

Safety Manual

Safety technology for machines and systems
in accordance with the international standards
EN ISO 13849-1 and IEC 62061



EAT•N

Powering Business Worldwide



TM2A Soluções e Componentes Industriais
Rua Cidade de Viena 2, Parque Ind. Arneiro
2660-456 São Julião do Tojal
PORTUGAL

T: +351 219737330
www.tm2a.pt

F: +351 219737339
info@tm2a.pt

All proprietary names and product designations are brand names or trademarks registered to the relevant title holders.

Extracts from the **DIN Standards with VDE Classification** are quoted with the authorisation of the DIN (Deutsches Institut für Normung e.V.) and the VDE (Verband der Elektrotechnik Elektronik Informationstechnik e.V.) It is imperative for the use of the standards that the issue with the latest date is used. These are available from VDE-VERLAG GMBH, Bismarckstr. 33, 10625 Berlin, www.vde-verlag.de and Beuth Verlag GmbH, Burggrafenstr. 6, 10787 Berlin.

The safety-related content of this manual has been tested by TÜV Rheinland Industrie Service GmbH.

1st published 2008, edition date 10/08,
2nd edition 10/2010
3rd edition 2015, edition date 07/15
© 2015 by Eaton Industries GmbH, 53105 Bonn

Authors: Lütfiye Dönoglu, Benjamin Papst, Rainer Menden
Production: Thomas Kracht

All rights, including those of translation, reserved.

No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, micro-filming, recording or otherwise, without the prior written permission of Eaton Industries GmbH, Bonn.

Subject to alteration.

Foreword

Dear reader,

In life it is often advisable to make compromises. However, this is not so when it comes to the subject of safety! Safety is always a fundamental basis for advancement and success both in the recreational sphere and at work. This particularly applies to the use of machines and plants.

We at Eaton know how much machine builders, operators and users depend on the continuous reliability and safe functioning of all components and systems. The machine should not present any hazards to persons at any time. For this reason, we develop and produce safety components that you can rely on, particularly when this is very important.

We are one of the largest manufacturers worldwide in the production of components for the safe emergency stopping of plants and machinery. Our emergency-stop pushbutton actuators and switching devices have been first choice for several decades, when it comes to establishing a safe state in the event of a hazard. Our future-oriented technologies includes the innovative **easy**Safety control relay which combines standard functions with the safety-related monitoring and processing of machine signals. We can thus offer our customers a comprehensive range of products for functional safety with a very favorable cost-benefit ratio.

Eaton components always meet the most stringent international safety requirements as stipulated by the relevant standards. This particularly applies to the currently valid safety standards EN ISO 13849-1 and IEC 62061. With Eaton you are always on the safe side.


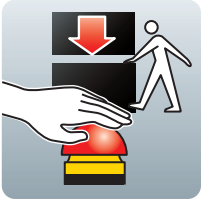
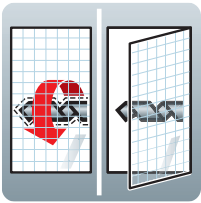
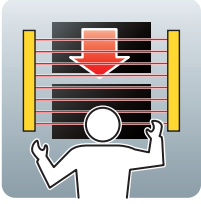
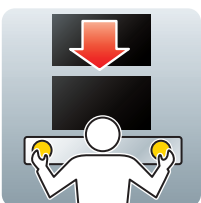
This edition of the Eaton Safety Manual explains what has changed on account of the new standards. Not only are all the relevant standards explained: This guide is an outstanding opportunity to become acquainted step by step with the wide ranging issues of functional safety technology. Several circuit examples with the relevant safety parameters help to illustrate the information provided. Like the Moeller Wiring Manual, which has been recognised over decades, the Safety Manual is a well-founded and competent guide for theoretical and practical issues.

„Safety Technology – Control the unexpected“

Control the unexpected – this is the motto with which Eaton wishes everyone interesting and useful reading of the “Safety Manual”!

May it always be a “safe” and reliable companion for you.

Your Eaton Industries GmbH

	Introduction Safety instructions and operating guidelines Functional safety for man, machine and environment	5 5 8
	1 Stopping in case of emergency (Emergency-stop disconnection) 1.1 In the main circuit 1.2 In the control circuit for simple drives 1.3 For interrupting several control circuits with safety relay 1.4 For interrupting several control circuits with easySafety 1.5 Two-channel with safety relay 1.6 Two-channel with easySafety 1.7 With electronically controlled drives 1.8 Two-channel configuration with variable frequency drive using STO 1.9 With SmartWire-DT 1.10 With CMD contactor monitoring relay 1.11 Single-channel with EMS electronic motor starter 1.12 Two-channel configuration with EMS electronic motor starter, safety shutdown	12 12 14 16 18 20 22 24 26 28 30 32 34
	2 Monitoring a movable guard 2.1 Single-channel with safety relay 2.2 Single-channel with easySafety 2.3 Several guards with safety relay 2.4 Several guards with easySafety 2.5 Two-channel with safety relay 2.6 Two-channel with safety relay and RS2 2.7 Two-channel configuration with safety relay and redundant RS2 2.8 Two-channel with easySafety 2.9 With guard locking – enable via timer 2.10 With guard locking – enable via zero speed monitoring	36 36 38 40 42 44 46 48 50 52 54
	3 Monitoring open hazardous area 3.1 With light curtain and safety relay 3.2 With light curtain and easySafety 3.3 With light curtain muting and easySafety	56 56 58 60
	4 Enabling safe operation 4.1 With two hand control type III C 4.2 With two hand control type III C	62 62 64

	5 Enabling setting 5.1 With operating mode selector switch	66 66
	6 Combining several safety functions 6.1 Stopping in an emergency (Emergency-stop disconnection) 6.2 Monitoring a movable guard 6.3 Speed monitoring with easySafety	68 68 70 72
	7 Preventing restarts 7.1 With contactors 7.2 With easySafety 7.3 With feedback circuit	74 74 76 78
	8 Preventing unexpected startup 8.1 For short interventions	80 80
	9 For repair and maintenance safety 9.1 With power disconnecting device (main switch) 9.2 With devices for isolating the electrical equipment 9.3 With repair, maintenance and safety switch	82 82 84 86
	10 Protection against electric shock 10.1 Protective isolation 10.2 ELV extra low voltage with safe isolation	88 88 90
	11 Machine engineering in accordance with IEC 60204-1 11.1 Power supply and protective devices 11.2 Long control cables 11.3 Circuit design and use of equipment	92 92 94 96



12	The way to a safe machine	98
12.1	Schedule	98
12.2	Directives important for machines	100
12.3	Overview of relevant safety standards	102
12.4	Machine-related product standards	116
12.5	Steps to the Performance Level PL in accordance with EN ISO 13849-1	118
12.6	Steps to SIL safety integrity level according to IEC 62061	126



13	Appendix	136
13.1	Glossary of terms	136
13.2	Overview of safety-related parameters	146
13.3	Safety integrity for circuits in chapters 1 to 6	148
13.4	Machines and safety components in compliance with the Machinery Directive	150
13.5	Requirements for existing machines	152
13.6	Reference sources for regulations, bibliography	154

	Index	156
--	--------------	-----

Introduction

Safety instructions and operating guidelines

To use this Safety Manual observe the following instructions and notes:

1. The creation of circuit diagrams and the commissioning of machines and plants require a specialist knowledge of safety and electrical engineering. Plant sections and persons are at risk if machines and plants are incorrectly connected or configured, and active components such as motors or pressure cylinders are incorrectly controlled.
2. The application examples shown in this safety manual were created by Eaton to the best of our knowledge and belief and in accordance with the current state-of-the-art. Nevertheless, errors in the examples cannot be excluded. If you encounter any malfunction, error and/or any other problem when using the examples, please contact your Eaton contact person.
3. The circuits shown in these application examples are only designed for use if the conditions, properties and functions expressly stated in the example are observed. The application examples do not cover all conditions, properties and functions that are available for the creation of circuit diagrams and the commissioning of machines and plants.
4. The application examples presented in this Safety Manual only take into account the safety parameters expressly listed in accordance with EN ISO 13849-1 and IEC 62061. In certain circumstances these safety-related parameters do not cover all safety aspects that are relevant for preparing the circuit diagrams and for the commissioning of machines and plants. This document does not take into account any modifications of safety-related parameters resulting from amendments to EN ISO 13849-1 and IEC 62061.
5. It is the sole responsibility of the user to observe the following when using the Safety Manual:
 - all relevant regulations regarding the preparation of circuit diagrams for machine and plant components in accordance with the latest user manuals of the relevant manufacturer,
 - all relevant regulations, directives, rules and standards of occupational safety and accident prevention, particularly those issued by employers' liability Insurance associations, regarding the commissioning, preparation of circuit diagrams and the use of machine and plant components for the application planned by the user,
 - acknowledged rule of technology and state of science as well as
 - all other general due diligence regarding the prevention of damages to life and physical condition of persons as well as material damage..
6. Eaton assumes no liability for any damage caused by the use of this Safety Manual contrary to the conditions of use stated in the preceding sections 1 to 4.

Introduction
Safety instructions and operating guidelines

Target group

This Safety Manual is directed at the following target groups that are responsible for machine safety:

- Manufacturer.
- Operators.
- Designers and planners.
- Safety operative.
- Service and maintenance personnel.

Specialist knowledge is required for the design and application of functional safety of machinery. All applicable directives, standards and regulations of the relevant country must be observed.

Other language versions of this manual can be ordered via the Internet at www.eaton.com/moellerproducts.

Layout of the manual

This Safety Manual provides an overview of the most important requirements of directives, standards and regulations that must be taken into account when using safety equipment on machines.

With example circuits, the manual illustrates how functional safety can be achieved with electrical, electronic and electronic programmable components and systems in safety-relevant applications.

Each example circuit is provided with all the relevant information on the selected circuit and the conditions of use. The descriptions of all example circuits are divided identically into the following areas:

Application This shows you the applications in which it can be used. The design of the application is explained by means of a circuit diagram.

Requirements The conditions listed here must be fulfilled in order to use the example circuit.

Properties Shows the particular properties of the application example.

Function Describes the circuit diagram of the application example in words.

Safety characteristic values in accordance with EN ISO 13849-1 and IEC 62061 were calculated for all safety applications and related assumptions. The result is shown in the form of a table in the header of the respective chapter.

Table with 3 rows and 6 columns. Row 1: Cat, B, 1, 2, 3, 4. Row 2: PL, a, b, c, d, e. Row 3: SIL, 1, 2, 3. To the right is a table with 3 rows: Category to EN 954-1 (1997), Performance level PL acc. to EN ISO 13849-1, Safety Integrity Level SIL acc. to IEC 62061.

Chapters with the cases A and B show that the determined safety levels may differ due to the different number of switching cycles.

Two tables labeled Case A and Case B. Case A table has 3 rows (Cat, PL, SIL) and 6 columns (B, 1, 2, 3, 4). Case B table has 3 rows (Cat, PL, SIL) and 6 columns (B, 1, 2, 3, 4).

ICapters 12.5 "Steps to the Performance Level PL in accordance with EN ISO 13849-1", page 118, and 12.6 "Steps to SIL safety integrity level according to IEC 62061", page 126, explain in detail how the results are achieved by means of an example.

Each chapter also shows a pictogram in the header for faster orientation. These pictograms help you to assign the circuit examples to the corresponding safety functions quickly and simply. They are explained in the following pages..

Terms, abbreviations and symbols

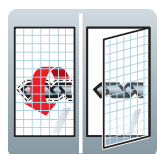
The **technical terms** used in this book are explained in alphabetical order in chapter 13.1 „Glossary of terms“, page 136.

Abbreviations and their meaning are explained in the fold-out section of the rear cover. This will enable you to view the abbreviations directly when the cover is opened out.

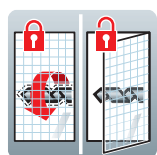
The **pictograms** in this Safety Manual have the following meaning:



Emergency-Stop circuits



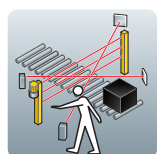
Monitoring of movable guards with guard monitoring without interlock/guard locking



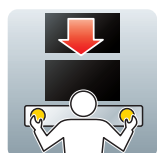
Monitoring of movable guards with guard monitoring with interlock/guard locking



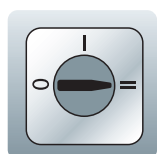
Monitoring open hazardous area with light curtain



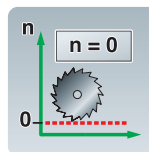
Monitoring open hazardous area with light curtain with mute function



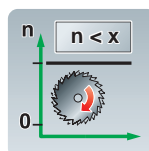
Safe operation with two-hand control



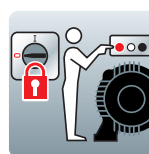
Enabling safe setting, with operating mode selector switch



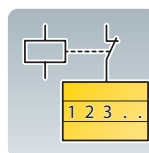
Zero speed monitoring



Monitoring maximum speed



Preventing restarts



Monitoring of externally connected actuators via feedback circuits



Preventing unexpected startup



Protection against electric shock



Danger!

Warns about the possibility of major property damage and serious injuries or death.



Draws your attention to interesting tips and supplementary information.

Introduction

Functional safety for man, machine and environment

Functional safety

During its entire life cycle – from manufacture to disassembling – a machine poses danger to man, machine and the environment. It is therefore necessary to identify these dangers already when the machine is designed and reduce them by means of suitable measures.

The EU Machinery Directive 2006/42/EC stipulates that a machine should not pose any danger. However, as there is no 100% safety in engineering, the aim is to reduce these dangers to a tolerable level of residual risk by means of risk reduction measures. The overall safety of a machine defines the state in which it can be considered as being free of unwarranted risks to persons or as free of danger. The functional safety is part of the overall safety of a system which depends on the correct functioning of the safety-related systems, other technology, safety-related systems and external risk reduction facilities.

