5.6 Safety engineering for machines with power drives

In the following we provide an overview of the EN norms covering safety engineering for machines. Then we deal in detail with the subject of safety engineering for machines with power drives. We refer specifically to IEC 61800 part 5-2 (draft), EN 954-1 and EN 60204-1. Furthermore, in section 5.6.5 we provide an overview of the future standards EN ISO 13849 and EN ISO 62061. The standards referred to are not reprinted in full. We merely quote from their content, or indicate areas of application.

EN 954-1/ISO 13849: The EN 954-1 norm, in future EN ISO 134849 or EN ISO 62061, lays down safety standards under the terms of the Geman Equipment Safety Act. It covers all the components of a machine control deployed in safety tasks. The said components may be hardware (contactors, limit switches, programmable logic controls, servocontrollers, drive controllers and the like) and/or software (user programs, firmware and the like). The future norms (see section 5.6.5) apply with regard to their implementation in programmable systems.

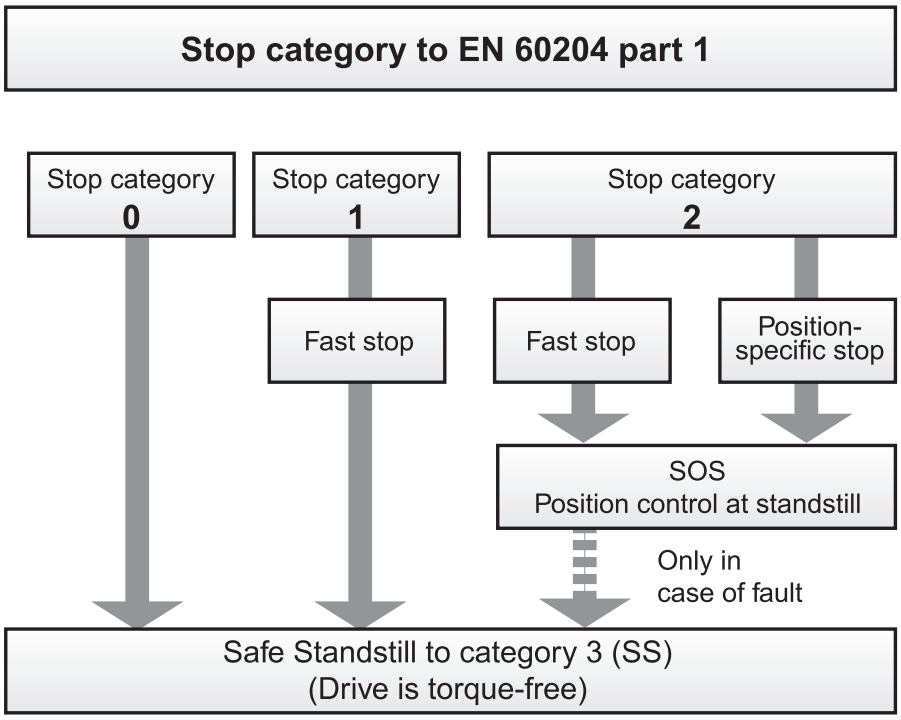
Application of one of the two norms, EN ISO 13849 or EN ISO 62061, is adequate to conform to the protective goals set out in the EU Machinery Directive.

IEC 61800 part 5-2 (draft): The product norm IEC 61800 part 5-2 lays down requirements and provides recommendations for the development of variable-speed power drives suitable for use in safety applications.
The norm is only applicable where the power drive is to be equipped with integrated safety systems.

The product norm IEC 61800-5-2 incorporates requirements from the EN 292, EN 1050, EN 9541 and IEC/EN 61508 norms and from the position paper DKE-AK 226.03.

EN 60204-1/IEC 60204-1 (rev. in preparation): The norm EN 60204 part 1 details various stop categories for differentiated shutdown of drives. Shutdown is not a stand-alone function, but describes the process which can be realized with the aid of a safety control. The future norms (see section 5.6.5) apply with regard to their implementation in programmable systems.

In practice, the functions are mostly realized with simple electromechanical components. You may, however, also be realized with programmable electronic variable-speed drives. Realization of the complex function with power drives is set out in Draft IEC 61800-5-2.



Stop category	System response/ Requirement	Example
0	**Uncontrolled shutdown:** By immediate cutting of the power to the machine drive elements.	The drive torque is cut by the "Safe Standstill (SS)" function. Any drive still in motion runs down to a stop.
1	**Controlled shutdown:** Power to the machine drive elements is maintained to bring about shutdown. The power is only cut when standstill is reached.	The drive is braked under speed control at the current limit and then switched to "Safe Standstill (SS)" mode.
2	**Controlled shutdown:** In which the power to the machine drive elements is also maintained at standstill.	The drive is braked under speed control and then switched to "Safe Operation" mode (position control at standstill).

Table 5.10 Stop category

Position paper DKE-AK 226.03

The position paper details the functions of power drive systems relating to the safety of personnel and lays down relevant requirements. Only power drive systems deployed primarily in machines and of which the electrical control components perform safety functions are considered.

The requirements set out in the position paper relate to the functional response of a drive system. The paper is an enhancement of EN 60204-1 referred to power drive systems, and serves, among other roles, as a discussion paper for drafting of the new norm EN 61800 part 5-2.

5.6.1 Guidelines and EN norm group

With effect from the beginning of 1995 the EU Machinery Directive has stipulated mandatory CE marking. It defines basic requirements for the safety of machines and thus for the protection of operators. The safety requirements are set out in the EN "Safety of machines" norms. The EN norms are divided into the principal groups A, B and C.

"A" norm
"A" norms set out basic terms, design principles and principles of risk assessment covering all machinery.

"B" norm
"B" norms comprise all norms containing safety standards which may relate to more than one kind of machine. "B" norms are important to all manufacturers of machinery to which no "C" norm applies.

"C" norm
"C" norms are norms covering specific machine types, such as machine tools, printing machines, lifts and so on. The "C" norms have priority over "A" and "B" norms.
The machine manufacturers can thus assume that they are conforming to the basic requirement of the Machinery Directive (automatic assumption of conformity).

A new EU Machinery Directive is planned for mid 2007. There will be an 18-month transition period.
Changes are expected with regard to:

- Incomplete machines (partial machines)
- MD Annex 1
- Market supervision
- Assessment of conformity
- Safety modules

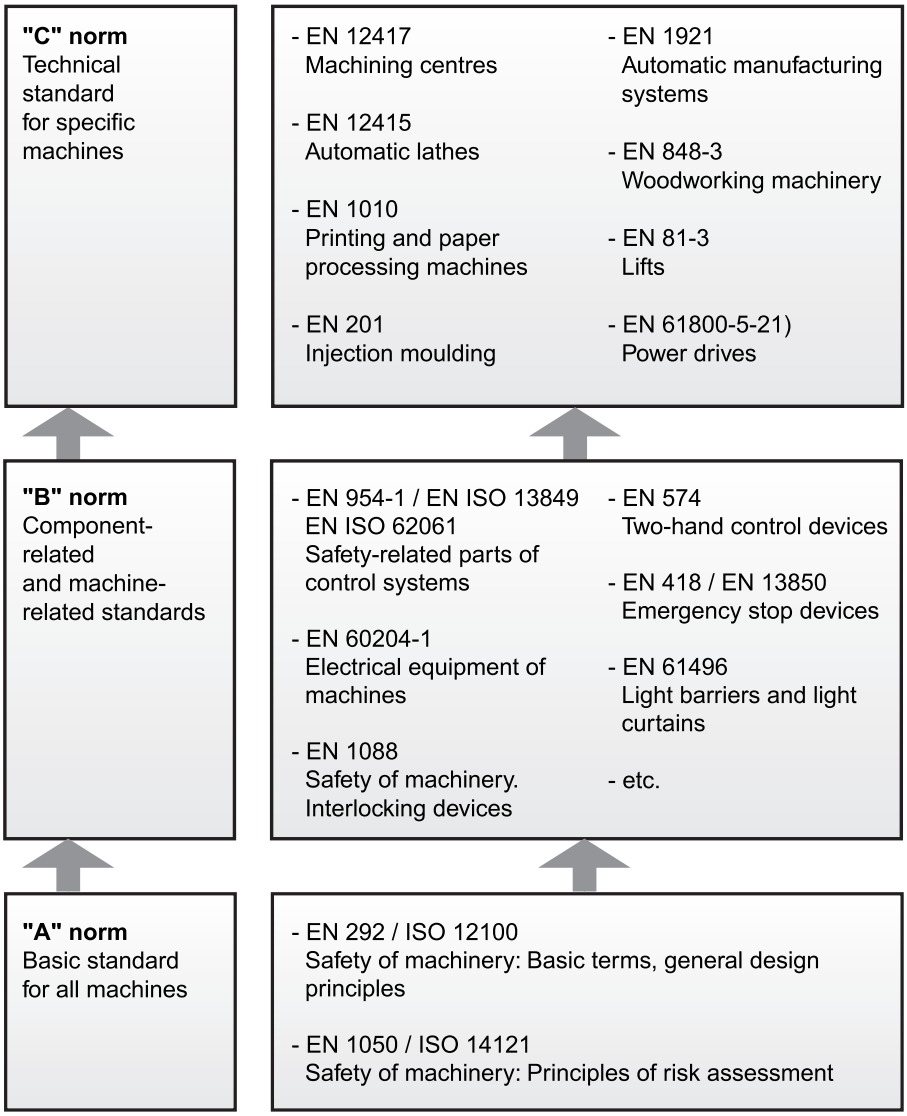


Figure 5.21 Overview of key "A", "B" and "C" norms

You can find a complete listing of all standards cited and the mandated standardization projects on the Internet at:
http//www.newapproach.org

