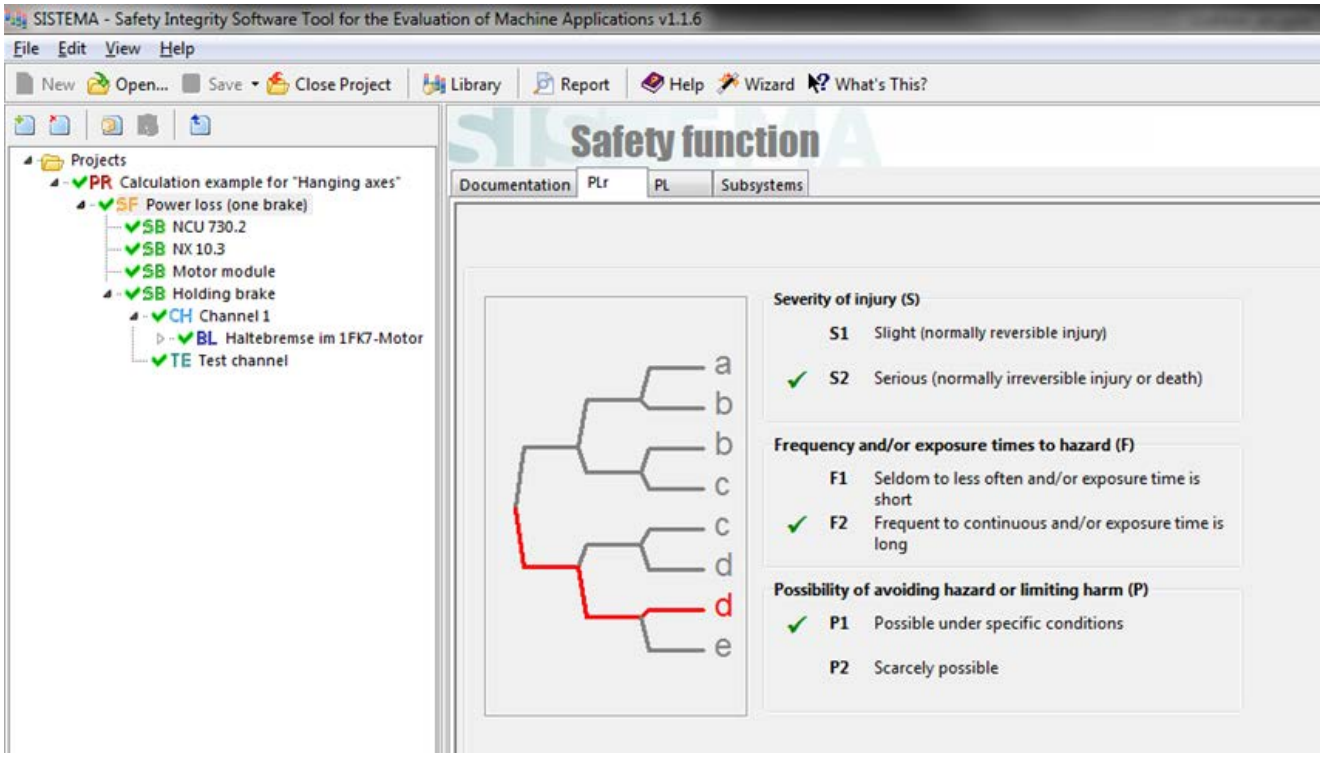


Figure 9-6 SISTEMA

See also

SISTEMA software wizard (http://www.dguv.de/ifa/Praxishilfen/Software/SISTEMA/index-2.jsp)

9.6 Calculation of safety functions

The PFH value of a safety function is calculated from the sum of the individual PFH values of the components used in the safety function.

9.6.1 Example of calculating the emergency stop safety function

The emergency stop safety function is calculated using a turning machine with one spindle and two axes (X axis, Z axis) as an example.

Task

After pressing the emergency stop button, the spindle and both axes are to be braked as quickly as possible (Stop C) and brought to a safe standstill after the braking operation.

The following components are involved in the safety function and must be considered:

- Detecting
  - Emergency stop button
- Evaluating
  - ET 200S safe input module
  - NCU 730.3 PN of the SINUMERIK 840D sl
- Reacting
  - Spindle Motor Module
  - X axis Motor Module
  - Z axis Motor Module
  - Spindle encoder interface
  - X axis encoder interface
  - Z axis encoder interface

A Single Motor Module is used for each spindle and axis. The axes and the spindle are equipped with a DRIVE-CLiQ encoder.