Reducing the risk of a machine

The international standard EN ISO 12100 "Safety of machinery – Basic concepts, general principles for design" provides the design engineer with detailed assistance in the identification of hazards and the resulting risks to be assessed. It contains design guidelines and methods for safe design and risk reduction. The first steps concern risk analysis and risk assessment in order to achieve the required level of machine safety.

The EN ISO 12100 stipulates detailed requirements that must be carried out in an iterative process and clearly documented. This therefore lays down the technical measures for the reduction of hazards.

All protective measures deployed in order to achieve the removal of hazards or reduction of risk must be implemented according to a fixed order as specified by EN ISO 12100:



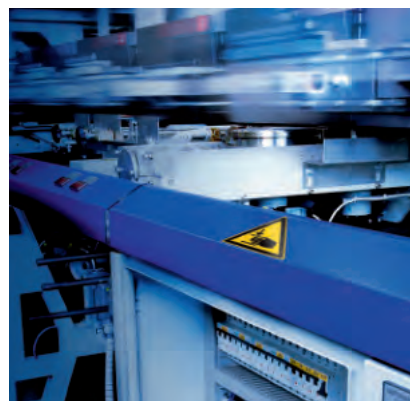
1st. stage: Avoid dangers

Eliminate and reduce risk by design measures during the planning and development stage of the machine.



2nd stage: Secure dangers

Reduce risk through the use of the necessary protective measures.



3rd stage: Indicated other dangers

Reduce risk through notification / hazard warning of residual risk

If the hazards cannot be prevented or sufficiently limited by means of design measures (step 1), safeguards must be provided in step 2 by means of safety-related parts of control systems (SRP/CS). These must be designed and selected so that the probability of functional errors is sufficiently low. If this is not possible, any faults that occur must not lead to the loss of the safety function. In addition to the safeguards of the machine designer, the machine operator or user may require additional protective measures for reducing the residual risk (e.g. personal protective equipment, training etc.).

Avoidance of dangers

Protect against
dangers

Indicate remaining
sources of danger

Risk reduction through the use of safety-related parts of control systems

The parts of machine control systems that handle safety tasks are defined in international standards as the “safety-related parts of control systems” (SRP/CS). These parts can consist of hardware or software and can be separate or integrated elements of the machine control system. Safety-related control system parts comprise the entire safety function consisting of the input level (sensor), the logic (safety signal processing) and the output level (actuator).

The general objective is to design these control system parts so that the safety of the control function and the behavior of the control system in the event of a fault match the level of risk reduction determined in the risk assessment.

Risk reduction through the use of safety-related parts of control systems
The parts of machine control systems that handle safety tasks are defined in international standards as the “safety-related parts of control systems” (SRP/CS). These parts can consist of hardware or software and can be separate or integrated elements of the machine control system. Safety-related control system parts comprise the entire safety function consisting of the input level (sensor), the logic (safety signal processing) and the output level (actuator).

The general objective is to design these control system parts so that the safety of the control function and the behavior of the control system in the event of a fault match the level of risk reduction determined in the risk assessment.

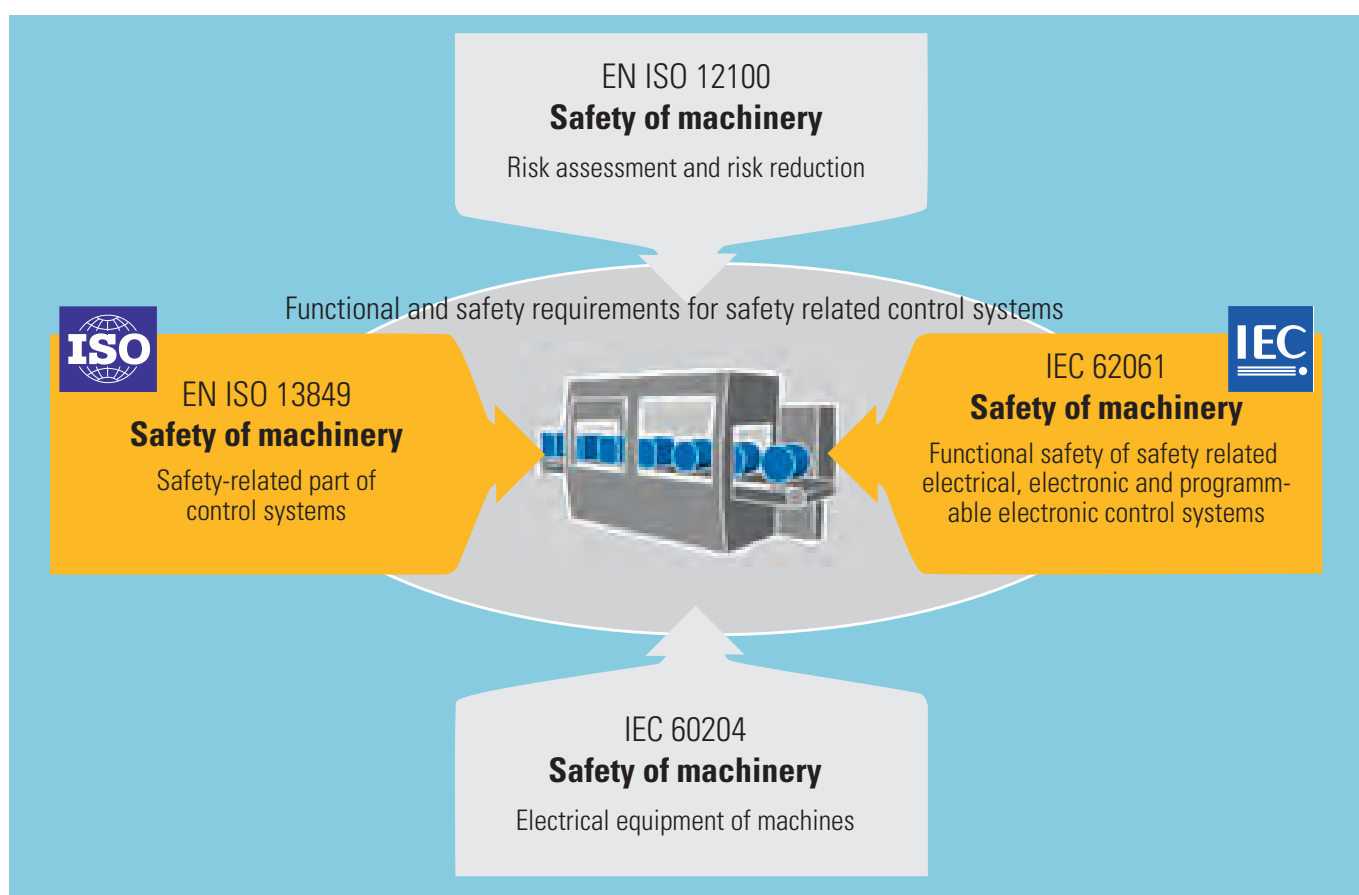


Figure 1: New normative situation



International Standardization Organisation

The ISO is a worldwide association of standards organizations. It draws up and publishes international standards primarily for non-electrical technologies.



International Electrotechnical Commission

The IEC is a global organization that draws up and publishes international standards for electrical engineering and associated technologies.

Introduction

Functional safety for man, machine and environment

EN ISO 13849-1 /-2 "Safety of machinery – Safety-related parts of control systems"

Part 1: General principles for design

Part 2: Validation

EN 954-1, which had already become established as the internationally applicable standard in machine safety, is superseded by EN ISO 13849-1, which was officially passed at the end of 2006 and which is listed as a harmonized standard in the EU Official Journal.

EN ISO 13849-1 implements a quantitative consideration of the safety functions beyond the qualitative approach of EN 954-1. Performance levels (PL) are defined in EN ISO 13849-1 in order to classify the different levels of safety-related performance. The five PLs (a, b, c, d, e) stand for average probability values of a dangerous failure per hour.

The final validation of all protective measures, ensuring the reliable operation of the desired safety functions is part of EN ISO 13849-2.

IEC 62061 "Safety of machinery – functional safety of safety-related electrical and electronic and programmable electronic control systems"

Within the general scope of EN ISO 12100, the IEC 62061 standard is an alternative standard to EN ISO 13849-1. The safety-related performance is described by the three SIL Safety Integrity Levels (1, 2, 3).

Table 1: Two standards for apparently identical application areas: Distinction between EN ISO 13849-1 / IEC 62061

EN ISO 13849-1	IEC 62061
Applicable to hydraulic, pneumatic and electromechanical systems without restriction.	Only applicable to electrical, electronic and programmable electronic systems.
Applicable to programmable electronic systems with restrictions. Only designated architectures up to PL d.	Use of EN ISO 13849 possible with mixed systems.
Calculation concept based on designated architectures	Any architecture possible.
Suitable for the safety verification of devices and all safety functions using tables.	Suitable for the safety verification of devices and all safety functions using calculations.

Iterative process for the design of safety-related parts of control systems

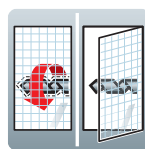
If the final result of stage 1 "Avoid dangers" does not lead to sufficient risk reduction in accordance with EN ISO 12100, the iterative process for designing the SRP/CS in accordance with EN ISO 13849-1 or IEC 62061 should be used in stage 2 "Secure dangers".

In accordance with both standards, the required safety functions to be executed by the SRP/CS are first identified in order to then determine the required properties for each safety function. The appropriate safety functions are used according to the application and required safeguard.

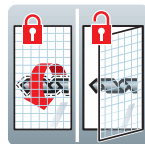
Examples of safety functions:



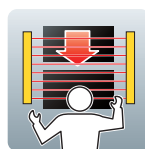
Stopping in case of emergency



Guard door monitoring without interlock/guard locking



Guard door monitoring with interlock/guard locking



Light curtain

The following chapters present a number of example circuits with different safety functions. These have been considered in accordance with both international standards EN ISO 13849-1 and IEC 62061, and the achievable level of safety integrity (PL or SIL) has been calculated with the relevant characteristic values.

General conditions for using the example circuits

The use of the example circuits described in this Safety Manual is subject to general conditions that are not listed in each individual example. These include:

- Observance of requirements in accordance with IEC 60204-1.
- Protection of circuits in accordance with IEC 60204-1.
- Mechanically safe routing of supply cables and components.
- Validation of safety functions in accordance with EN ISO 13849 and IEC 62061.
- When the circuit examples indicate EN ISO 13849, version EN ISO 13849-1 + AC:2009 is meant
- When the circuit examples indicate IEC 62061, version IEC 62061 + AC:2010 + AC1:2013 is meant

Safety Technology from Eaton

Eaton offers you an extensive product portfolio for implementing safety-related solutions. These components with Safety Technology meet the most stringent requirements of the latest international safety standards and are certified by TÜV Rheinland as well as the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA).

Eaton Safety Technology components cover the entire safety chain:

- Fast and safe detection in the input area.
- Safe monitoring and processing by means of logic units.
- Reliable disconnection in the output area.



Safety Technology

Control the unexpected

Fast and secure detection



Input

Safe monitoring and processing



Logic

Reliable shutdown



Output

1 Stopping in the event of an emergency (Emergency-stop disconnection)

1.1 In the main circuit

Application

- For simple drives in which the power disconnecting device (main switch) can be the emergency stop in an emergency situation (Emergency Stop).
- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

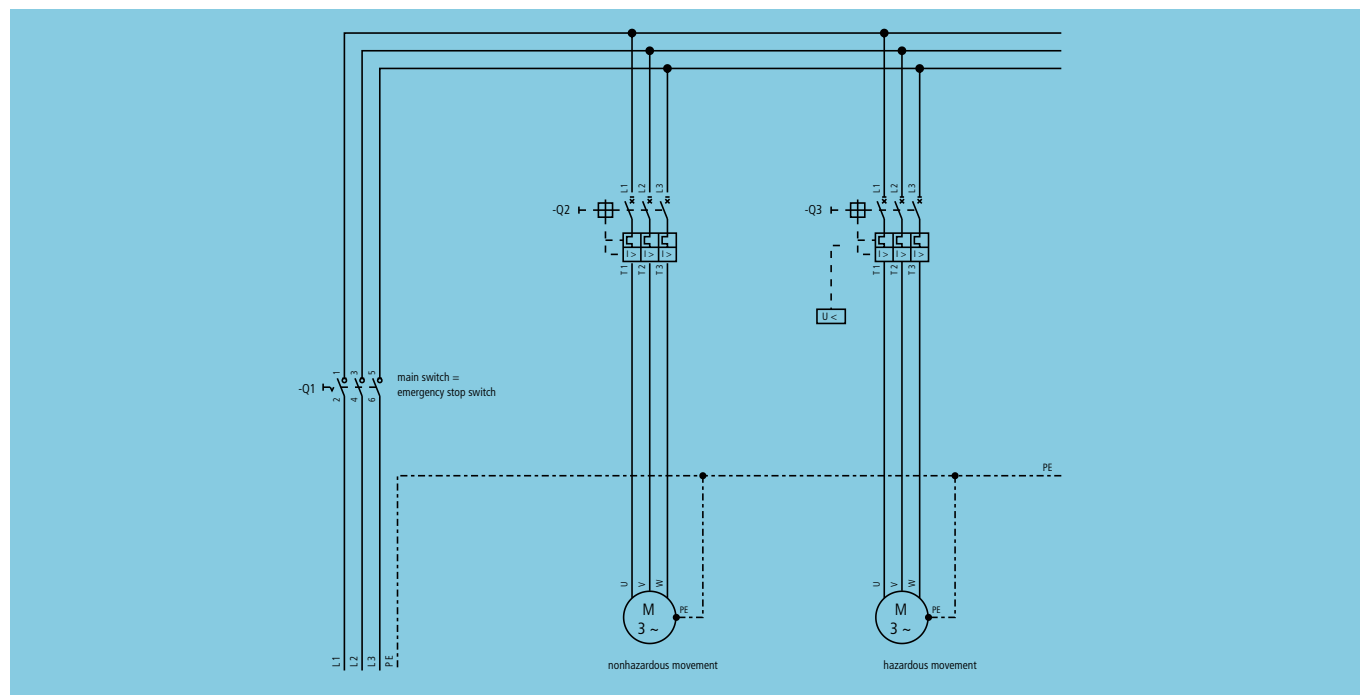


Figure 2: Main switch with emergency stop function

Requirements

- Emergency stop main switch with red handle on yellow background.
- Choose emergency-stop switch with defined switch position (O/I).
- Emergency-stop switch must be easily accessible.
- Switch disconnector features in accordance with IEC 60947-3, lockable in OFF position.
- Breaking capacity sufficient for the currents of all loads and current of the largest motor in the blocked state.
- Main switch only as device for Emergency-stop if the disconnection of all loads does not lead to hazardous conditions.
- If necessary protect drives with undervoltage releases in order to prevent a hazardous automatic restart when the restart command is given.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with well-tried components and operating principles (EN ISO 13849-1 and EN ISO 13849-2).
- Bridging in the switch causes the loss of the safety function.