5.6.2 Risk assessment and reduction

Before a machine can be brought into circulation on the market, the machine's manufacturer must carry out a risk assessment in accordance with the EU Machinery Directive 98/37/EEC. The risk assessment determines all the potential hazards associated with use of the machine. The procedure is detailed in EN 1050 ("A" norm): "Principles for risk assessment". It represents an interactive process aimed at attaining safety.

Safety is a relative term in the technical environment. One hundred percent safety is sadly not feasible. The residual risk is defined as: "The risk remaining after implementation of the protective measures". The protective measures cited are the measures taken to reduce risk.

The risk assessment and the risk reduction measures establish the preconditions for specifying the category of safety-related parts of control systems to EN 954-1. The categories are graduated according to the level of risk, see Table 5.11. For more details on risk assessment and reduction and on determining the necessary control requirements refer to the applicable standards and legislation, as space does not allow us to detail them in this brief overview.

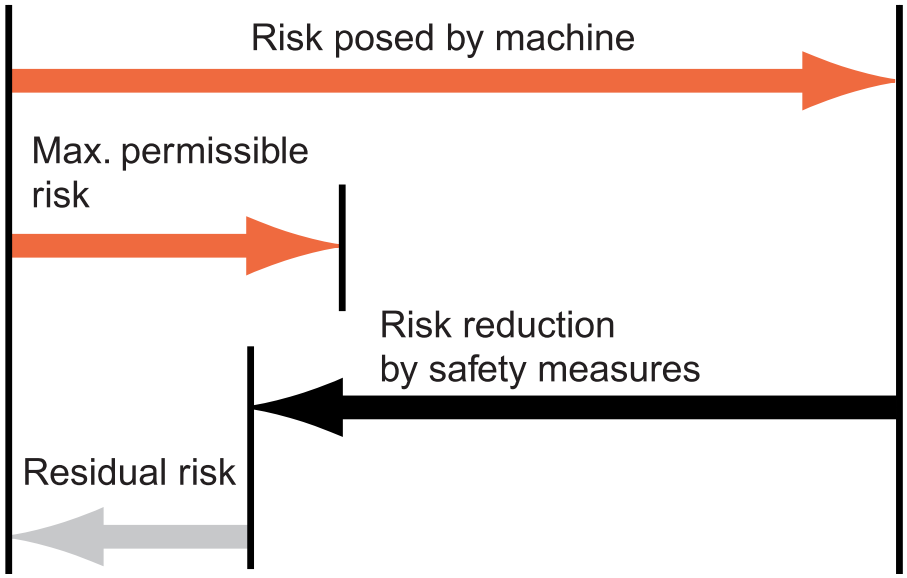


Figure 5.22 Risk assessment system

Safety category[1)]	Summary requirements	System response[2)]	Principles for attaining safety
B	The safety-related parts of control systems and/or their protective devices and their components must be designed, built, selected, assembled and combined in conformance to the applicable standards such that they are able to withstand the expected influences.	The occurrence of a fault may lead to loss of the safety function.	Primarily characterized by selection of components
1	The requirements of B must be met. Tried and proven components and safety principles must be applied.	The occurrence of a fault may lead to loss of the safety function, but the likelihood of occurrence is less than in category B.	
2	The requirements of B must be met and tried and proven safety principles must be applied. The safety function must be tested at appropriate intervals by the machine control system.	• The occurrence of a fault may lead to loss of the safety function between the testing points. • Loss of the safety function is detected by the test.	Primarily characterized by the structure
3	The requirements of B must be met and tried and proven safety principles must be applied. Safety-related parts must be designed such that: • a single fault in any of the said parts does not result in loss of the safety function and • whenever feasible in an appropriate manner, the single fault is detected.	• If the single fault occurs, the safety function is always maintained. • Some - but not all - faults are detected. • A series of undetected faults may lead to loss of the safety function.	
4	The requirements of B must be met and tried and proven safety principles must be applied. Safety-related parts must be designed such that: • a single fault in any of the said parts does not result in loss of the safety function and • the single fault is detected on or before the next request to the safety function or, if this is not possible, a series of faults does not then lead to loss of the safety function.	• If faults occur, the safety function is always maintained. • The faults are detected in time to prevent loss of the safety function.	

1) The categories are not intended to be applied in any given sequence or hierarchical order with regard to the safety requirements.
2) The risk assessment will determine whether the complete or partial loss of the safety function(s) resulting from faults is acceptable.

Table 5.11 Description of the requirements for determining safety categories to EN 954-1

5.6.3 "Safe Standstill" to EN 954-1 category 3

"Safe Standstill" to EN 954-1 designates a protective measure as an interlocking or control function. Category 3 signifies that when a single fault occurs the safety function is maintained. The safety-related parts must be designed such that:

- a single fault in any of the said parts does not result in loss of the safety function and
- whenever feasible in an appropriate manner, the single fault is detected.

For the "Safe Standstill" function to EN 954-1 category 3 the drive controllers are equipped with an integrated circuit with checkback contact. The logic cuts the power supply to the pulse amplifiers to activate the power stage. Combined with the "ENPO" controller enable, a two-channel block is placed on the occurrence in the power circuit of a pulse pattern suitable to generate a rotating field in the motor.

Important notes for implementation

Safety category: Responsibility for determining the safety category required for an application (risk reduction) lies with the machine builder.
Electrical isolation: The "Safe Standstill" function of the drive controller provides no electrical isolation. There is thus no protective function against electric shock hazard.
Action of external forces: If a drive system with the "Safe Standstill" function is expected to be subject to the action of external forces (e.g. dropping of suspended loads), additional measures must be taken to safety prevent movement (a mechanical brake).

Function testing:

You must always check the correct functioning of the "Safe Standstill, protection against unexpected start-up" function:

- on first commissioning,
- after any modification of the system wiring,
- after any replacement of one or more items of system equipment.

Short-circuit in the drive controller power pack:

Shorts in two remote branches of the power pack may activate a short-time axis movement dependent on the number of poles of the motor.

Example - synchronous motor: With a 6-pole synchronous motor the movement may be a maximum of 30 degrees. For a directly driven ball screw, e.g. 20 mm per revolution, this corresponds to a one-time maximum linear movement of 1.67 mm.

When using an asynchronous motor, the shorts in two remote branches of the power pack have virtually no effect, as the exciter field collapses when the inverter is disabled and has fully decayed after about 1 second.

Emergency off system:

Views expressed on this subject have become somewhat ambiguous, so in the following our comments are broken down into those relating to practice and those relating to the standard.

Practice: With the "Safe Standstill" function no emergency off is possible without additional measures. There is no electrical isolation between the motor and the drive controller.

Action in case of emergency to EN13850: EN 13850 (2004), relating to the safety of the machine's emergency stop, replaces EN 418 (Protection of machine emergency-off device).

New definition of terms:

EMERGENCY STOP for shutdown in emergency
Emergency stop is an action in case of emergency designed to stop a hazardous process or movement (EN 60204-1).

EMERGENCY OFF for switch-off in emergency
Emergency off is an emergency action designed to shut off the power supply source if there is a risk of electric shock or other electrical risk (EN 60204-1).

Safe Standstill (emergency stop) with CDE3000

1) This solution provides an "emergency stop (SC3)" as per EN 13850 if the "short via emergency off 11/ 12" fault exclusion can be justified and documented, e.g. by appropriate cable layout or protective devices.