Block diagram

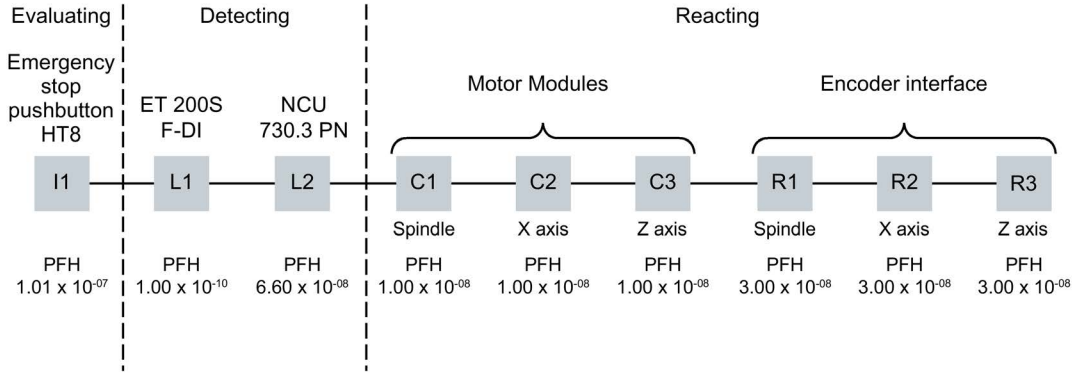


Figure 9-7 Components in the block diagram

The PFH values are available in the Safety Evaluation Tool (SET) in the form of a SISTEMA library and on the Internet.

The following table shows the PFH values of the deployed components:

Designation	Component	PFH value
I1	HT8 emergency stop button	1.01×10^{-07}
L1	ET 200S (F-DI)	1.00×10^{-10}
L2	NCU 730.3 PN	6.60×10^{-08}
C1	Spindle Motor Module	1.00×10^{-08}
C2	X axis Motor Module	1.00×10^{-08}
C3	Z axis Motor Module	1.00×10^{-08}
R1	1-encoder safety spindle	3.00×10^{-08}
R2	1-encoder safety X axis	3.00×10^{-08}
R3	1-encoder safety Z axis	3.00×10^{-08}
	Total	**2.871×10^{-07}**

Calculation

The addition of the PFH values results in a total PFH value of 2.871×10^{-07}.

This safety function therefore satisfies the requirements of PL d and SIL 2.

9.6.2 Application examples for the calculation of safety functions for SINUMERIK

Further examples for the calculation of safety functions with a SINUMERIK can be found via the following links.

SINUMERIK 828

Example of the calculation of safety functions on a machine with six axes and two spindles:

Calculation of safety functions for the SINUMERIK 828
(https://support.industry.siemens.com/cs/ww/en/view/62985658) (Intranet)

SINUMERIK 840D sl

Calculation of safety functions for a horizontal axis
(https://support.industry.siemens.com/cs/ww/en/view/81304594)

Calculation of safety functions for a vertical axis
(https://support.industry.siemens.com/cs/ww/en/view/69870640)

Mode selection via standard components
(https://support.industry.siemens.com/cs/ww/en/view/108866318)

PFH values

10

10.1 Determination of the current PFH values

The current PFH values can be found in our Safety Evaluation Tool.

An additional PFH value document is also available for SINUMERIK and SINAMICS products and can be found via the following link:

PFH value document (https://support.industry.siemens.com/cs/ww/en/view/76254308)

Appendix A

A.1 Application examples for the SINUMERIK 840D sl

Examples of the acceptance test, the configuration and the secure communication can be found via the following links.

Acceptance test

Instructions for the acceptance test
(https://support.industry.siemens.com/cs/ww/en/view/63012568)

Example of the acceptance test
(https://support.industry.siemens.com/cs/ww/en/view/62985807)

Configuration example

Configuration example (https://support.industry.siemens.com/cs/ww/en/view/63012172)

Secure communication

Safe coupling between two SINUMERIK 840D sl
(https://support.industry.siemens.com/cs/ww/en/view/83145979)

Safe I-Device coupling between a SINUMERIK 840D sl and a SIMATIC IM 151-8 F CPU
(https://support.industry.siemens.com/cs/ww/en/view/83146707)

Safe coupling between a SINUMERIK 840D sl and a SIMATIC IM 151-7 F CPU
(https://support.industry.siemens.com/cs/ww/en/view/83145990)

A.2 Certifications

The safety functions of the SINUMERIK and the SINAMICS comply with the requirements of Category 3 as well as Performance Level PL d according to EN ISO 13849 and Safety Integrity Level SIL 2 according to EN 61508-5-2.