Function

The operation of the Emergency-stop switch Q1 disconnects the power supply of the entire installation. The undervoltage release at Q3 prevents a restart of the dangerous drive.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 1	Structure	SS A
MTTF _d	100 years	PFH _d	6.25×10^{-7}
B10 _d	Q1: 10000	B10	Q1: 2000
n _{op}	Q1: 360	λ_d/λ	Q1: 0.2
CCF	not relevant	C	Q1: 0.0625
DC _{avg}	not relevant	β	not relevant
PL	c	DC	not relevant
T10 _d	> 20 years	SIL	1

Safety-related switching devices



NZMB1-A63 circuit-breaker with NZM1-XTVDVR door coupling handle

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-3	Low-voltage switchgear and controlgear – Part 3: Switches, disconnectors, switch-disconnectors and fuse-combination units	–

Stopping in case of emergency

info@tm2a.pt

WWW.TM2A.PT

Stopping in case of emergency (Emergency-stop disconnection)

1.2 In the control circuit for simple drives

Application

- For simple drives in which the motor contactor is switched for operation.
- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

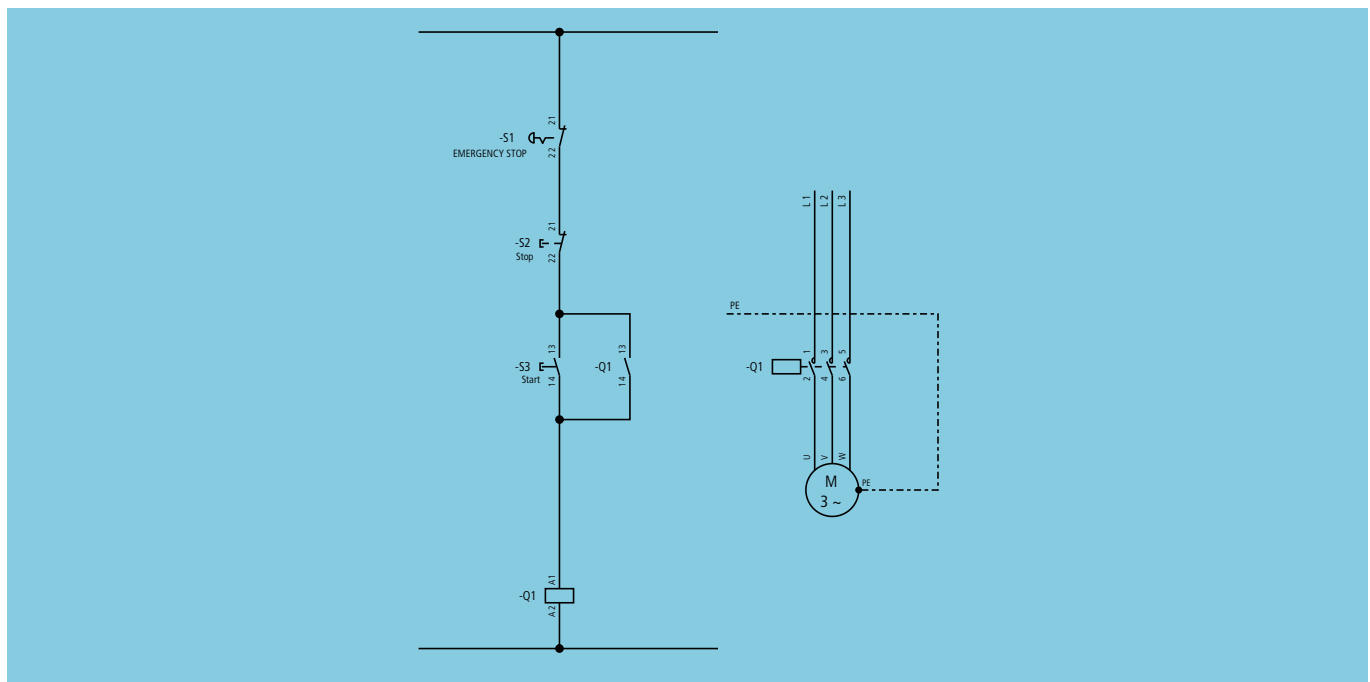


Figure 3: Emergency-stop disconnection of a self-maintained circuit

Requirements

- Use Emergency-stop actuators with positive opening to IEC 60947-5-1, Annex K, and function to EN ISO 13850.
- Hard wire with electromechanical components.
- Protect supply conductor.
- Emergency-stop function must be tested regularly.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with well-tried components and operating principles (EN ISO 13849-1 and EN ISO 13849-2).
- Bridging in the switch or the non drop-out of Q1 causes the loss of the safety function.
- Wire break causes immediate disconnection.

Function

The operation of the Emergency-stop actuator S1 de-energizes contactor Q1. Q1 disconnects the power supply (closed-circuit principle).



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Condition	EN ISO 13849-1	Condition	IEC 62061
Structure	Cat. 1	Structure	SS A
MTTF _d	100 years	PFH _d	1.59 x 10 ⁻⁷
B10 _d	S1: 100000, Q1: 1300000	B10	S1: 20000, Q1: 975000
n _{op}	S1: 360, Q1: 7200	λ _d /λ	S1: 0.2, Q1: 0.75
CCF	not relevant	C	S1: 0.0625, Q1: 1.25
DC _{avg}	not relevant	β	not relevant
PL	c	DC	not relevant
T10 _d	>20 years	SIL	1

Stopping in case of emergency

Safety-related switching devices



M22-PV/KC02/IY Emergency-stop actuator



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

info@tm2a.pt

WWW.TM2A.PT

Stopping in case of emergency (Emergency-stop disconnection)

1.3 For interrupting several control circuits with safety relay

Application

- For extensive control systems in which several circuits must be disconnected.
- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

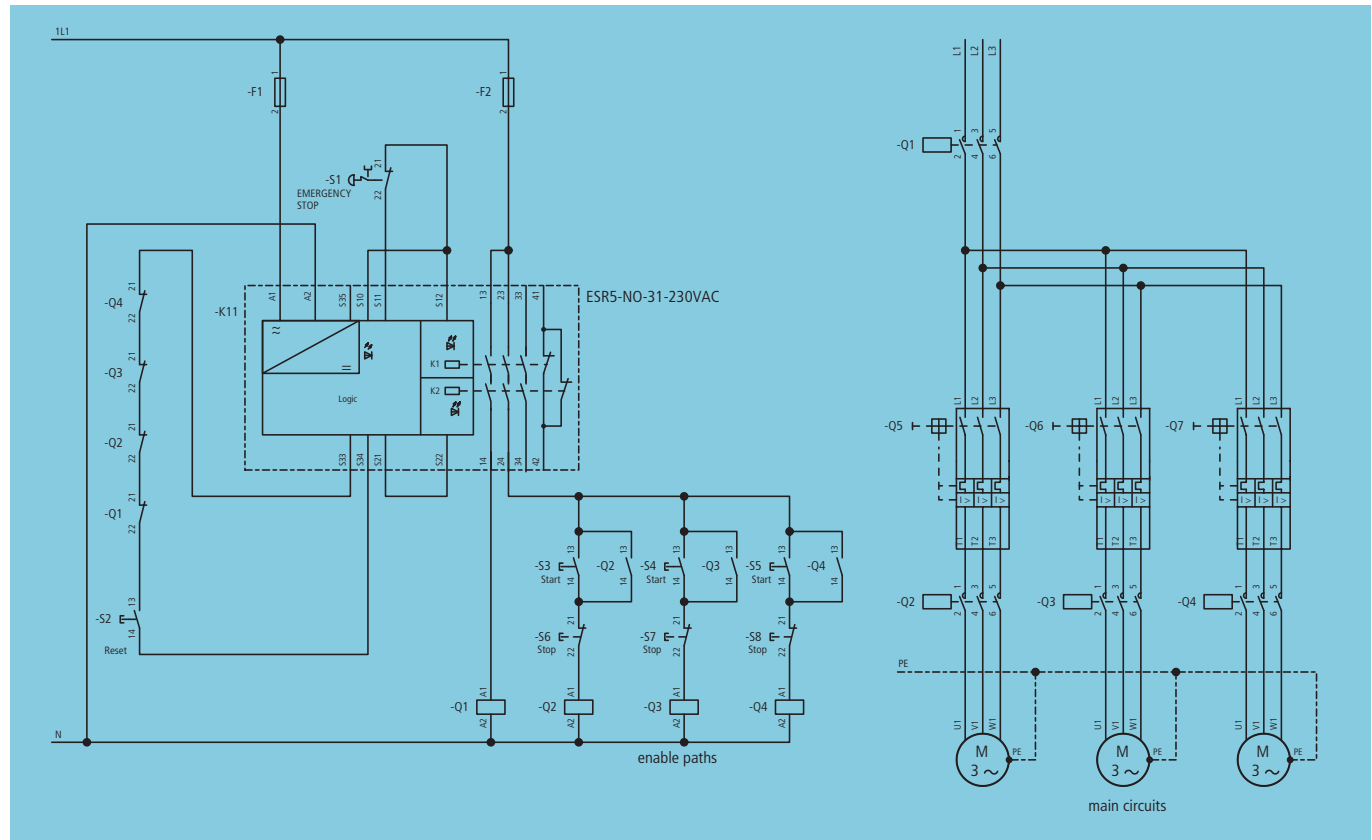


Figure 4: Single-channel emergency stop with ESR5

Requirements

- Emergency-stop actuators with positive opening (IEC 60947-5-1 Annex K) and function to EN ISO 13850.
- Use safety relays with mechanically linked contacts.
- Hard wire with electromechanical components.
- Install the emergency-stop actuator outside of the hazardous zone so that it is recognizable and accessible.
- Activate hazardous movements after enable with separate Start command (S3 to S5).
- Emergency-stop function must be tested regularly.
- Observe additional applicable standards, e.g. IEC 60204-1.

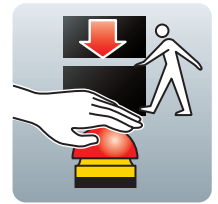
Properties

- Design with well-tried components and operating principles (EN ISO 13849-1 and EN ISO 13849-2).
- Monitoring of redundant contactors via feedback loop (K11).
- Bridging in the Emergency-stop actuator or supply conductor causes the loss of the safety function.

→ A higher safety integrity can be achieved by simple expansion to a redundant emergency-stop disconnection circuit,
→ chapter 1.5 „Two-channel with safety relay“, page 20



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

If the input voltage of 230 V AC is applied to A1 and A2, the Power LED indicates readiness to activate the enabling paths. When the RESET pushbutton S2 is actuated, the N/C contacts of the feedback circuit Q1 – Q4 check first of all that the contactors are in their rest position. If this state is present, the internal relays pick up with the rising edge, which is indicated via LEDs K1 and K2. The non-safety signal path (terminal 41-42) is opened and the enabling paths (terminal 13-14, 23-24 and 33-34) are closed.

The contactors Q2, Q3 and Q4 can be activated via the corresponding start command S3, S4, S5. The enable contactor Q1 is used for the redundant safe disconnection of the drives.

Condition	EN ISO 13849
Structure	Cat. 1
MTTF _d	100 years
B10 _d	S1: 100000, Q1-Q4: 1300000
n _{op}	S1, Q1: 1800, Q2-Q4: 7200
CCF	80
DC _{avg}	61.81 %
PL	c
T10 _d	>20 years

Condition	IEC 62061
Structure	SS A and SS D, asymmetrical
PFH _d	3.23×10^{-7}
B10	S1: 20000, Q1-Q4: 975000
λ_d/λ	S1: 0.2, Q1-Q4: 0.75
C	S1, Q1: 0.3125, Q2-Q4: 1.25
β	0.05
DC	S1: 0 %, K1: 99 %, Q1-Q4: 99 %
SIL	1

Safety-related switching devices



M22-PV/KC02/IY Emergency-stop actuator



Safety relays ESR5-NO-31-230VAC



DILM12 and DILM25 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

1.4 For interrupting several control circuits easySafety

Application

- For extensive control systems in which several circuits must be disconnected.
 - When danger can arise for the operator or the machine.
 - When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