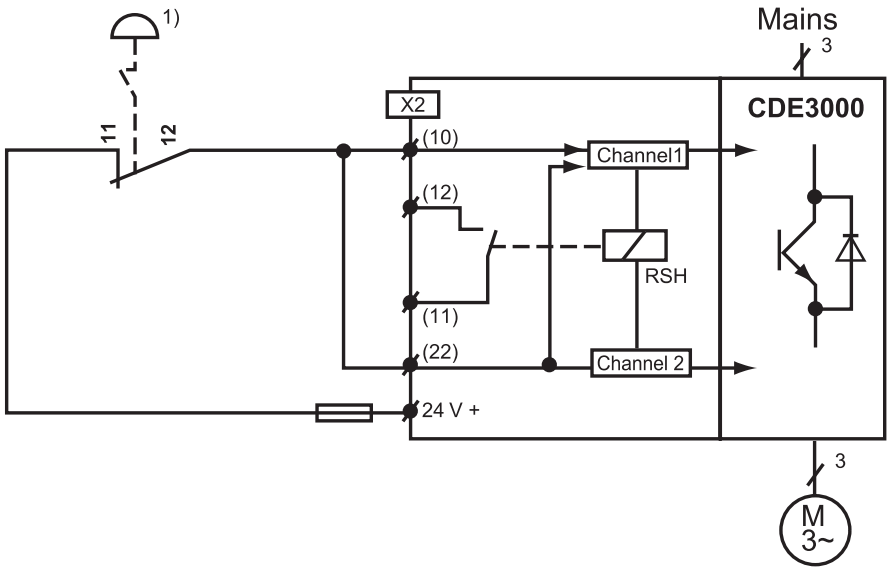


Figure 5.23 Request Safe Standstill for shutdown in emergency (emergency off shutdown)

ENPO	ISD00 (CDB) ISDSH (CDE)	Safe Standstill	Controller state	Relay 1) OSD02 / (CDB)4) RSH (CDE)
L	L	ON3)	Power stage disabled over two channels. Hardware restart lockout active.	
L	(L) ➜ H	ON	Power stage disabled over two channels. Hardware restart lockout active.	
(H) ➜ L	H	OFF	Power stage disabled over one channel.	
H	L	ON	Power stage disabled over two channels. Hardware restart lockout active.	
H	(L) ➜ H	ON	Power stage disabled over two channels. Hardware restart lockout active.	
(L) ➜ H2)	H2)	OFF3)	Power stage ready.	

( ) Preceding state
1) 3 x 10^6 switching cycles at 200 mA (rest: NO contact)
2) To deactivate the restart lockout, the control signals must be set simultaneously (max. error 5 ms) to High (H) or ISD00 (ISDSH) must be set safely before ENPO to High (H)
3) Switching combination for Safe Standstill, category 3
4) CDB3000 is only available in special design with "Safe Standstill".

Circuitry examples with CDE3000 and safety relay module

The following circuitry examples were devised jointly with ELAN Schaltelemente GmbH & Co. KG. The suggested circuit designs are intended to provide an overview of the possible solutions. Please always check the suggested solutions are suitable to your specific application and draw up a validation plan.

Elan Schaltelemente GmbH & Co. KG
Im Ostpark 2
D-35435 Wettenberg
www.elan.de

Lust Antriebstechnik GmbH and ELAN Schaltelemente GmbH & Co KG can consequently accept no responsibility or liability for any loss resulting from use of the suggested circuit designs.

Validation: Does the solution meet the safety requirements?

Always draw up a validation plan. The plan details the tests and analyses you employed to establish the compliance of the solution (e.g. the proposed circuit diagram) with the requirements arising from your particular application case. Always check that

- all safety-related output signals are generated correctly and logically from the input signals.
- the response in case of a fault conforms to the specified circuit categories.
- the control system and the equipment are adequately dimensioned for all operation modes and ambient conditions.

On completing the analyses and tests draw up a validation report.

It should include as a minimum:

- all items to be tested
- the personnel responsible for testing
- test equipment (including details of calibration) and simulation instrumentation
- the tests performed
- the problems found and their remedies
- the results.

Retain the documented results in traceable form.

Advise the user of the correct usage, performance capability and performance limits of the safety-related parts.

Instruct the user how to maintain the performance capability of the safety-related parts, in particular when fault exclusions carried out by you necessitate special maintenance work.

In specifying safety categories (SCs) for the circuitry examples we carried out the following fault exclusion.

Fault exclusion:

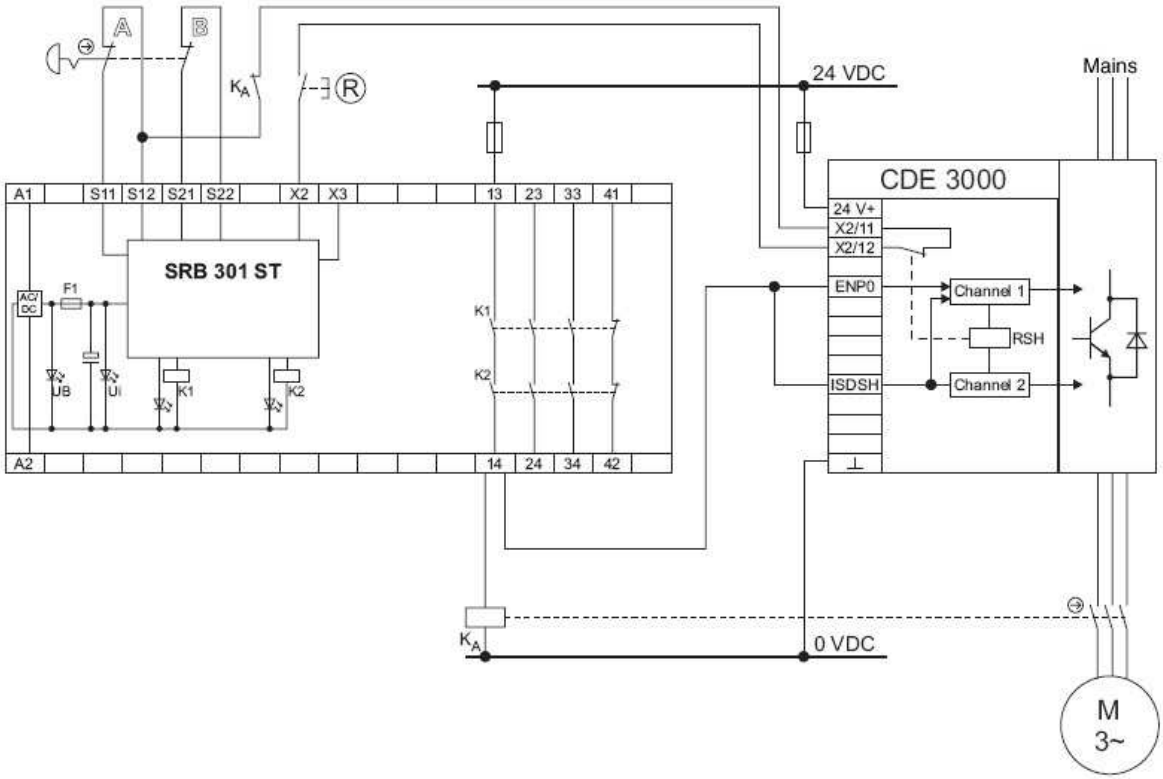
- Bridging within the wiring in the cabinet

Reason:

- Protected installation in cabinet; tried and proven technology

Two-channel emergency off/emergency stop circuit EN 418/ EN 60947-5-5 with cross-circuit detection