A.2.1 SINUMERIK 828

A Manufacturer's declaration (https://support.industry.siemens.com/cs/document/69037484) is available for the SINUMERIK 828.

A.2.2 SINUMERIK 840D sl

Links to the current certificates and the Manufacturer's declaration:

Manufacturer's declaration (https://support.industry.siemens.com/cs/document/51770733)

IFA (Institute for Occupational Safety and Health of the German Social Accident Insurance) (https://support.industry.siemens.com/cs/document/29754745)

German Technical Inspectorate Rheinland of North America (https://support.industry.siemens.com/cs/document/36172737)

German Technical Inspectorate Rheinland (https://support.industry.siemens.com/cs/document/31929148)

A.3 Safety Integrated Function Descriptions

A.3.1 SINUMERIK 828

Link to the current documentation for the SINUMERIK 828:

SINUMERIK 828 (https://support.industry.siemens.com/cs/ww/en/ps/14590/man)

The current Function Description for Safety Integrated can be found by entering the search term "Safety Integrated".

A.3.2 SINUMERIK 840D sl

Link to the current documentation for the SINUMERIK 840D sl:

SINUMERIK 840D sl (https://support.industry.siemens.com/cs/ww/en/ps/14599/man)

The current Function Description for Safety Integrated can be found by entering the search term "Safety Integrated".

A.3.3 SINAMICS

Link to the current documentation for the drive technology:

Drive technology (https://support.industry.siemens.com/cs/ww/en/ps/13204/man)

The current Function Description for Safety Integrated can be found by entering the search term "Safety Integrated".

A.4 Internet presence

A.4.1 Internet presence

Link to general information on the topic of Safety Integrated at Siemens:

Functional safety (http://www.industry.siemens.com/topics/global/en/safety-integrated/Pages/functional-safety.aspx)

A.4.2 SINUMERIK Safety Integrated

You can find further information on the topic of SINUMERIK Safety Integrated on the Internet at the following links:

SINUMERIK 828D Safety Integrated (http://w3.siemens.com/mcms/mc-systems/en/automation-systems/cnc-sinumerik/sinumerik-controls/sinumerik-828/sinumerik-828d/Pages/sinumerik-828d-safety-integrated.aspx)

SINUMERIK 840D sl Safety Integrated (http://w3.siemens.com/mcms/mc-systems/en/automation-systems/cnc-sinumerik/sinumerik-controls/sinumerik-840/sinumerik-840d-sl/Pages/sinumerik-840d-sl-safety-integrated.aspx)

A.5 Further documentation and information

General information on our products can be found in our Industry Online Support (https://support.industry.siemens.com/cs/ww/en).

Note

All the links contained in this document can also be found as Link collection (https://support.industry.siemens.com/cs/ww/en/view/109475885) in our Industry Online Support.

List of abbreviations

B

B.1 Abbreviations

CCF	Common Cause Failure
CU	Control Unit
DC	Diagnostic Coverage
DIN	German Institute for Standardization
EG	European Community
EN	European Standard
EEA	European Economic Area
IEC	International Electrotechnical Commission
IFA	Institute for Occupational Safety and Health
ISO	International Standards Organization
MSS	Modulare Safety System
MTTFd	Mean Time To Failure dangerous
NCK	Numerical Control Kernel
PDS (SR)	Adjustable speed electrical Power Drive System suitable for use in Safety-Related applications
PFH	Probability of Failure per Hour
PL	Performance Level
PLC	Programmable Logic Control
PN	PROFINET
SAM	Safe Acceleration Monitor
SBC	Safe Brake Control
SCA	Safe Cam
SDI	Safe Direction
SG	Safely-limited speed
SI	Safety Integrated
SIL	Safety Integrity Level
SLP	Safely-Limited Position
SLS	Safely-Limited Speed
SOS	Safe Operating Stop
SPL	Safe Programmable Logic
SS1	Safe Stop 1
SS2	Safe Stop 2
SSM	Safe Speed Monitor
STO	Safe Torque Off
TÜV	Technischer Überwachungs-Verein (German Technical Inspectorate)

Siemens AG
Digital Factory
Motion Control
Postfach 3180
91050 ERLANGEN
GERMANY

www.siemens.com/motioncontrol