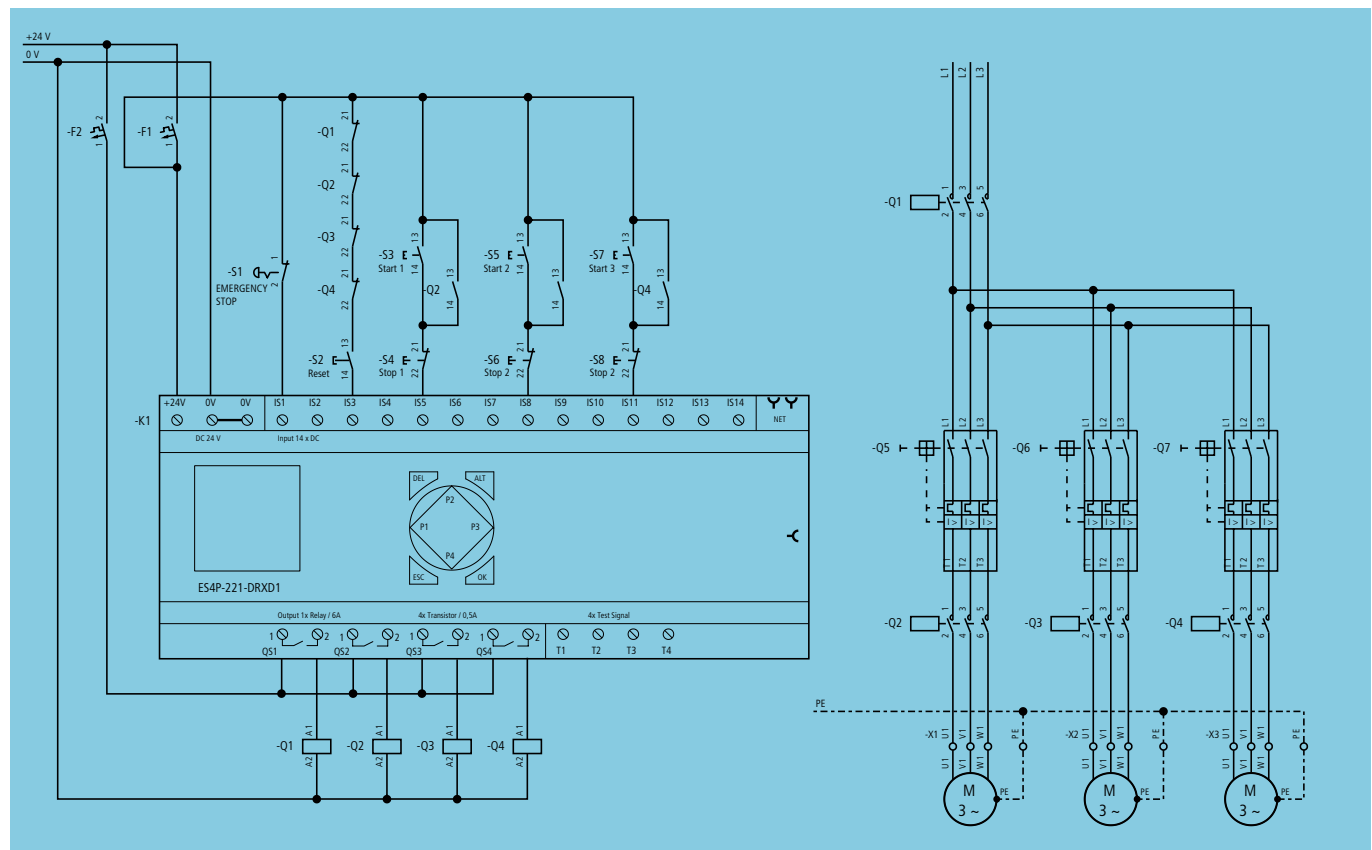


Figure 5: Single-channel Emergency-stop with **easySafety**

Requirements

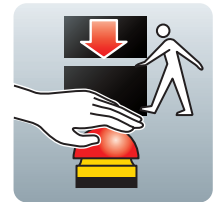
- Emergency-stop actuators with positive opening (IEC 60947-5-1 Annex K) and function to EN ISO 13850.
- Hard wire with electromechanical components.
- Install emergency-stop actuators in a visible position and not in the hazardous area.
- Activate hazardous movements after enable with separate Start command.
- Emergency-stop function must be tested regularly.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with well-tried components and operating principles (EN ISO 13849-1 and EN ISO 13849-2).
- Monitoring of redundant contactors via feedback loop (K1).
- Bridging in the Emergency-stop actuator or supply conductor causes the loss of the safety function.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

The Emergency-stop actuator S1 must be in the enable position (N/C contacts closed) so that the enable signal can be issued via the RESET pushbutton S2. Actuating the START pushbutton (S3, S5, S7) for the respective drive starts the hazardous movement. The self maintaining function and its interruption are implemented with additional mirror contacts of the enable contactors Q2 to Q4. The appropriate contactor drops out. Restarting is possible by actuating the START actuator. If

Emergency-stop actuator S1 is pressed during the hazardous movement, **easySafety** removes the enable from the outputs. Contactors Q1 - Q4 drop out. A restart is only possible after the Emergency-stop actuator and its enable are reset via by actuating the RESET pushbutton S2.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 1	Structure	SS A
MTTF _d	100 years	PFH _d	3.21 x 10 ⁻⁷
B10 _d	S1: 100000, Q1, Q4: 1300000	B10	S1: 20000, Q1-Q4: 975000
n _{op}	S1, Q1: 1800, Q2-Q4: 7200	λ _d /λ	S1: 0.2, Q1-Q4: 0.75
CCF	80	C	S1, Q1: 0.3125, Q2-Q4: 1.25
DC _{avg}	39.66 %	β	0.05
PL	c	DC	S1: 0 %, K1: 99 %, Q1-Q4: 99 %
T10 _d	>20 years	SIL	1

Safety-related switching devices



M22-PV/KC02/IY Emergency-stop actuator



easySafety ES4P-221-DRXD1 safety control relay



DILM12 and DILM25 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

Stopping in case of emergency (Emergency-stop disconnection)

1.5 Two-channel with safety relay

Application

- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- When danger can arise for the operator or the machine.

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

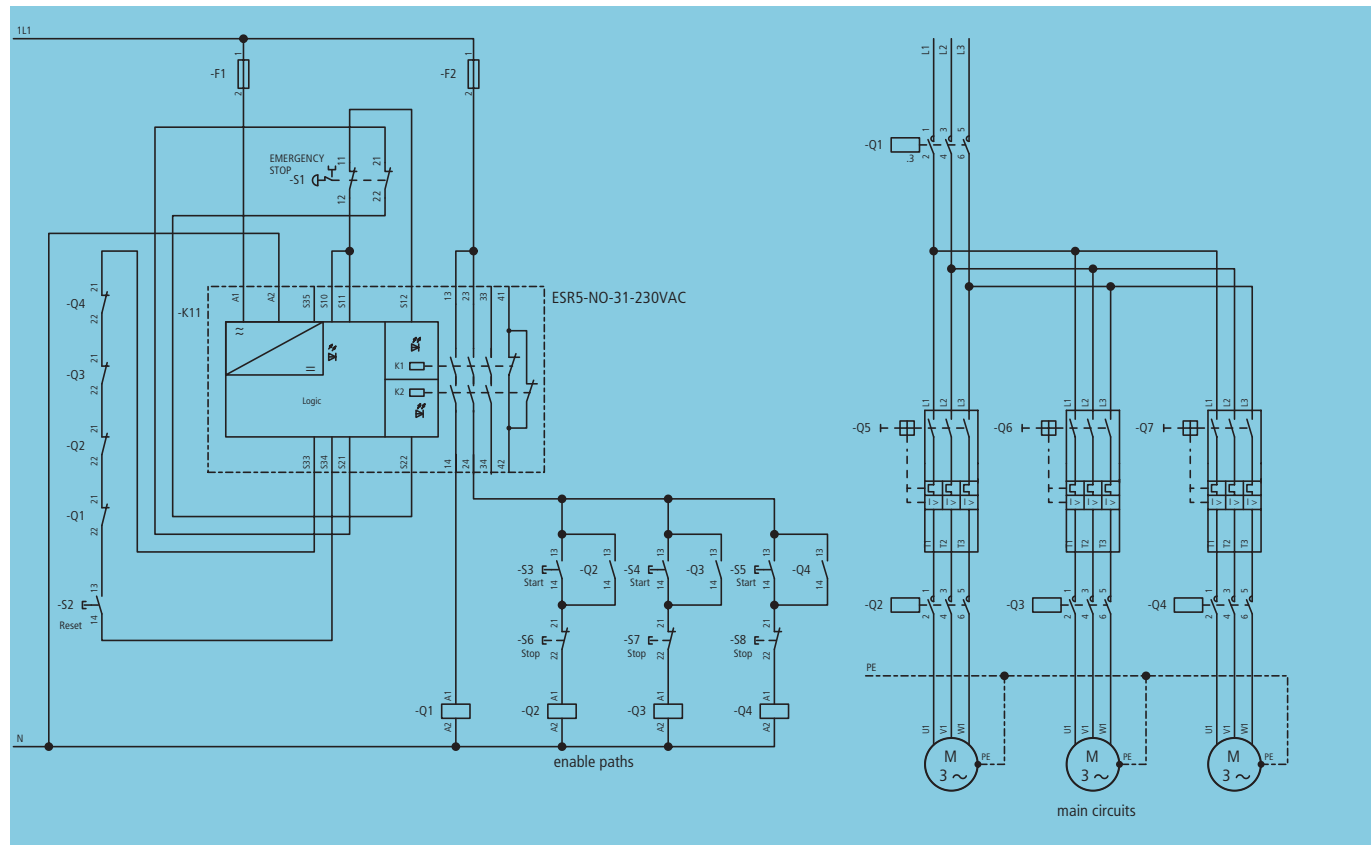


Figure 6: Two-channel emergency stop with ESR5

Requirements

- Emergency-stop actuator with positive opening to IEC 60947-5-1, Annex K, and wire function with two-channel circuit and with cross-circuit detection on ESR5 to EN ISO 13850.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Acknowledgement with reset required after releasing of Emergency-stop actuator.
- Activate hazardous movements after enable with separate Start command.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break, connection fault and cross circuit are detected immediately or with the next start command.
- Accumulation of undetected faults can not lead to the loss of the safety function.
- Increasing the enable paths with additional contacts possible (e.g. with ESR5-NE-51-24VAC-DC).



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

If the input voltage of 230 V AC is applied to A1 and A2, the Power LED indicates readiness to activate the enable paths. When the RESET pushbutton S2 is actuated, the N/C contacts of the feedback circuit Q1-Q4 check first of all that the contactors are in their rest position. If this state is present, the internal enable relays pick up with a rising edge, which is indicated via LEDs K1 and K2. The not safety related signalling path

(terminal 41-42) is opened and the enable paths (terminal 13-14, 23-24 and 33-34) are closed.

The contactors Q2, Q3 and Q4 can be activated via the corresponding start command S3, S4, S5. The enable contactor Q1 is used for central safe disconnection of the drives.

Condition	EN ISO 13849
Structure	Cat. 4
MTTF _d	100 years
B10 _d	S1: 100000, Q1-Q4: 1300000
n _{op}	S1, Q1: 1800, Q2-Q4: 18000
CCF	80
DC _{avg}	99 %
PL	e
T10 _d	>20 years

Condition	IEC 62061
Structure	SS D, asymmetrical
PFH _d	2.96×10^{-8}
B10	S1: 20000, Q1-Q4: 975000
λ_d/λ	S1: 0.2, Q1-Q4: 0.75
C	S1, Q1: 0.3125, Q2-Q4: 3.125
β	0.05
DC	S1: 99 %, K1: 99 %, Q1-Q4: 99 %
SIL	3

Safety-related switching devices



Emergency-stop actuator M22-PVT45P-MPI + M22-A + M22-CK02



Safety relays ESR5-NO-31-230VAC



DILM12 and DILM25 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

Stopping in case of emergency (Emergency-stop disconnection)

1.6 Two-channel with easySafety

Application

- When danger can arise for the operator or the machine.
- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850)

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

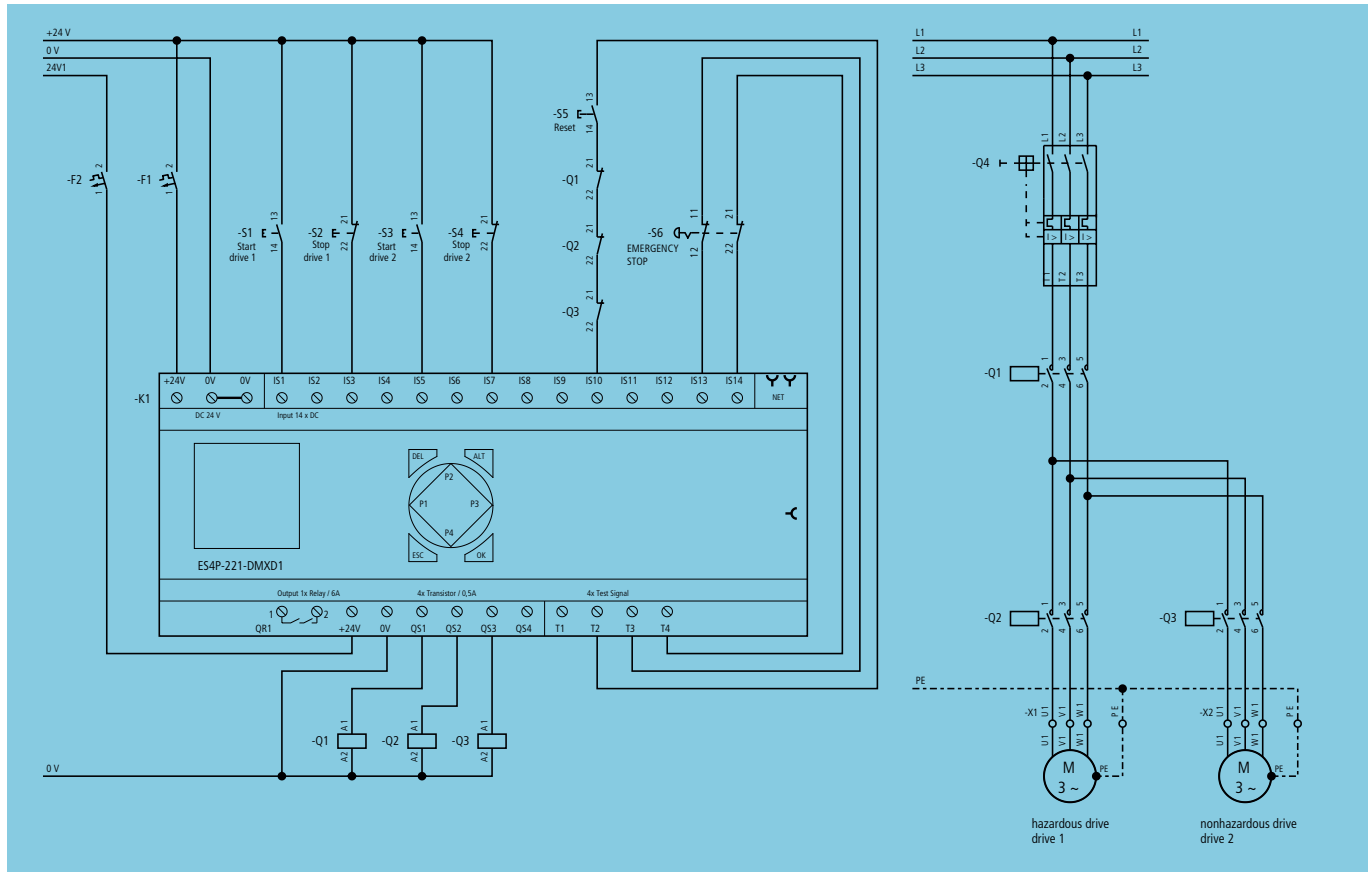


Figure 7: Two-channel Emergency-stop with easySafety

Requirements

- Emergency-stop actuator with positive opening to IEC 60947-5-1, Annex K, and wire function with two-channel circuit and with cross-circuit detection on easySafety to EN ISO 13850.
- Use inputs with different test signals.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Acknowledgement with reset required after releasing of Emergency-stop actuator.
- Activate hazardous movements after enable with separate Start command.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break, connection fault and cross circuit are detected immediately or with the next start command.
- Accumulation of undetected faults can not lead to the loss of the safety function.
- Increasing the enable paths with additional contacts possible (e.g. with ESR5-NE-51-24VAC-DC).