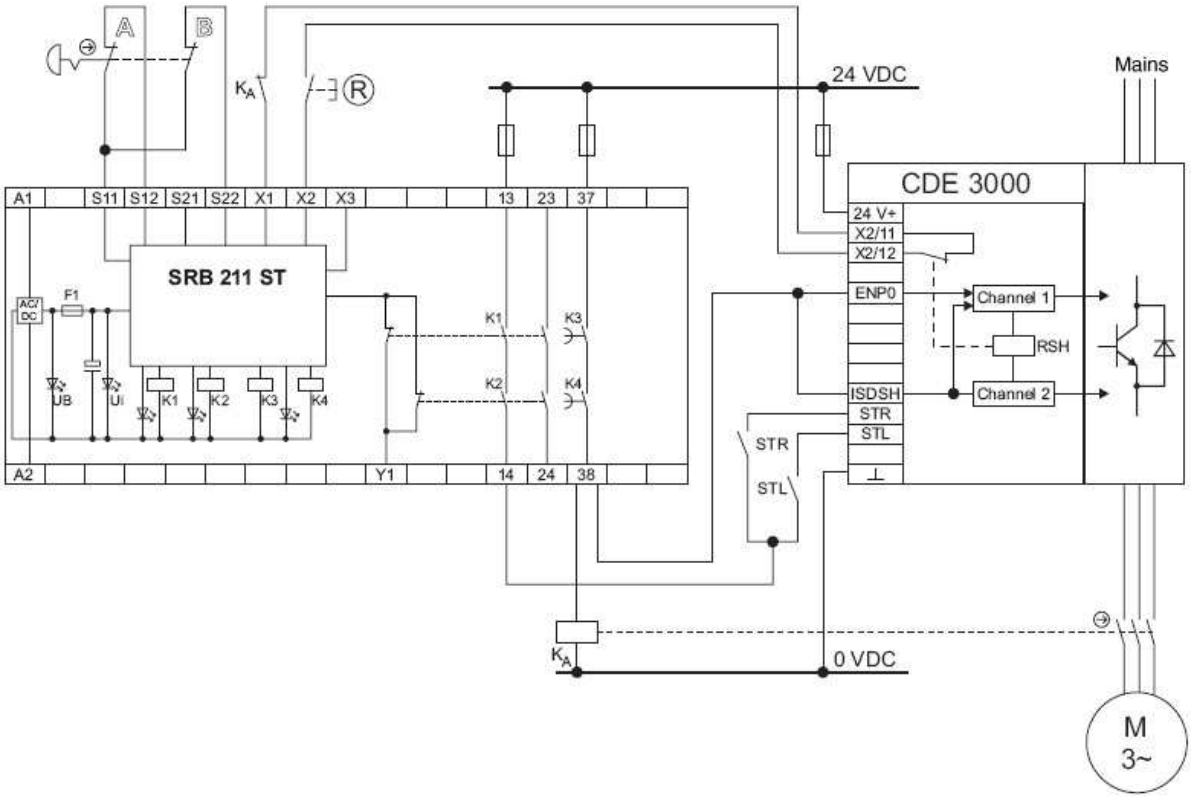
Configuration	Safety category (SC) EN 954-1	Stop category EN 60204-1
Sensor	SC4 with cross-circuit detection	-
CDE3000 with power contactor K_A	SC4 based on in-series configuration of power contactor K_A with positioning drive CDE3000 in SC3 design	Stop category 0 (uncontrolled shutdown)
CDE3000 without power contactor K_A	Emergency stop to EN 13850 with SC3 based on positioning drive CDE3000 in SC3 design	Stop category 0 (uncontrolled shutdown)



Where the drive controller and safety relay are installed in separate locations, preference should be given to the solution with power contactor K_A. It should be ensured that the wiring to K_A and CDE3000 is kept separate, or an appropriate fault exclusion (e.g. protective tubing) is executed.

Two-channel emergency off/emergency stop circuit EN 418/ EN 60947-5-5 with stop category 1 to EN 60204-1

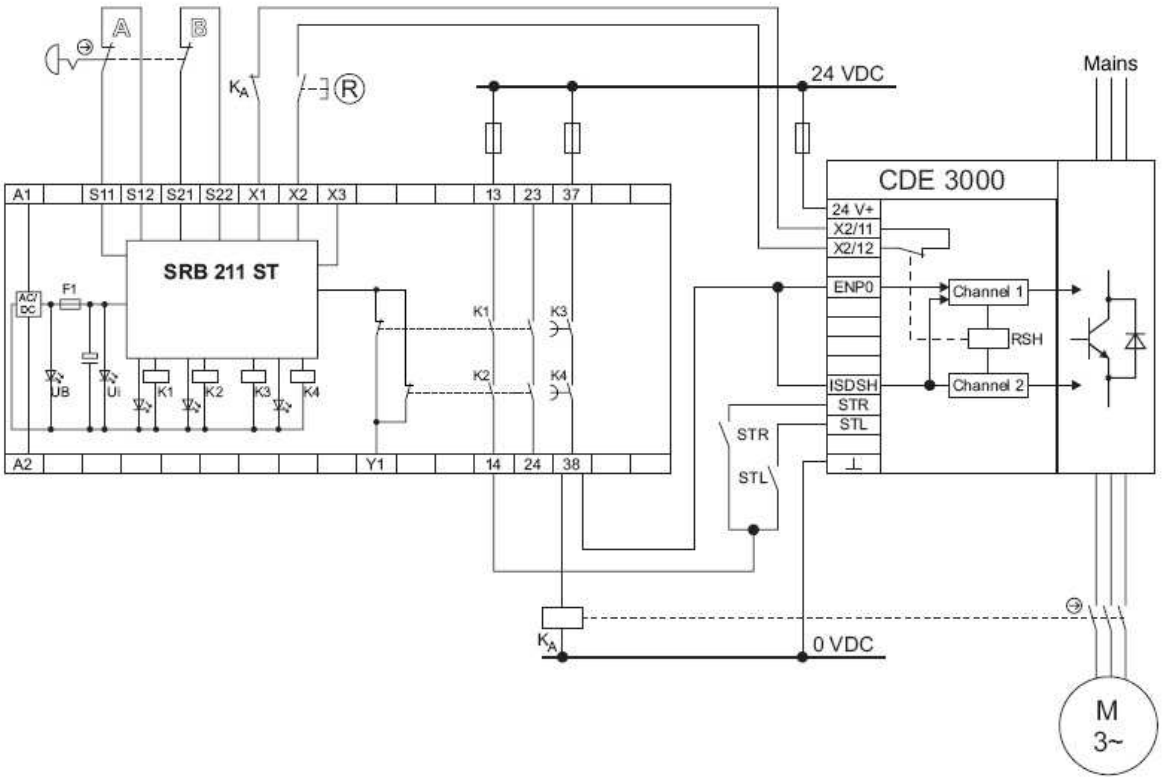
Configuration	Safety category (SC) EN 954-1	Stop category EN 60204-1
Sensor	SC3 without cross-circuit detection	-
CDE3000 with power contactor K_A	SC4 based on in-series configuration of power contactor K_A with positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)
CDE3000 without power contactor K_A	Emergency stop to EN 13850 with SC3 based on positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)



Where the drive controller and safety relay are installed in separate locations, preference should be given to the solution with power contactor K_A. It should be ensured that the wiring to K_A and CDE3000 is kept separate, or an appropriate fault exclusion (e.g. protective tubing) is executed.

Two-channel emergency off/emergency stop circuit EN 418/ EN 60947-5-5 with stop category 1 to EN 60204-1 and cross-circuit detection

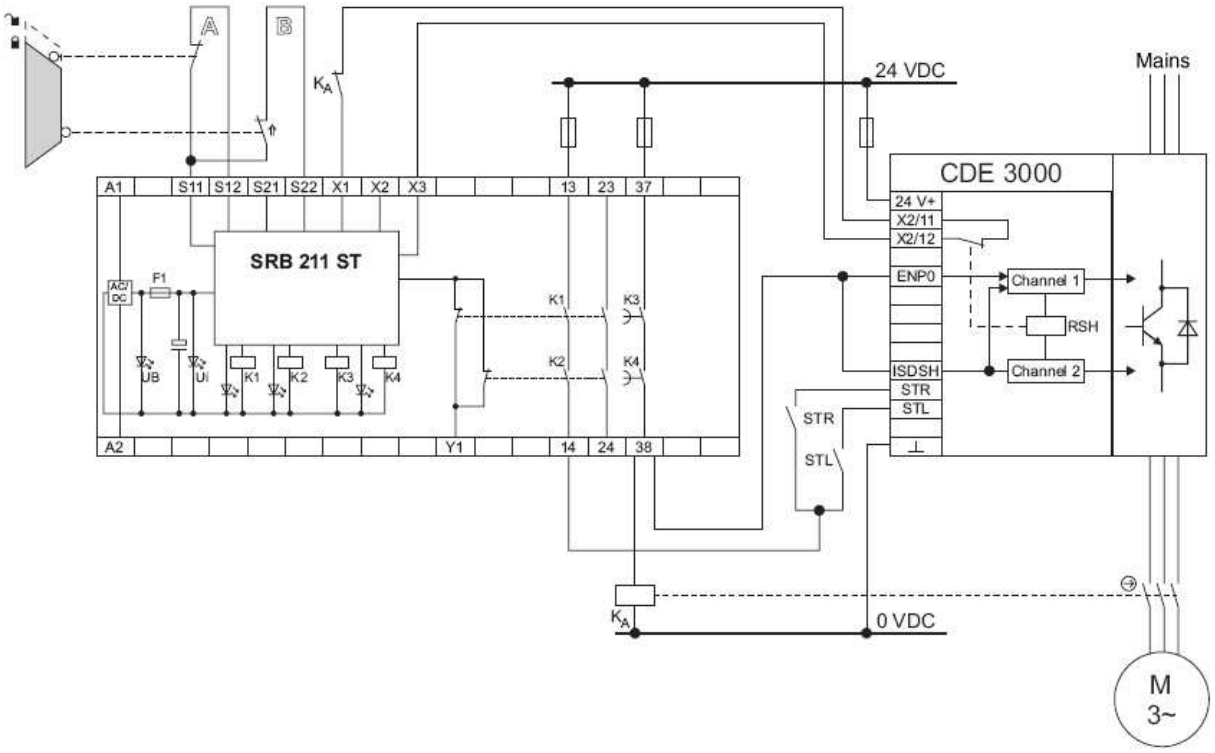
Configuration	Safety category (SC) EN 954-1	Stop category EN 60204-1
Sensor	SC4 with cross-circuit detection	-
CDE3000 with power contactor K_A	SC4 based on in-series configuration of power contactor K_A with positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)
CDE3000 without power contactor K_A	Emergency stop to EN 13850 with SC3 based on positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)



Where the drive controller and safety relay are installed in separate locations, preference should be given to the solution with power contactor K_A. It should be ensured that the wiring to K_A and CDE3000 is kept separate, or an appropriate fault exclusion (e.g. protective tubing) is executed.

Two-channel guard door monitoring to EN 1088 with at least one forced-opening position switch

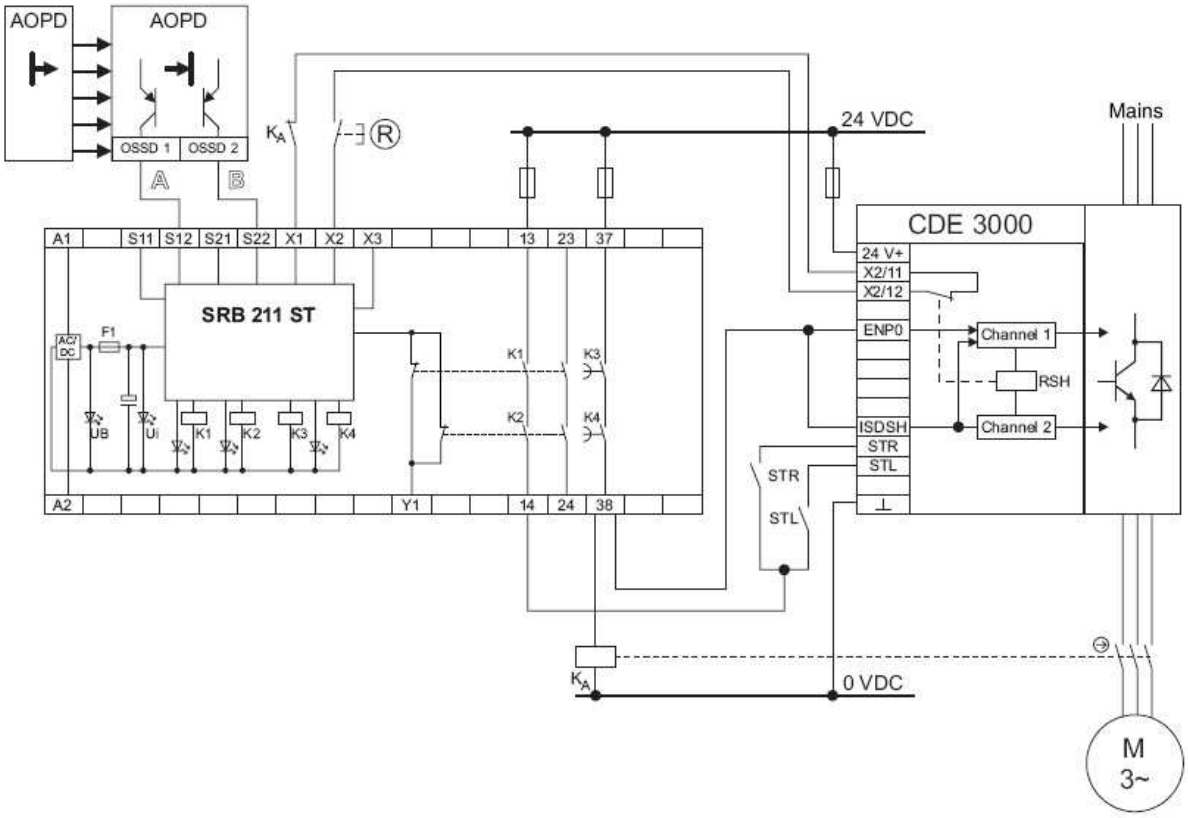
Configuration	Safety category (SC) EN 954-1	Stop category EN 60204-1
Sensor	SC3 without cross-circuit detection	-
CDE3000 with power contactor K_A	SC4 based on in-series configuration of power contactor K_A with positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)
CDE3000 without power contactor K_A	Emergency stop to EN 13850 with SC3 based on positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)



Where the drive controller and safety relay are installed in separate locations, preference should be given to the solution with power contactor K_A. It should be ensured that the wiring to K_A and CDE3000 is kept separate, or an appropriate fault exclusion (e.g. protective tubing) is executed.

Two-channel actuation with safety-oriented p-switching semiconductor elements, e.g. AOPD's to EN 61496

Configuration	Safety category (SC) EN 954-1	Stop category EN 60204-1
Sensor	SC3 with cross-circuit detection in sensor (not by safety relay)	-
CDE3000 with power contactor K_A	SC4 based on in-series configuration of power contactor K_A with positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)
CDE3000 without power contactor K_A	Emergency stop to EN 13850 with SC3 based on positioning drive CDE3000 in SC3 design	Stop category 1 (controlled shutdown)



Where the drive controller and safety relay are installed in separate locations, preference should be given to the solution with power contactor K_A. It should be ensured that the wiring to K_A and CDE3000 is kept separate, or an appropriate fault exclusion (e.g. protective tubing) is executed.

Advantages of using drive controllers with certified "Safe Standstill" to EN 954-1, category 3

Benefits to you	Drive controllers with "Safe Standstill" control function	Conventional solution based on external switching elements
Reduced componentry and circuit complexity	• Easy procurement of certified safety function possible. • Group drive with one main contactor possible.	Two safety-oriented power contactors in-series required.
Frequent routine testing permissible	The "Safe Standstill" state is attained by use of non-wearing electronic components.	This feature is not attainable by conventional technical means.
Short restart times	The drive controller is not disconnected from the mains on the power side, so no discernible wait times occur on restarting.	The drive must be disconnected from the mains on the power side, so ever longer restart times must be accepted.
Improved EMC	Improved EMC based on full screening of the motor cable.	Not possible based on power contactors in the motor cable.

Table 5.12 Advantages of using drive controllers with "Safe Standstill"

5.6.4 Safety functions for movement control

The basic principles of safety functions in drive systems are summarized in the position paper DKE-AK226.03.
The paper serves, among other roles, as a discussion paper for drafting the product norm EN 61800-5-2 (Development of variable-speed drive systems).

The paper details safety functions. Safety functions which ensure comparable safety to an isolating safety device and disconnection of the drive from the mains.