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

The Emergency-stop actuator S6 must be in the enable position (N/C contacts closed) so that the enable signal can be issued via the RESET pushbutton S5. Pressing the START pushbutton S1 starts the hazardous movement. The self-latching function and its interruption, triggered by the the STOP actuator S2, are implemented by the program. Contactor Q2 drops out. A restart is possible by pressing the START pushbutton.

If the hazardous movement is stopped by pressing the Emergency-stop actuator, the enable is removed from the outputs and the contactors Q1 - Q3 drop out. A restart is only possible after the Emergency-stop actuator is reset and enabled by pressing the RESET pushbutton.

Condition	EN ISO 13849
Structure	Cat. 4
MTTF _d	100 years
B10 _d	S6: 100000, Q1-Q3: 1300000
n _{op}	S6, Q1: 1800, Q2-Q3: 18000
CCF	80
DC _{avg}	99 %
PL	e
T10 _d	>20 years

Condition	IEC 62061
Structure	SS D, asymmetrical
PFH _d	2.28 x 10 ⁻⁸
B10	S6: 20000, Q1-Q3: 975000
λ _d /λ	S6: 0.2, Q1-Q3: 0.75
C	S6, Q1: 0.3125, Q2-Q3: 3.125
β	0.05
DC	S6: 99 %, K1: 99 %, Q1-Q3: 99 %
SIL	3

Safety-related switching devices



Emergency-stop actuator M22-PVT45P-MPI + M22-A + M22-CK02



easySafety ES4P-221-DMXD1 safety control relay



DILM12 and DILM25 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

Stopping in case of emergency (Emergency-stop disconnection)

1.7 With electronically controlled drives

Application

- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- When hazards may occur on machines with electronically controlled drives.

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

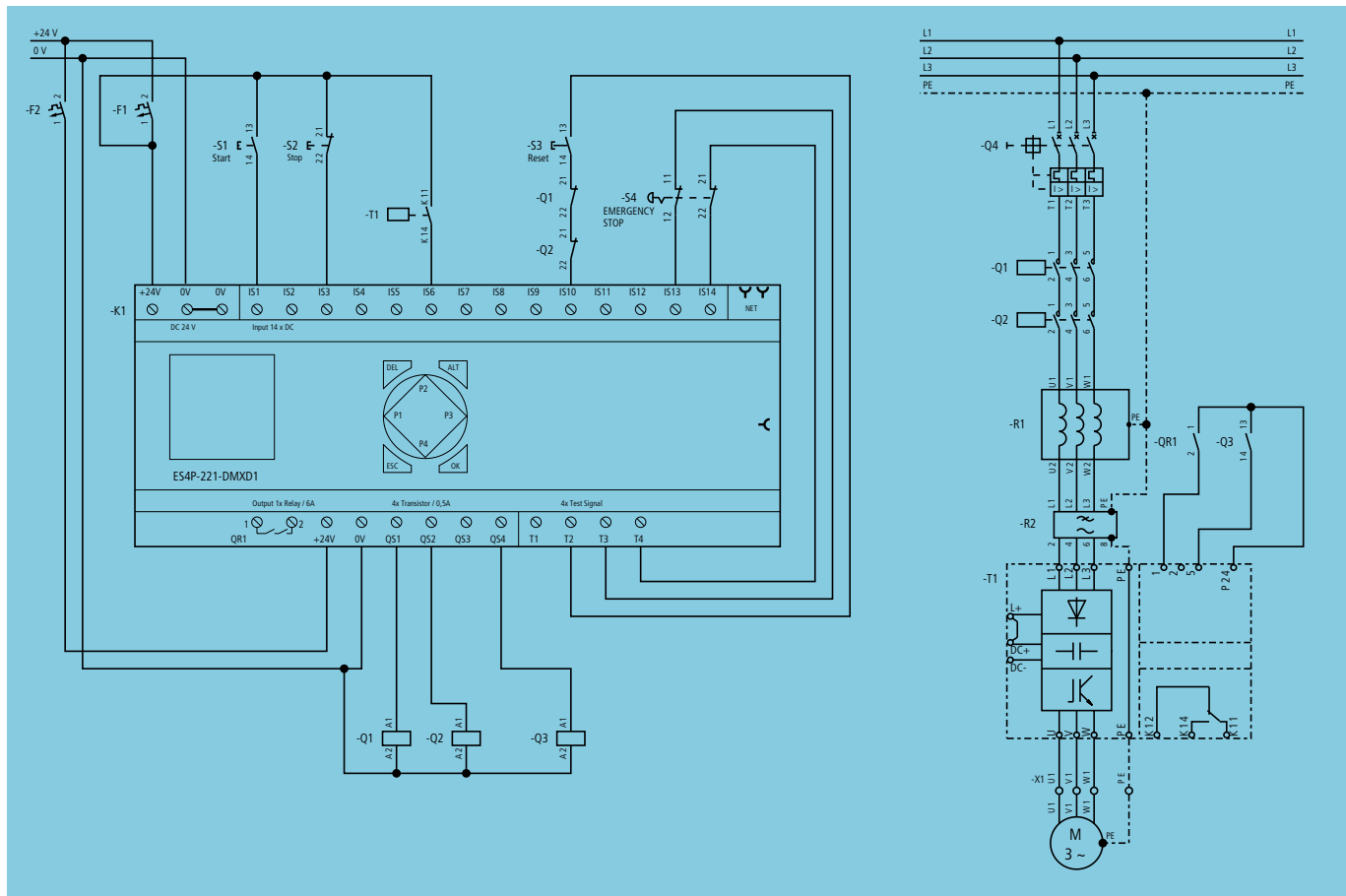


Figure 8: Emergency-stop with **easySafety** electronically controlled drive

Requirements

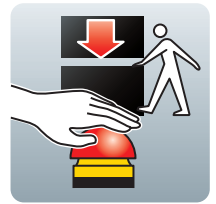
- Emergency-stop actuator with positive opening to IEC 60947-5-1, Annex K, and wire function with two-channel circuit and with cross-circuit detection on **easySafety** to EN ISO 13850.
- Use inputs with different test signals.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Acknowledgement with reset required after releasing of Emergency-stop actuator.
- Activate hazardous movements after enable with separate Start command.
- Separation of power supply from mains contactor.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break, connection fault and cross circuit are detected immediately or with the next start command.
- Accumulation of undetected faults can not lead to the loss of the safety function.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

The Emergency-stop actuator S4 must be in the enable position (N/C contacts closed) so that the enable signal can be issued via the RESET pushbutton S3. Pressing the START pushbutton S1 starts the hazardous movement. The self-latching function and its interruption are implemented in the program. The two contactors drop out, and a restart is possible by pressing the START actuator. If the hazardous movement is stopped by pressing the Emergency-stop actuator S4, the enable for outputs QS1 and

QS2 is removed and the contactors drop out. A restart is only possible after the Emergency-stop actuator is reset and enabled by pressing the RESET pushbutton.

The drive can be braked actively by using output QS4. However, this option is not included in the safety consideration since the frequency inverter does not support the safe braking operation.

Condition	EN ISO 13849
Structure	Cat. 4
MTTF _d	100 years
B10 _d	S4: 100000, Q1, Q2: 1300000
n _{op}	1800
CCF	80
DC _{avg}	99 %
PL	e
T10 _d	>20 years

Condition	IEC 62061
Structure	SS D, symmetrical
PFH _d	1.74×10^{-8}
B10	S4: 20000, Q1, Q2: 975000
λ_d/λ	S4: 0.2, Q1-Q2: 0.75
C	0.3125
β	0.05
DC	S4: 99 %, K1: 99 %, Q1-Q2: 99 %
SIL	3

Safety-related switching devices



FAK foot and palm switch



easySafety ES4P-221-DMXD1 safety control relay



DILM12 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111

Stopping in case of emergency (Emergency-stop disconnection)

1.8 Two-channel configuration with variable frequency drive using STO

Application

- The STO function can be used anywhere where the corresponding motor will come to a stop by itself in a sufficiently short amount of time (PST) as a result of the corresponding load torque or friction, as well as in cases in which coasting has no safety implications. (Stop category 0)
 - When hazards may occur on machines with electronically controlled drives.
- The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

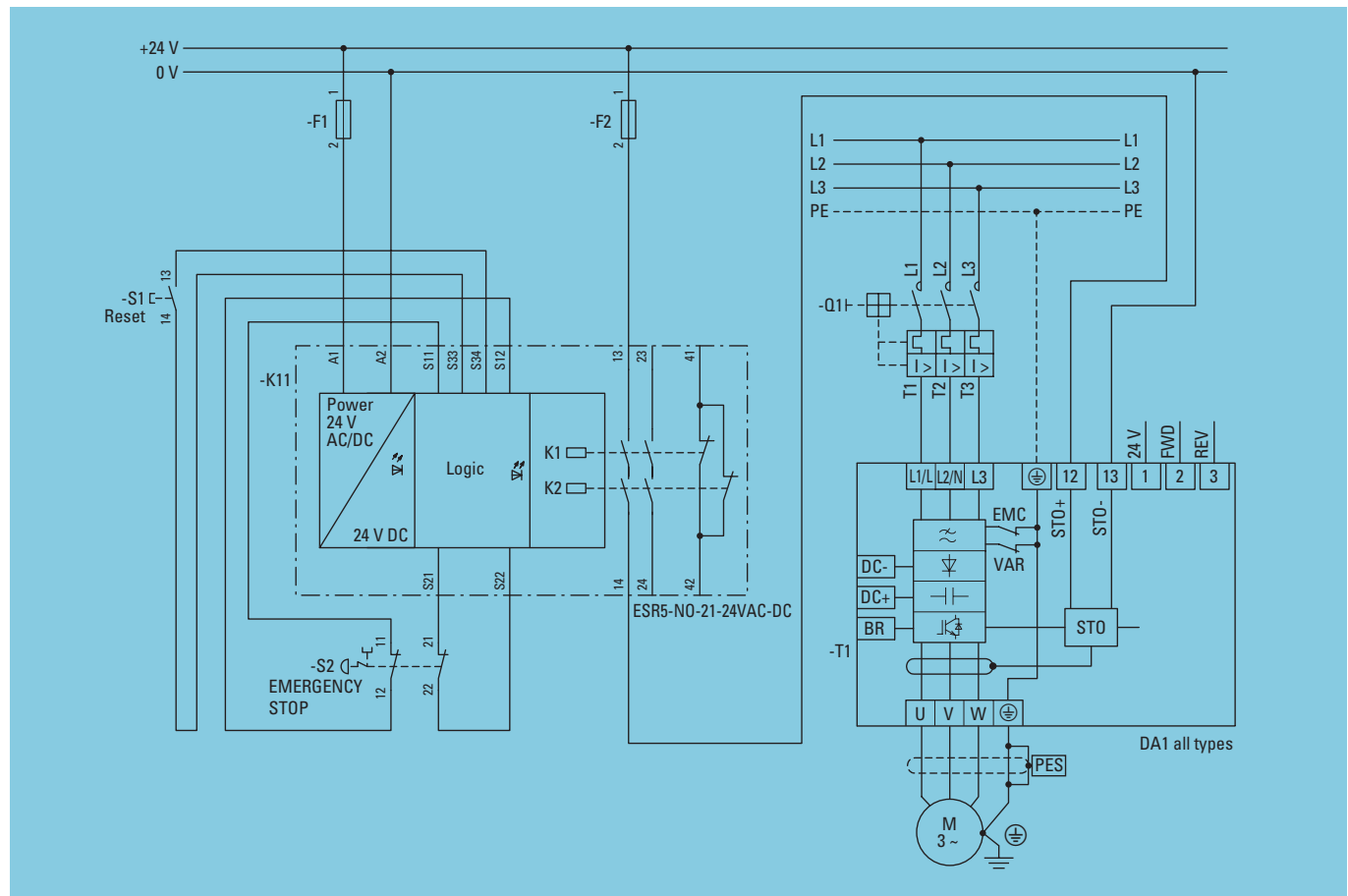


Figure 9: Two-channel emergency stop using STO on DA1 with ESR5 safety relay

Requirements

- Emergency-stop buttons with positive opening (IEC 60947-5-1 Annex K) and function to EN 13850.
- Use safety relays with positive opening contacts.
- Install emergency-stop actuators in a visible position and not in the hazardous area.
- Activate hazardous movements after enable with separate Reset.
- Only use variable frequency drives that achieve at least PL d or SIL 2 for STO.
- Emergency-stop function must be tested regularly.
- Observe additional applicable standards, e.g. IEC 60204-1.
- Fault exclusion for the STO supply cables.
- The supply cable connected to 12 (STO+) and 13 (STO-) must be twisted and screened.
- Route the supply cable in a closed cable duct.
- Ground the screen braid (PES).