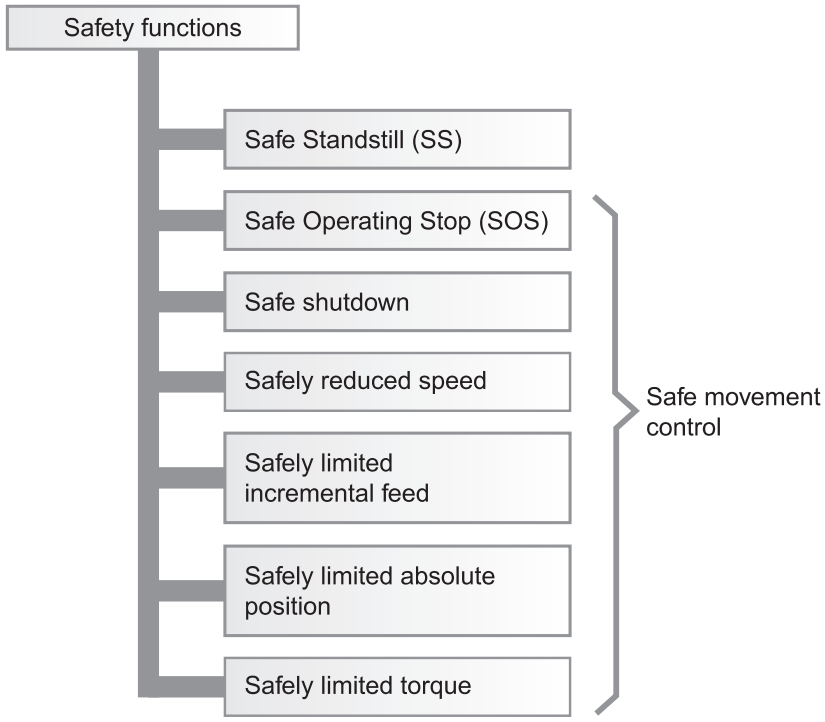


Figure 5.24 Safety functions

With the exception of the "Safe Standstill" (SS) function, all safety functions require an at least two-channel monitoring and shutdown principle. This requirement is met by means of a two-channel computer structure fulfilling the demands for safe movement control and of EN 954-1 category 3.

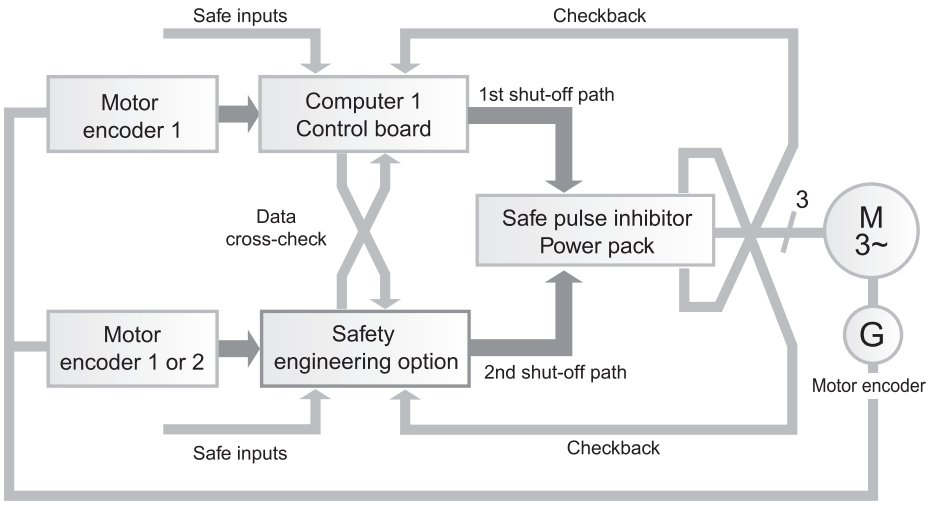


Figure 5.25 Two-channel computer structure for the safety function of a movement control

Movement control

In practice a motor encoder is in most cases replaced by a motor model implemented on the computer.

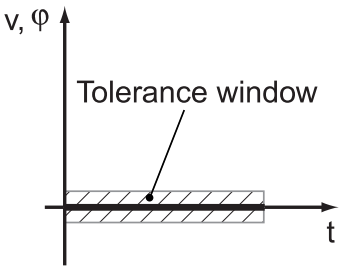
The signals generated in the encoders are evaluated over two channels by computers 1 and 2. This means velocity, position, end stop and cam monitors are implemented in two-channel mode. All safe inputs, e.g. for selecting the safety-related machine functions such as safely reduced velocity etc., are likewise implemented redundantly. The "pulse inhibitor" function block processes stop requests over two channels. In case of a fault (that is, if the safety function fails) both computers have an independent shutdown path.

In order to detect faults in the safety control system, both computers execute a cross-check of the safety-related data as well as self-tests. Inputs with slow or infrequent signal changes are checked by means of forced signal changes (forced dynamization). The outputs are tested in regularly required stop states (test stops).

The computer structure illustrated is implemented in different ways in practice. This section does not deal with that implementation as such, but with the safety function itself.

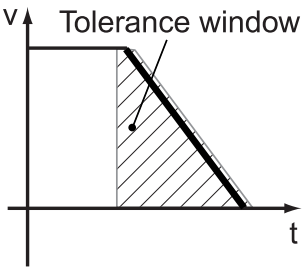
Safety functions

Safe Operating Stop (SOS)



Safe Operating Stop is the state in which the mechanical component is held at standstill, whereby the drive in speed or position control mode.

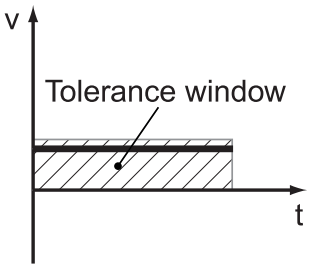
Safe Standstill



Standstill is the reduction of movement to a stop. The process begins with the stop request and ends when the movement has come to a standstill. The safety drive monitors the speed curve and, where appropriate, the time.

Safe Standstill: The Safe Standstill function can be executed in a range of variants. The variant applied depends on the machine and on the risk assessment. The variants (stop categories 0, 1, 2) are defined in EN 60204 part 1, see section 5.6.

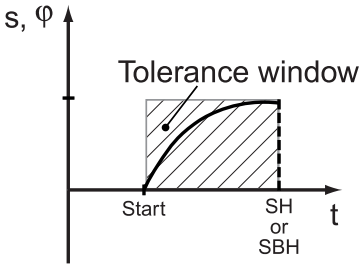
Safely reduced speed



A reduced speed is set by the control system. The speed of a drive is monitored for exceeding of a maximum.

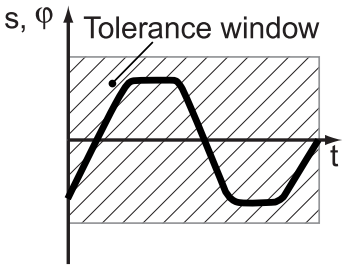
Safely reduced speed: Application of the "Safely reduced speed" function is subject to the proviso that a person is still able to escape danger arising from hazardous movements. Generally this can be assumed where the resultant speed of hazardous movements not involving risk of crushing and shearing does not exceed 15 m/min., and in the case of hazardous movements involving risk of crushing and shearing does not exceed 2 m/min.

Safely limited incremental feed



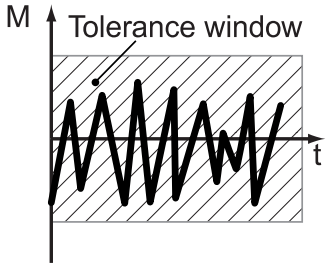
Limited incremental feed is a position change which begins at standstill, in which a pre-determined path/ angle is covered and which ends at standstill. A preset incremental feed must not be exceeded. Then a "Safe Standstill" (SS) or "Safe Operating Stop" (SOS) takes effect.

Safely limited absolute position



The limited absolute position is the absolute position at which a movement must have come to a standstill. The position of a drive is monitored for exceeding of the permissible end position.

Safely limited torque



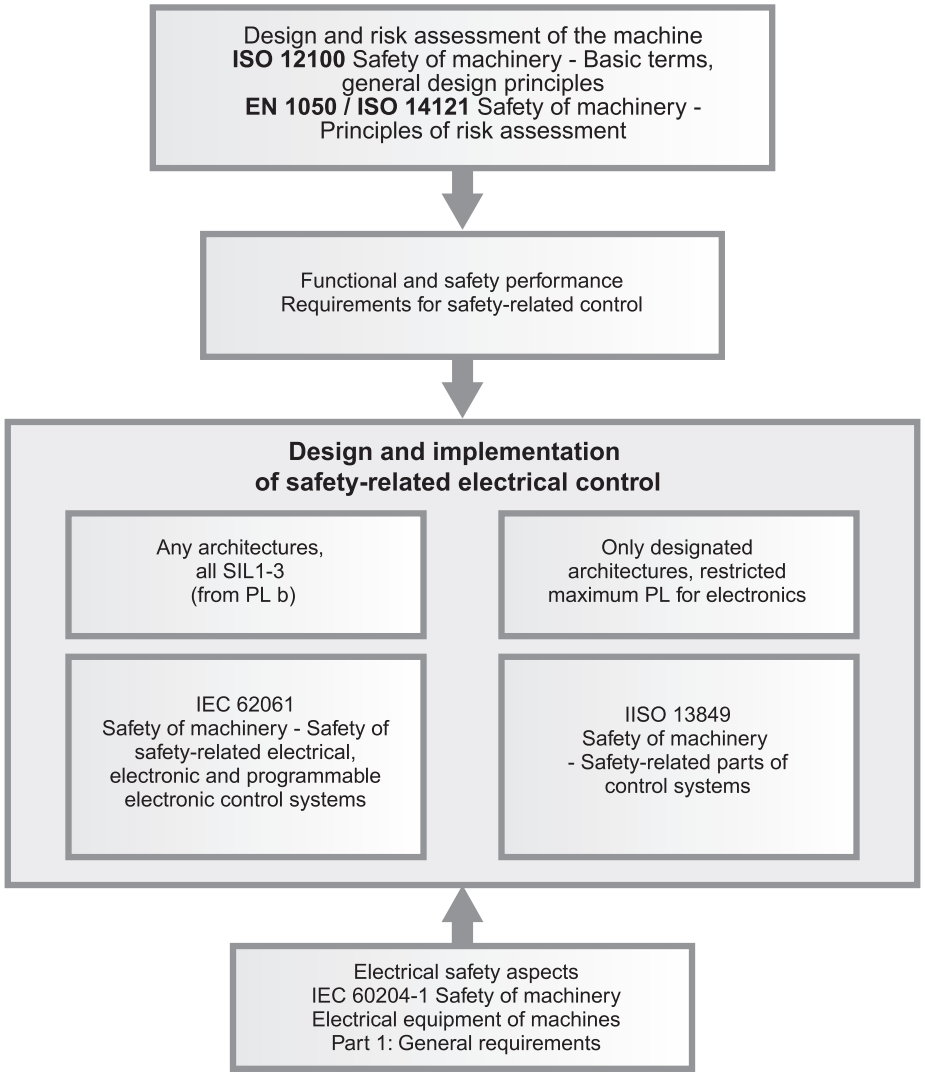
Monitoring of the torque of a drive for exceeding of the permissible maximums. The danger from hazardous movements is limited.

5.6.5 Application of future EN ISO 13849-1 (EN 954-1) and EN IEC 62061

The content of this section is based primarily on the ZVEI (Geman Electrical and Electronic Manufacturers' Association) Flyer issued in November 2004 titled "Anforderungen an moderne Steuerungssysteme für Sicherheitsaufgaben an Maschinen" [Requirements made of modern control systems for safety functions on machines].

Scope of the norm

The EU Machinery Directive stipulates that machines must be safe, and requires inherent safety as the primary design goal. To protect against hazards that cannot be eliminated by design additional safety devices must be installed. EN ISO 12100 parts 1 and 2 detail fundamental design principles and technical principles by which this goal can be attained. Where safety depends on control functions, the control system must be executed such that the likelihood of malfunction is suitably low. When using programmable electronic systems, the IEC 61508 standard must also be observed. EN ISO 13849 and EN IEC 62061 provide instructions specifically for the safety of machine control systems.



With regard to the potential hazards of a machine, risk assessments must be carried out in accordance with EN 1050 (in future EN ISO 14121) in order to ascertain whether adequate safety has been attained. The requirements of EN IEC 62061 and EN ISO 13849-1 relating to the implementation of safety-related control functions are classified according to the level of risk. The basis for this classification set out in EN IEC 62061 (as in IEC 61508) is the Safety Integrity Level (SIL) and in EN ISO 13849-1 the Performance Level (PL).

Performance Level (PL)		
Performance level (PL)	**Average probability of a dangerous failure per hour [l/h]**	**SIL [EN 61508-1 (IEC 61508-D]**
a	$\geq 10^{-5}$ to $< 10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3
NOTE 1 The performance for each hazardous situation in this standard is divided into five levels "a" to "e" where the risk reduction contributed by the SRP/CS in "a" is low and in "e" is high.		
NOTE 2 It should be noticed that performance levels b and c together cover only one order of magnitude on the scale of average probability of a dangerous failure per hour (or one step on the SIL scale).		

Table 5.13 Comparison of Safety Integrity Level (SIL) and Performance Level (PL)

As there is no prospect of "testing out" all faults occurring in complex machine control systems once built, these standards also embody the all-embracing approach of aligning all development and project planning of safety-related control systems to the avoidance of faults from the very beginning. The two standards also share a probabilistic approach in determining hazardous failure rates.

The qualitative analysis as per EN 954-1 is no longer adequate to the technology of modern-day control systems. Among other criteria, EN 954-1 does not take into account time factors (e.g. test intervals and cyclic testing; lifetime). This resulted in the probabilistic approach embodied in IEC 61508, EN IEC 62061 and EN ISO 13849-1 (failure probability per time unit).

The areas of application of EN ISO 13849-1 and EN IEC 62061 are largely the same. Consequently, as a decision-making aid for users, the IEC and ISO committees have detailed the areas of application of the two standards in a single table contained in both their introductions.

Depending on the technology (mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic), risk classification and architecture, EN ISO 13849-1 or EN IEC 62061 will be applicable.

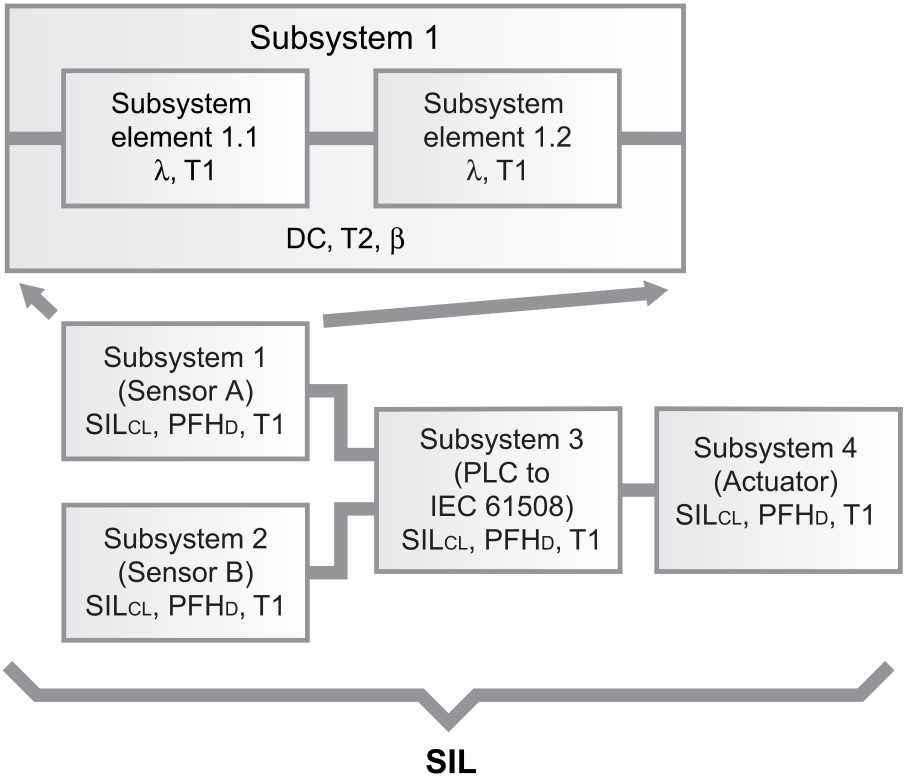
Technology implementing the safety-related control functions	EN ISO 13849-1 (rev)	EN IEC 62061
A Non-electrical, e.g hydraulic, pneumatic	X	Not covered
B Electromechanical, e.g. relays and/or simple electronics	Limited to designated architectures (see Note 1) and maximum PL = e	All architectures and up to SIL 3
C Complex electronics (e.g. programmable electronics)	Limited to designated architectures (see Note 1) and up to PL = d	All architectures and up to SIL 3
D A combined with B	Limited to designated architectures (see Note 1) and up to PL = e	X See Note 3
E C combined with B	Limited to designated architectures (see Note 1) and up to PL = d	All architectures and up to SIL 3
F C combined with A or C combined with A and B	X See Note 2	X See Note 3
Note 1: Designated architectures are defined in Annex B of EN ISO 13849-1 and provide a simplified approach for quantification **Note 2:** For complex electronics: Use of designated architectures according to EN ISO 13849-1 up to PL = d or any architecture according to EN IEC 62061 **Note 3:** For non-electrical technology: Use parts according to EN ISO 13849-1 (rev) as subsystems.		

Application of either of these standards can be presumed to fulfil the protective goals of the Machinery Directive.

EN IEC 62061: Safety-related electrical control systems for machines

EN IEC 62061 is a sector-specific norm subsidiary to IEC 61508. It details the implementation of safety-related electrical control systems of machines and considers the entire lifecycle from the concept phase through to decommissioning. The bases are quantitative and qualitative analyses of safety functions.