Properties

- Design with well-ried components and operating principles (EN ISO 13849-1 and EN ISO 13849-2).
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- In this example, the STO function is controlled using an external power supply. Alternatively, the 24 V supply from the variable frequency drive can also be used.

- The STO function is always activated and enabled in DA1 variable frequency drives - regardless of the operating mode or of parameter changes made by the user.
- Further information on the DA1 variable frequency drive is provided in the manual MN04020005Z



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

If the ESR5 is being powered through terminals A1 and A2, the enable path can be activated by pressing the RESET button. When -K1 and -K2 in the safety relay are energized, a voltage will be applied to the STO input and the safety enable signal for starting will be activated. The functional start command and the desired operating direction (if any) will be provided to terminals REV and FWD through the variable frequency drive's circuitry.

Activating an emergency stop will result in the safety relay's outputs being switched off, which in turn will result in the voltage at the variable frequency drive's STO input being removed. After a max. of 1 ms, the outputs in the power section (U, V, W) will be in a state in which no more torque is produced in the motor (STO function activated). The time it takes for the motor to coast to a stop will depend on the mechanical system's inertia and frictional forces.

If there is a short circuit or the supply voltage drops out, this will also result in a safe state, as the 24 V at the STO input will drop out as well.

Condition	EN ISO 13849
Structure	Cat. 3
MTTF _d	80 years
B10 _d	S2: 100000
n _{op}	S2: 1800
CCF	80
DC _{avg}	99 %
PL	d
T10 _d	>20 years

Condition	IEC 62061
Structure	SS B
PFH _d	1.82 x 10 ⁻⁸
B10	S2: 20000
λ _d /λ	S2: 0.2
C	S2: 0.0625
β	0.05
DC	99 %
SIL	2

Safety-related switching devices



M22-PV/KC02/IY Emergency-stop actuator



Safety relays ESR5-NO-21-24 V AC DC



Variable frequency drive DA 1

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111

Stopping in case of emergency (Emergency-stop disconnection)

1.9 With SmartWire-DT

Application

- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- When hazards may occur on machines fitted with SmartWire-DT.
→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

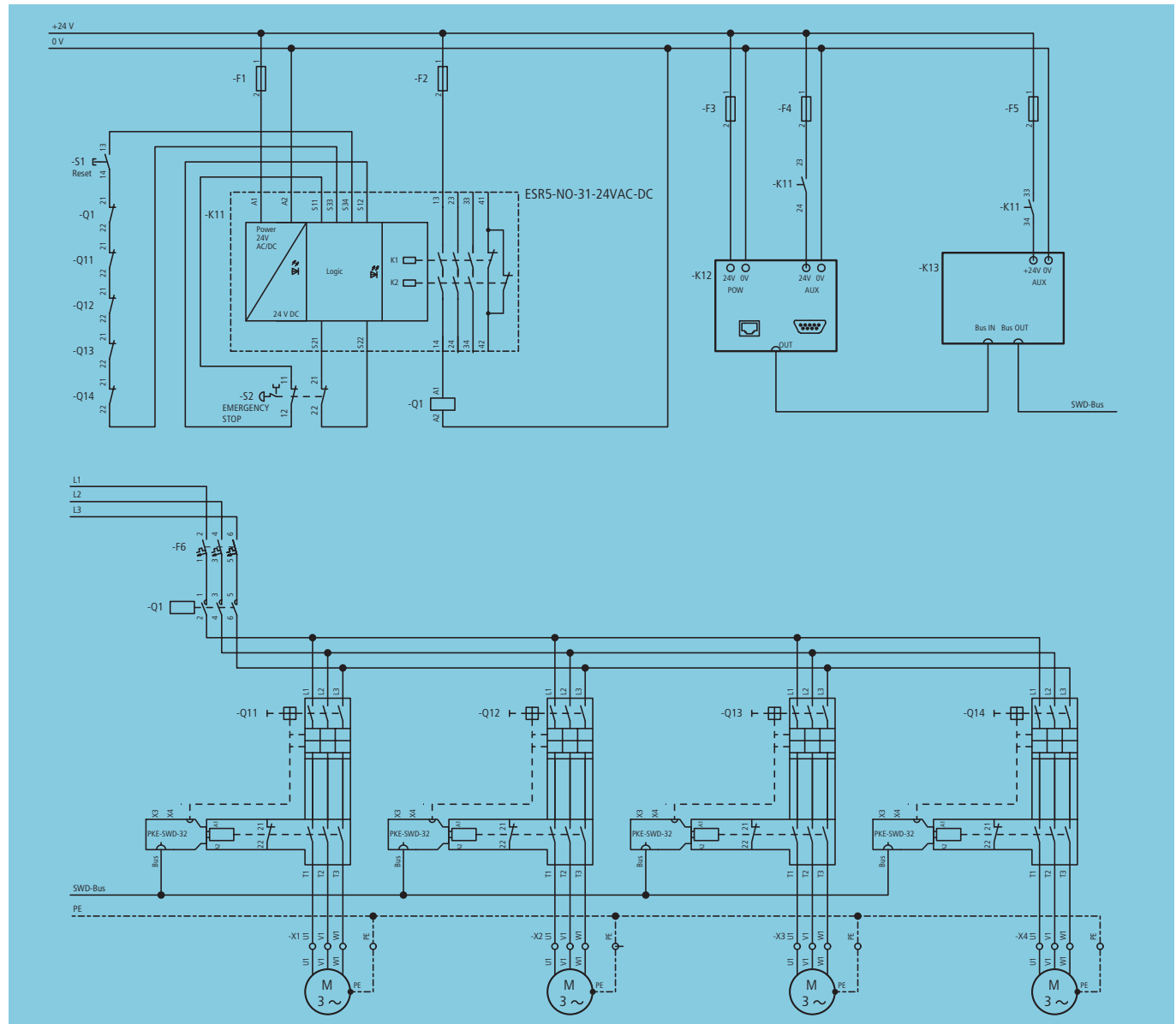


Figure 10: Emergency stop disconnection of a machine networked with SmartWire-DT

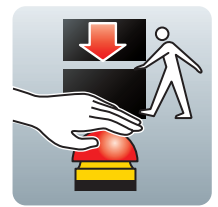
- The SmartWire-DT devices EU5C-SWD-... (K12 and K13) and PKE-SWD-... (Q11 - Q14) are not relevant for the safety consideration. The possibility of the power supply of the SmartWire-DT system accidentally switching on the connected contactors and preventing the disconnection of the connected contactors can be excluded. This fault exclusion also applies to all other SWD slaves EU5E-SWD-..., M22-SWD-..., DIL-SWD-... and NZM-SWD-...

Requirements

- Emergency-stop actuator with positive opening to IEC 60947-5-1, Annex K, and wire function with two-channel circuit and with cross-circuit detection on easySafety to EN ISO 13850.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Acknowledgement with reset required after releasing of Emergency-stop actuator.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



- Two-channel power supply via shutdown stages Q1 and Q11 - Q14.
- Activate hazardous movements after enable with separate Start command.
- SmartWire-DT network must be parameterized so that the disconnection is detected.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tries safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break, connection fault and cross-circuit in supply conductor and safety relay are detected immediately or with the next start command.
- Category 3 system behavior allows the accumulation of undetected faults to lead to the loss of the safety function.

Condition	EN ISO 13849
Structure	Cat. 3
MTTF _d	65.23 years
B10 _d	S2: 100000, Q1 und Q11-Q14: 1300000
η_{op}	S2, Q1: 1800, Q11-Q14: 7200
CCF	80
DC _{avg}	99 %
PL	d
T10 _d	K4: 7.5 years, all others: >20 years

Function

If the input voltage of 24 V AC is applied to A1 and A2, the Power LED indicates readiness to activate the enable paths. When the RESET pushbutton S1 is actuated, the N/C contacts of the feedback circuit Q1 and Q11-Q14 check first of all that the contactors are in their rest position. If this state is present, the internal enable relays pick up with a rising edge, which is indicated via LEDs K1 and K2.

The not safety related signalling path (terminal 41-42) is opened and the enable paths (terminal 13-14, 23-24 and 33-34) are closed. The start commands of a higher-level control system can then be applied via motor contactors Q11 to Q14. If the emergency-stop actuator is pressed, the higher-level contactor Q1 and the AUX power supply of the SmartWire-DT modules is disconnected. The individual motor contactors Q11-Q14 thus disconnect their respective drive in addition to contactor Q1.

Condition	IEC 62061
Structure	SS D symmetrical and asymmetrical
PfH _d	2.07×10^{-8}
B10	S2: 20000, Q1 und Q11-Q14: 975000
λ_d/λ	S2: 0.2, Q1, Q11-Q14: 0.75
C	S2, Q1: 0.3125, Q11-Q14: 1.25
β	0.05
DC	S2: 99%, K4: 99%, Q1, Q11-Q14: 99%
SIL	2

Safety-related switching devices



M22-PV/KC02/IY Emergency-stop actuator



ESR5-NO-31-24VAC-DC



DILM12 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–

Stopping in case of emergency (Emergency-stop disconnection)

1.10 With CMD contactor monitoring relay

Application

- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- When danger can arise for the operator or the machine.

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

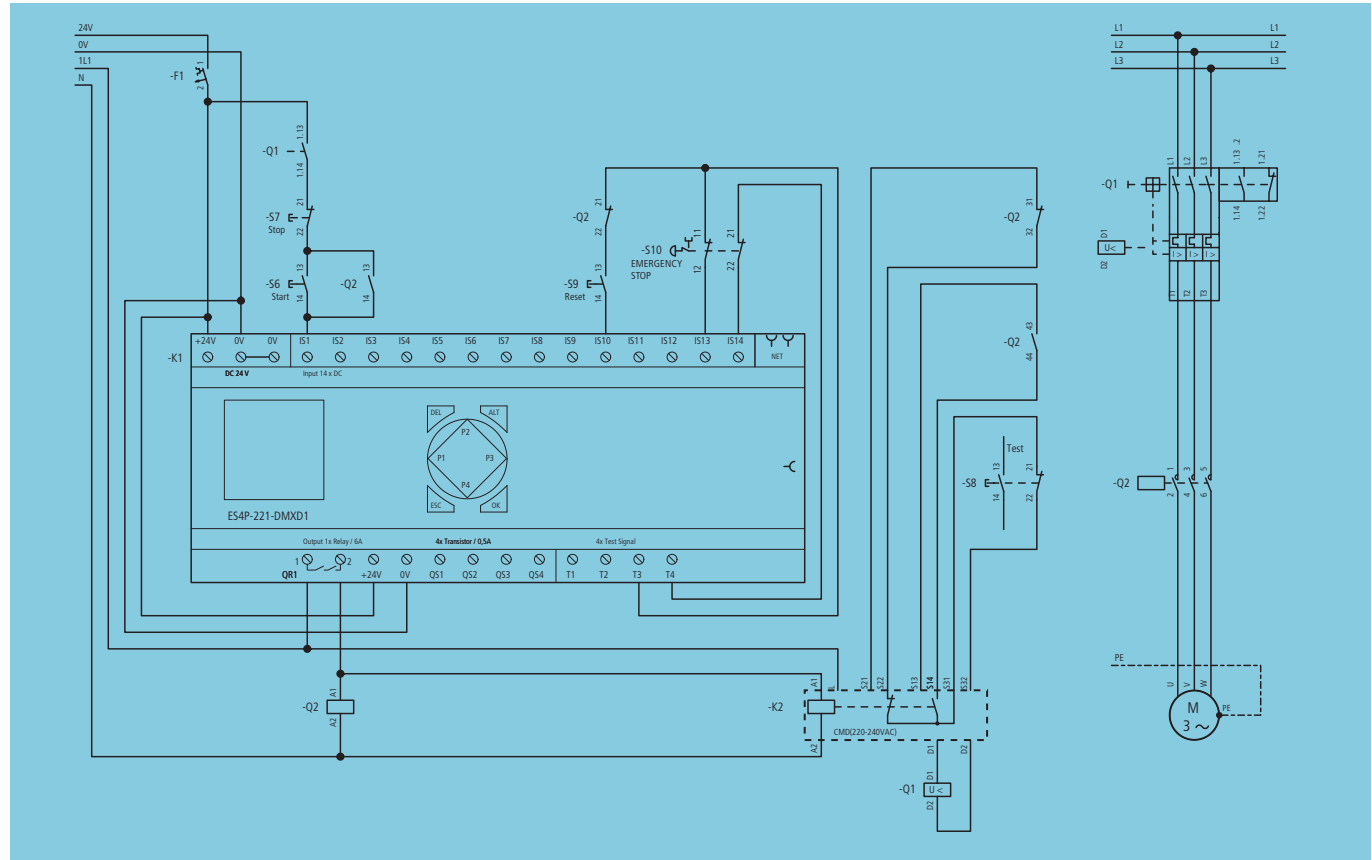


Figure 11: Emergency-stop with **easySafety** and CMD contactor monitoring device

Requirements

- Use Emergency-stop actuators with positive opening to IEC 60947-5-1, Annex K, and function to EN ISO 13850.
- Wire emergency-stop to **easySafety** in a two-channel circuit and with cross-circuit detection.
- Use inputs with different test signals.
- Contactor with mechanically linked feedback contact element and with additional auxiliary N/O contact.
- Combine motor-protective circuit-breaker with undervoltage release.
- Hard wire with electromechanical components.
- Acknowledgement with reset required after releasing of Emergency-stop actuator.
- Activate hazardous movements after enable with separate Start command.
- The function of the undervoltage release must be tested manually at regular intervals.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break, connection fault and cross circuit are detected immediately or with the next start command.
- Category 3 system behavior allows the accumulation of undetected faults to lead to the loss of the safety function.

→ Further information on the CMD contactor monitoring device is provided in the manual MN04913001Z-EN.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

In the event of a hazard the upstream **easySafety** switches off the contactor Q1 via the enable contact QR1. The CMD contactor monitoring relay compares the control voltage of the contactor with the status of the main contacts. The status of the main contacts of the contactor is monitored via an auxiliary N/C contact that acts as a mirror contact in accordance with IEC/EN 60947-4-1 Annex F. If the contactor is welded, the status of the main contacts does not correspond to the status of the control voltage. The undervoltage release of the backup circuit-breaker

Q1 is disconnected via an internal relay in the CMD. This disconnects the outgoer. The undervoltage release prevents the welded contactor from being switched on again. If the contacts of the circuit-breakers are welded, this cannot be determined until the main and auxiliary contacts have been disconnected and scanned. In this case the load can still be disconnected via Q2.

Condition	EN ISO 13849
Structure	Cat. 3
MTTF _d	67.59 years
B10 _d	S1: 100000, Q1: 1300000, Q2: 10000
n _{op}	S1: 1800, Q1: 5400, Q2: 500
CCF	80
DC _{avg}	83.88 %
PL	d
T10 _d	> 20 years

Condition	IEC 62061
Structure	SS D, asymmetrical
PFH _d	7.55×10^{-8}
B10	S1: 20000, Q1: 975000, Q2: 7500
λ_d/λ	S1: 0.2, Q1-Q2: 0.75
C	S1: 0.3125, Q1: 0.9375, Q2: 0.087
β	0.05
DC	S1: 99 %, K1: 90 %, K2: 99 %, Q1: 99 %, Q2: 60 %
SIL	2

Safety-related switching devices



Emergency-stop actuator
M22-PVT45P-MPI + M22-A +
M22-CK02



easySafety ES4P-221-DMXD1
safety control relay



DILM150 contactor



CMD contactor
monitoring device



NZM 1
circuit-breaker

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

Stopping in case of emergency (Emergency-stop disconnection)

1.1.1 Single-channel with EMS electronic motor starter

Application

- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- When danger can arise for the operator or the machine.

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

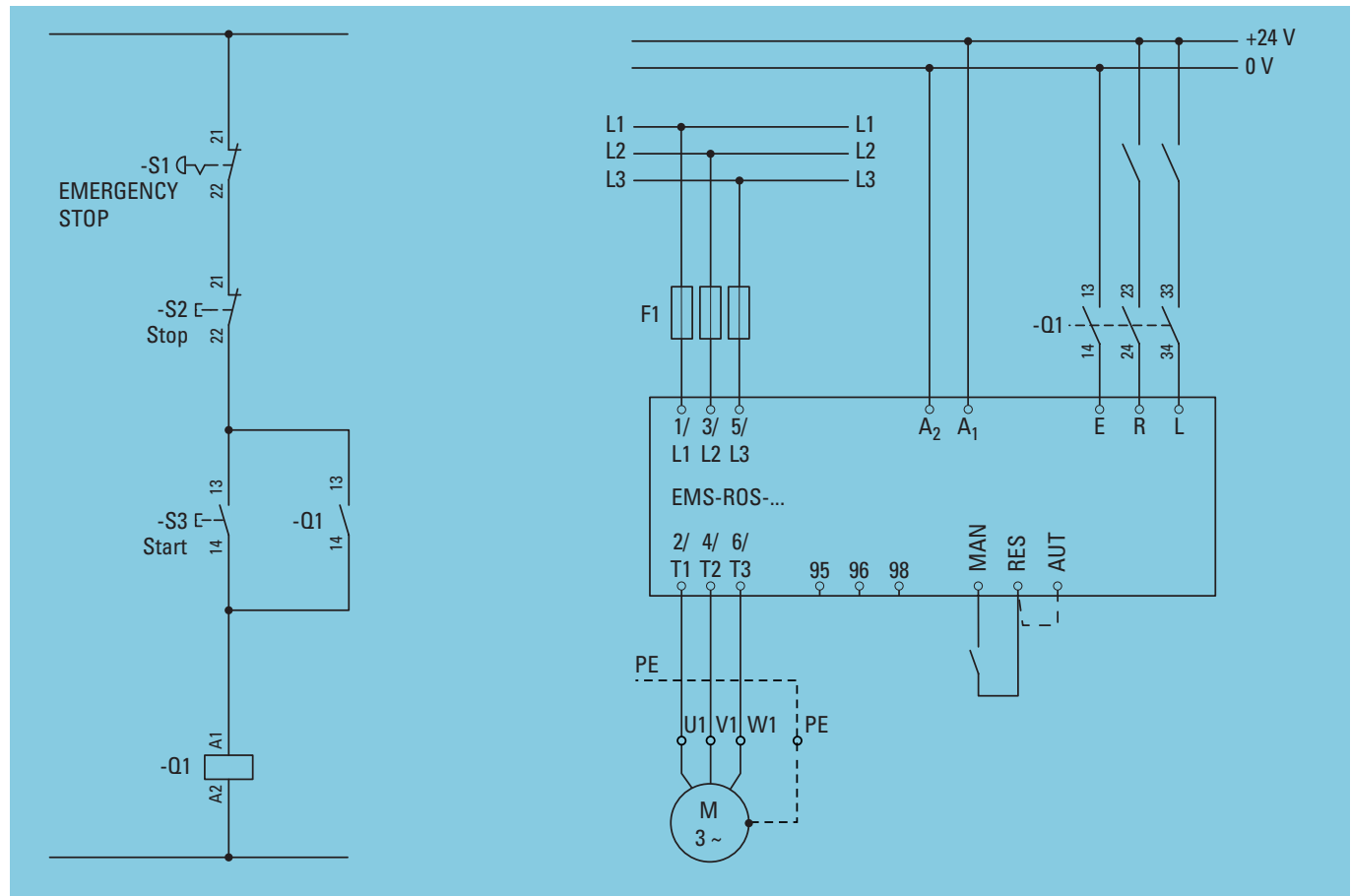


Figure 12: Emergency stop with EMS electronic motor starter

Requirements

- Emergency-stop actuators with positive opening (IEC 60947-5-1 Annex K) and function to EN ISO 13850.
- Hard wire with electromechanical components.
- Install emergency-stop buttons in a visible position and not in the hazardous area.
- Activate hazardous movements after enable with separate Start command.
- Emergency-stop function must be tested regularly.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with well-tries components and operating principles (EN ISO 13849-1 and EN ISO 13849-2).
- Bridging in the switch or the non drop-out of Q1 causes the loss of the safety function.

→ Further information on the EMS electronic motor starter is provided in the manual MN03407009Z-DE/EN.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

The operation of the Emergency-stop actuator S1 de-energizes contactor Q1. Q1 switches the EMS' control section off.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 1	Structure	SS A
MTTF _d	164 years	PFH _d	8.08×10^{-8}
B10 _d	S1: 100000 Q1:400000	B10	S1: 20000, Q1: 300000
n _{op}	360	λ_d/λ	S1: 0.2, Q1:0.75
CCF	not relevant	C	0.625
DC _{avg}	not relevant	β	not relevant
PL	c	DC	not relevant
T10 _d	>20 years	SIL	1

Safety-related switching devices



M22-PV/KC02/IY Emergency-stop actuator



DIL A contactor



Electronic motor starter EMS-ROS...

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	96
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	97
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	101
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

Stopping in case of emergency (Emergency-stop disconnection)

1.12 Two-channel configuration with EMS electronic motor starter, safety shutdown

Application

- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- When danger can arise for the operator or the machine.

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

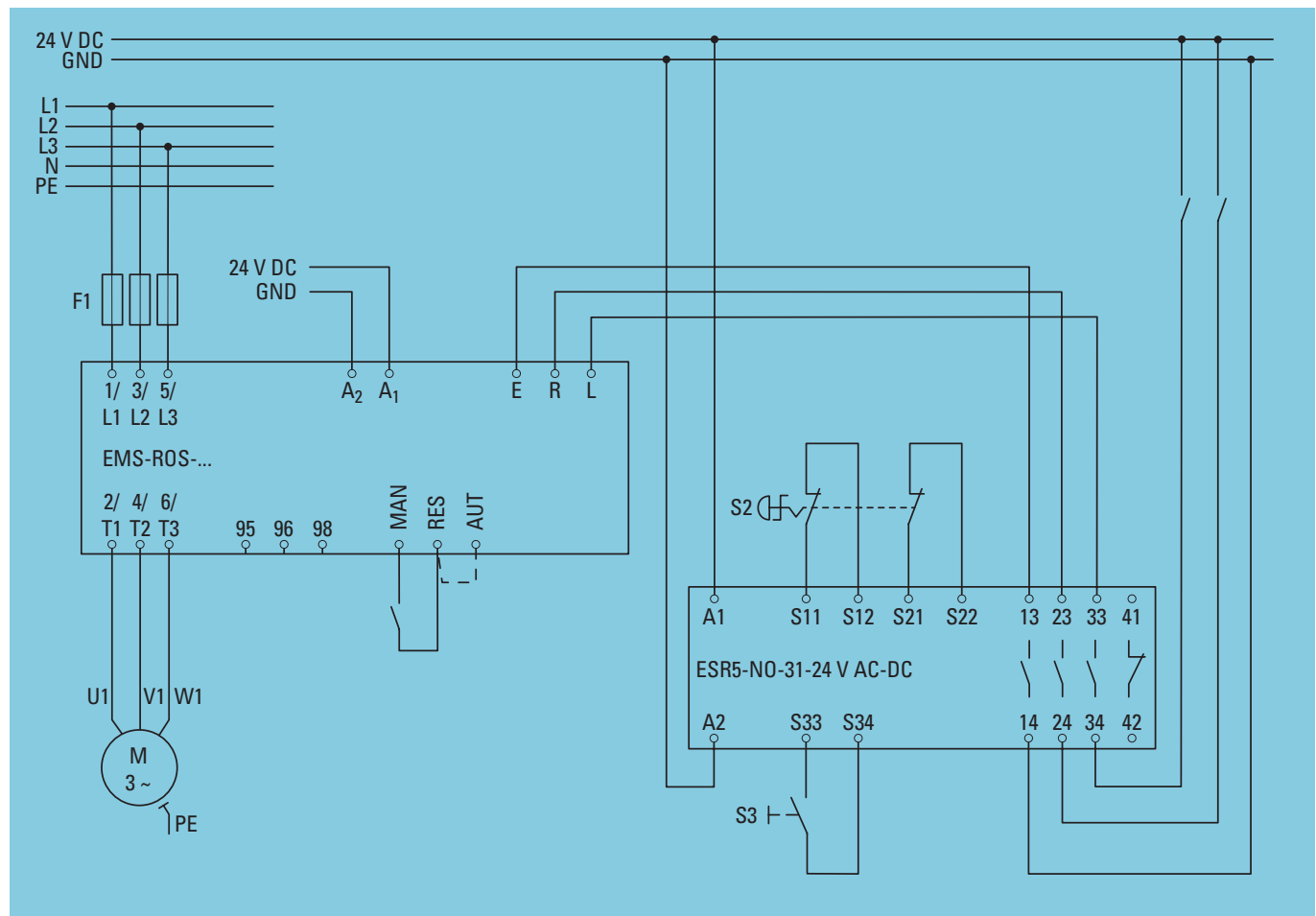


Figure 13: Emergency stop with EMS electronic motor starter and safety relay

Requirements

- Emergency-stop actuators with positive opening (IEC 60947-5-1 Annex K) and function to EN ISO 13850.
- Hard wire with electromechanical components.
- Install emergency-stop buttons in a visible position and not in the hazardous area.
- Activate hazardous movements after enable with separate Start command.
- Emergency-stop function must be tested regularly.
- Observe additional applicable standards, e.g. IEC 60204.

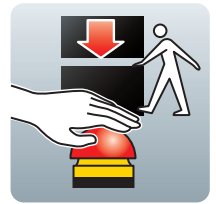
Properties

- Design with well-tried components and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.

→ Further information on the EMS electronic motor starter is provided in the manual MN03407009Z-DE/EN.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

In applications in which a safety shutdown is a normal operating state, the supply voltage is not switched - instead, the actuating circuit is switched. In this particular case, a dual-channel application has been implemented. Accordingly, the input wiring for controlling clockwise and counterclockwise operation, as well as the corresponding ground cable, is routed through the safety relay as well.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 3	Structure	SS B
MTTF _d	68.5 years	PFH _d	3.16×10^{-7}
B10 _d	S2: 100000	B10	S2: 20000
n _{op}	S2: 1800	λ _d /λ	S2: 0.2
CCF	80	C	S2: 0.3125
DC _{avg}	99 %	β	0.05
PL	e	DC	99 %
T10 _d	> 20 years	SIL	3

Safety-related switching devices



M22-PV/KC02/IY Emergency-stop actuator



Safety relays ESR5-NO-21-24 V AC DC



Electronic motor starter EMS-ROS...

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

2 Monitoring a movable guard

2.1 Single-channel with safety relay

Application

- For occasional interventions in the hazardous area and possible prevention of the hazard under certain conditions or when the hazard potential is low.
- If the stopping time is less than the entry and access time.