The standard applies a consistent top-down approach in the implementation of complex control systems, termed Functional Decomposition. Based on the safety functions resulting from the risk assessment, this establishes a breakdown by safety subfunction, and finally assigns those subfunctions to real equipment, termed subsystems and subsystem elements. Both hardware and software are covered. EN IEC 62061 also sets out requirements for the implementation of application programs.



A safety-related control system comprises various subsystems. The subsystems are classified in safety terms by their characteristics (SIL claim limit and PFH).

Safety characteristics of subsystems:

- SIL_{CL}: SIL claim limit
- PFH_D: Probability of dangerous failure per hour
- T_1: Lifetime

These subsystems may in turn comprise varyingly configured subsystem elements (equipment) with the characteristics determining the corresponding PFH rating of the subsystem concerned.

Safety characteristics of subsystem elements (equipment):

- λ: Failure rate; for elements subject to wear: BIO value
- T_1: Lifetime

For electromechanical equipment the failure rate λ is specified by the manufacturer referred to a number of switching cycles. The time-based failure rate and the lifetime must be determined on the basis of the switching frequency for the application concerned.

Parameters to be specified in design of the subsystem comprising subsystem elements:

- T_2: Diagnostic test interval
- ß: Susceptibility to common cause failure
- DC: Diagnostic coverage

The PFH rating of the safety-related control system is determined by adding together the individual PFH values of the subsystems.

When constructing a safety-related control system the user has the following options:

- Use of equipment and subsystems already conforming to EN 954-1 and IEC 61508 or EN IEC 62061. For this the standard stipulates how qualifying equipment can be integrated in the implementation of safety functions.
- Development of dedicated subsystems
  - Programmable electronic systems and complex systems: Application of IEC 61508.
  - Simple equipment and subsystems: Application of EN IEC 62061.

There are no specifications relating to non-electrical systems however. The standard represents a comprehensive norm for implementing safety-related electrical, electronic and programmable electronic control systems.

For non-electrical systems EN 954-1 / EN ISO 13849-1 is applicable.

EN ISO 13849-1 is intended to supplant EN 954-1

EN ISO 13849-1 is based on the familiar categories from
EN 954-1:1996. It now also considers complete safety functions with all the equipment involved in its execution.

EN ISO 13849-1 goes beyond the qualitative approach of
EN 954-1 to also provide a quantitative analysis of the safety functions. Based on the categories, Performance Levels (PL's) are used for this. The following safety characteristics of components/equipment are required:

- **Category** (structural requirement)
- **PL:** Performance Level
- **MTTFd:** Mean time to dangerous failure
- **DC:** Diagnostic coverage
- **CCF:** Common cause failure

The standard details calculation of the Performance Level (PL) for safety-related parts of control systems based on designated architectures. In case of non-conformance to those architectures, EN ISO 13849-1 makes reference to IEC 61508.

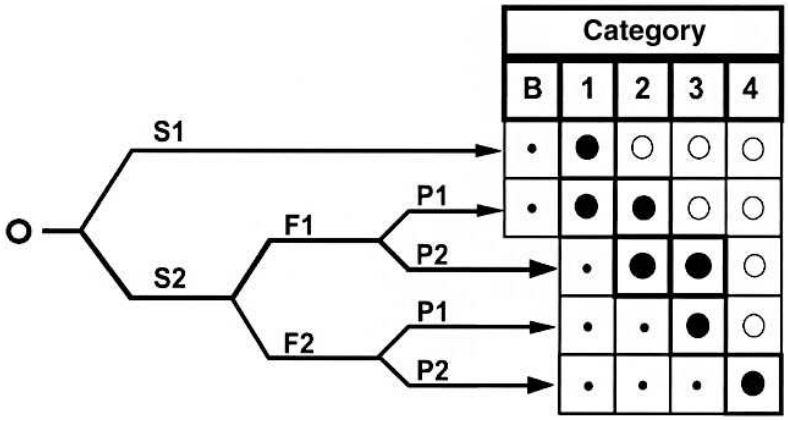
Where multiple safety-related parts are combined to form a single overall system, the standard sets out stipulations for determining the resultant PL.

For further information on validation EN ISO 13849-1 refers to part 2, which was published at the end of 2003. It contains stipulations regarding fault analysis, maintenance, technical documentation and directions for use.

IEC 61508 and EN IEC 62061 are also ratified as EN norms.
EN ISO 13849-1 (rev) is in draft form. Until its adoption, scheduled for September 2005, EN 954-1:1996 will continue to apply.
It must be assumed that EN ISO 13849 will be applicable as from 2006/7.
It can therefore be estimated that EN 954-1 will be withdrawn and replaced by EN ISO 13845 around 2009/10.

Comparison of the old and new risk graphs

EN 954-1



S: Severity of injury
F: Frequency and/or duration of hazard
P: Possibility of avoiding hazard

EN ISO 13849

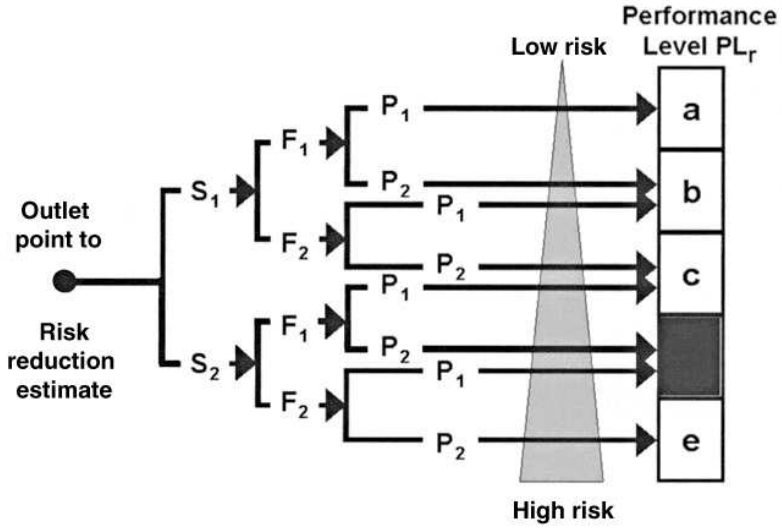


Figure 5.26 Risk graph - EN 954-1/ EN ISO 13849

Comparison chart of the various levels

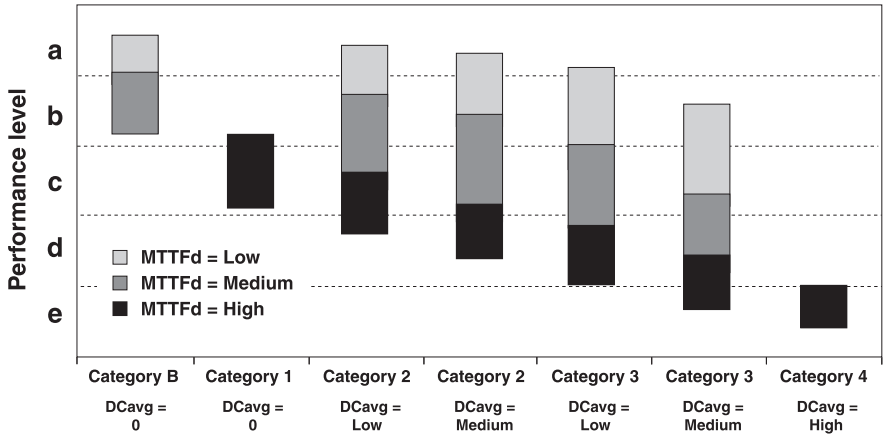


Figure 5.27 Simplified determination of Performance Level PL

EN 954-1 SC[1)]	EN ISO 13849-1 PL[2)]	IEC 62061 SIL[3)]	IEC 61508 SIL[3)]
B	a	-	-
1	b	1	1
2	c		
3	d	2	2
4	e	3	3

1) Safety category
2) Performance Level
3) Safety Integrity Level

Table 5.14 Comparison chart of the various classification systems

ISO	International Organization for Standardization www.iso.org
IEC	International Electrotechnical Commission www.iec.ch
CEN	European Committee for Standardization (Comité Européen de Normalisation) www.cenorm.be
CENELEC	European Committee for Electrotechnical Standardization Comité Européen de Normalisation en ELECtronique www.cenelec.org
DKE	Deutsche Kommission Elektrotechnik und Elektronik (Geman Commission for Electrical, Electronic & Information Technologies) www.dke.de
DIN	Deutsches Institut für Normung (Geman Institute for Standardization) www.din.de