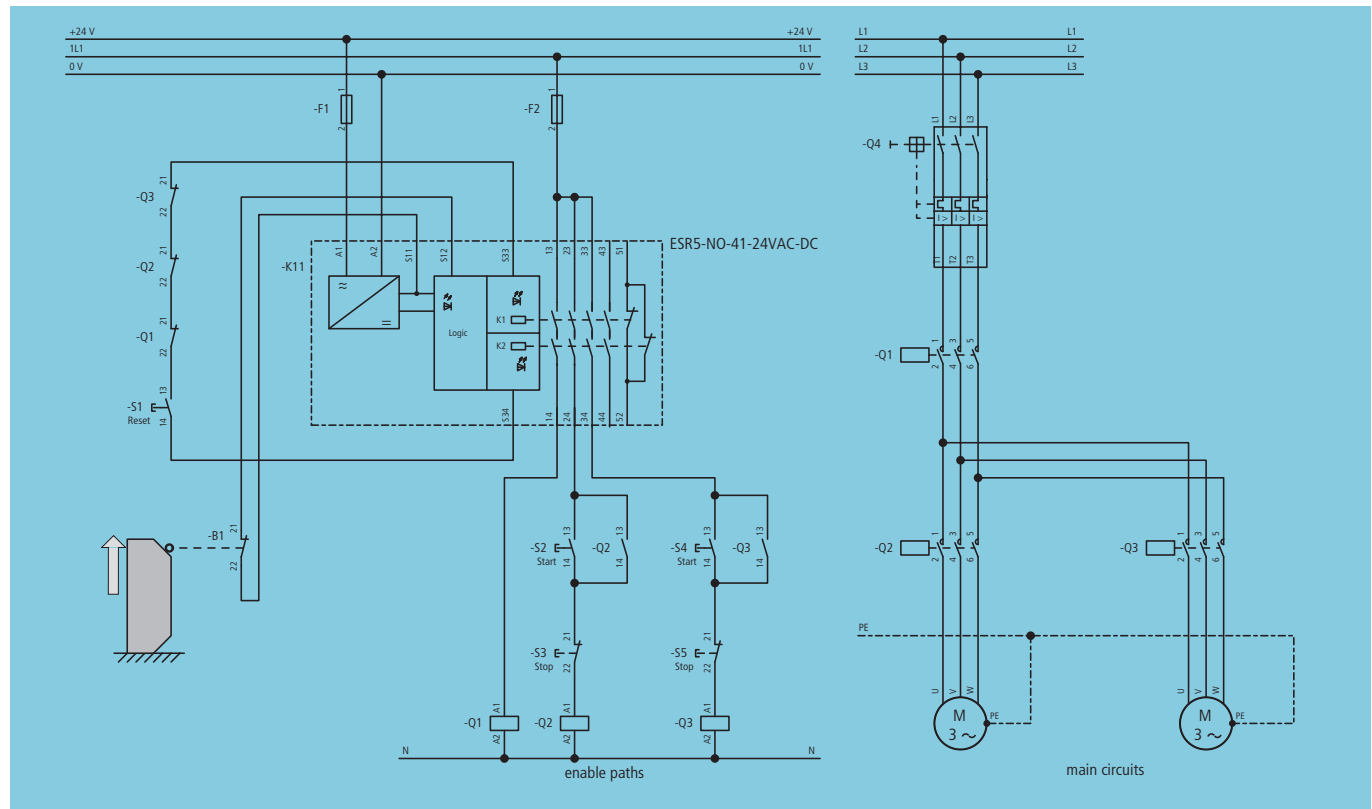


Figure 14: Single-channel guard door monitoring with ESR5

Requirements

- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Use safety relays with mechanically linked contacts.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Protect position switch and supply conductor from mechanical stresses.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- Observe additional applicable standards, e.g. IEC 60204-1.

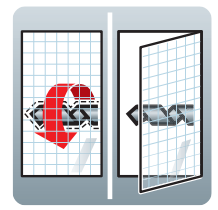
Properties

- Design with well-tried components and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Monitoring of redundant contactors via feedback loop.
- Connection fault in position switch or supply conductor as well as mechanical failure of the position switch causes loss of the safety function.

➔ A higher safety integrity can be achieved by simple expansion to a redundant guard door monitoring.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

After the supply voltage is applied to the safety relay (terminal A1-A2), the Power LED indicates readiness for activation of the enable paths. When the Reset pushbutton S1 is actuated, the N/C contacts of the feedback loop Q1 - Q3 check first of all that the contactors are in their rest position. If this state is present, the internal enable relays pick up with a rising edge, which is indicated via LEDs K1 and K2. The not safety-related signal path (terminal 51-52) is opened and the enable paths (terminal 13-14, 23-24, 33-34 and 43-44) are closed. The contactors Q2

and Q3 can now be activated via the corresponding start command S2 and S4. The enable contactor Q1 is used for the safety disconnection of both drives.

Condition	EN ISO 13849
Structure	Cat. 1
MTTF _d	100 years
B10 _d	B1: 20000000, Q1-Q3: 1300000
n _{op}	B1, Q1: 12960, Q2-Q3: 6500
CCF	80
DC _{avg}	90.79 %
PL	c
T10 _d	K1: 10 years, all others: > 20 years

Condition	IEC 62061
Structure	SS A
PFH _d	5.24 x 10 ⁻⁸
B10	B1: 4000000, Q1-Q3: 975000
λ _d /λ	B1: 0.2, Q1-Q3: 0.75
C	B1, Q1: 2.25, Q2-Q3: 11.285
β	0.05
DC	B1: 0 %, K1: 90 %, Q1-Q3: 99 %
SIL	1

Safety-related switching devices



LS-11 position switch (1 N/O, 1 N/C)



Safety relays ESR5-NO-41-24VAC-DC



DILM12 and DILM25 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.2 Single-channel with easySafety

Application

- For occasional interventions in the hazardous area and possible prevention of the hazard under certain conditions or when the hazard potential is low.
- If the stopping time is less than the entry and access time.

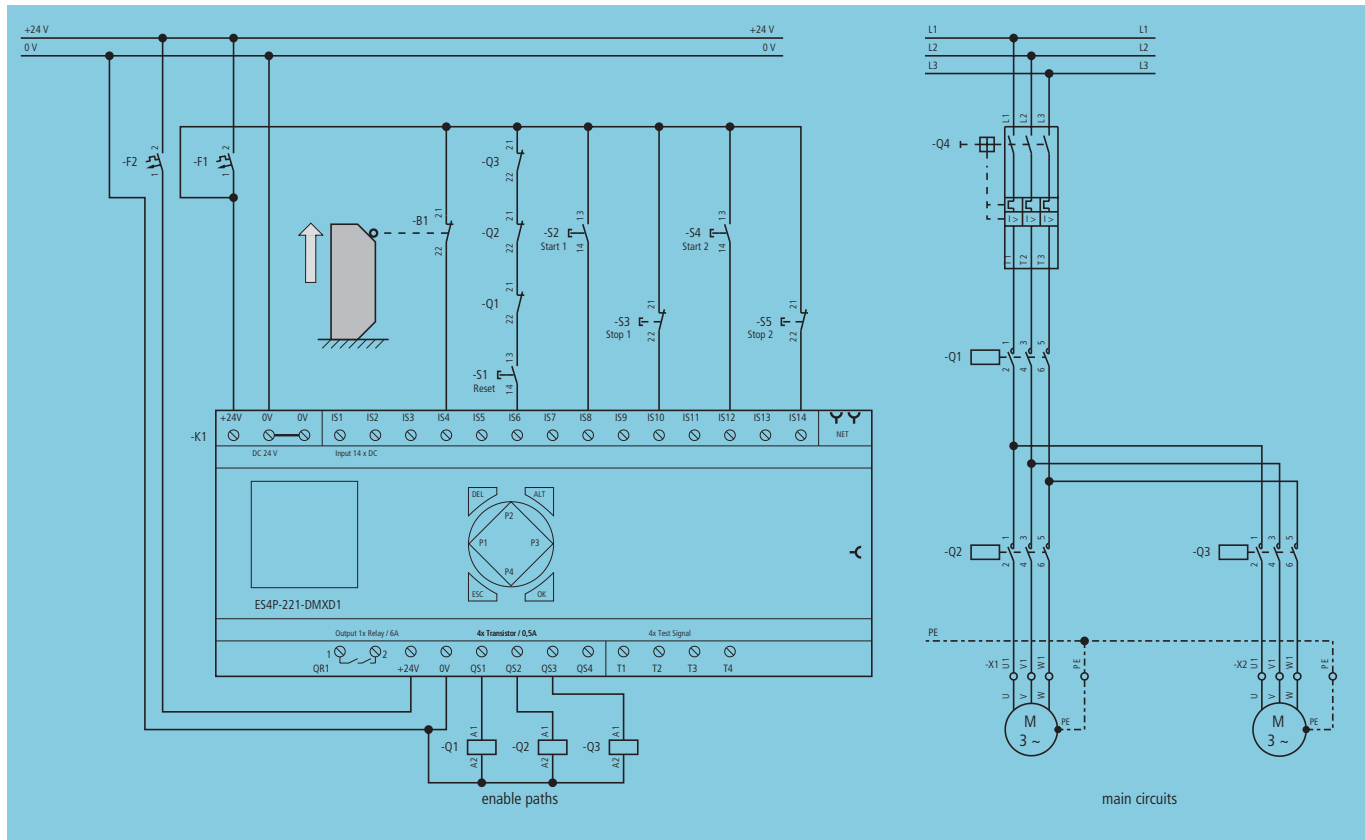


Figure 15: Single-channel guard door monitoring with easySafety

Requirements

- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Protect position switch and supply conductor from mechanical stresses.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with well-tried components and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Monitoring of redundant contactors via feedback loop.
- Connection fault in position switch or supply conductor as well as mechanical failure of the position switch causes loss of the safety function.

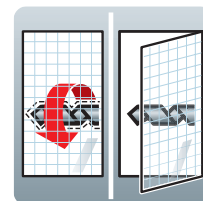
Function

The guard door must be in a closed position (N/C contact B1 closed) for the enable signal to be issued. The feedback loop of the N/C contacts can ensure the normal position of the disconnection contactors Q1 - Q3. If the status is present, the enable can be issued by actuating the RESET button S1. The output QS1 of easySafety switches through, contactor Q1 picks up and its feedback signalling contact opens. Pressing the START actuator S2, S4 for the respective drive starts the hazardous movement.

The self-latching function and its interruption are implemented by the easySafety program. The appropriate contactor drops out. Restarting is possible by actuating the START actuator. Opening the guard causes the easySafety outputs QS1 - QS3 to disconnect and thus de-energize the enable paths. The easySafety is switched to operational readiness by the reclosed N/C contacts.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 1	Structure	SS A
MTTF _d	100 years	PFH _d	3.98×10^{-8}
B10 _d	B1: 20000000, Q1-Q3: 1300000	B10	B1: 4000000, Q1-Q3: 975000
n _{op}	B1, Q1: 12960, Q2-Q3: 65000	λ_d/λ	B1: 0.2, Q1-Q3: 0.75
CCF	80	C	B1, Q1: 2.25, Q2-Q3: 11.285
DC _{avg}	97.27 %	β	0.05
PL	c	DC	B1: 0 %, K1: 99 %, Q1-Q3: 99 %
T10 _d	> 20 years	SIL	1

Safety-related switching devices



LS-11 position switch (1 N/O, 1 N/C)



easySafety ES4P-221-DMXD1
safety control relay



DILM12 and DILM25 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.3 Several guards with safety relay

Application

- For cyclical interventions in the hazardous area.
- When only a protective door is actuated during interventions in the hazardous area.
- If the stopping time is less than the entry and access time.

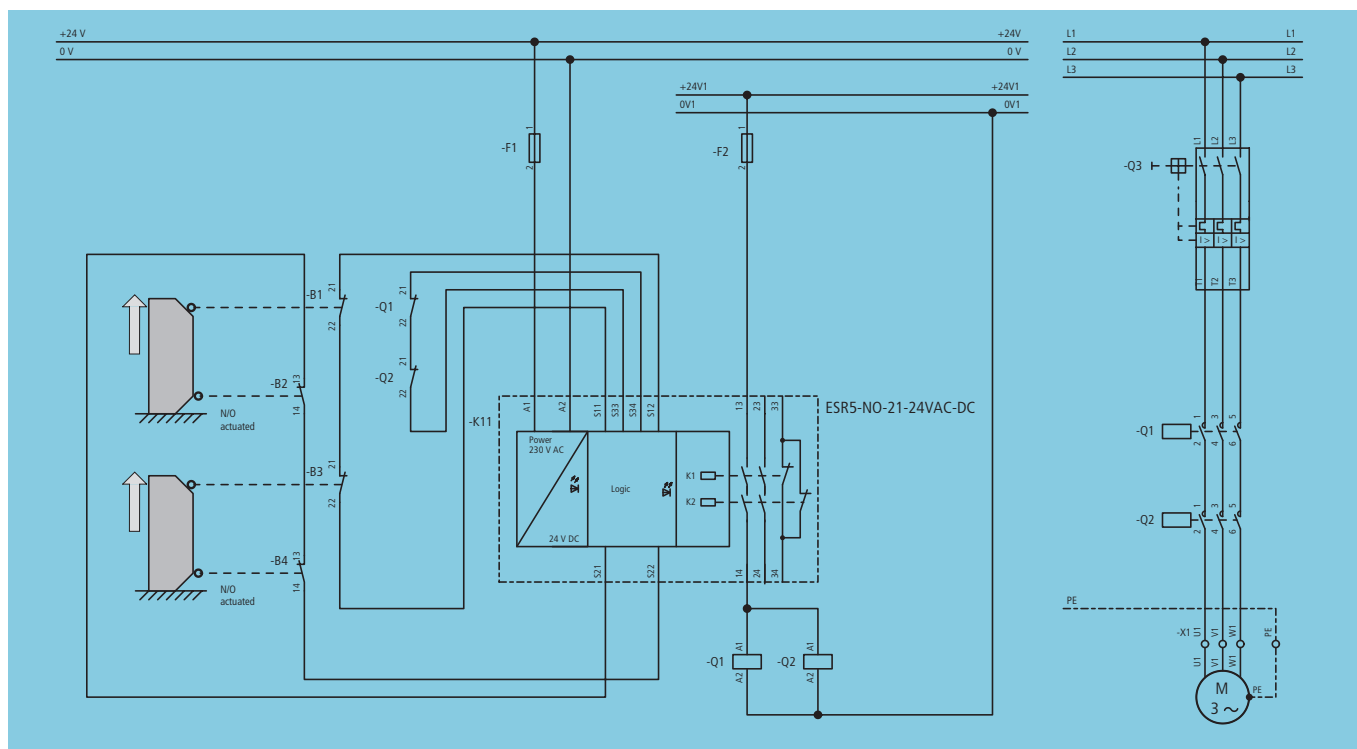


Figure 16: Guard door application with two guards on ESR5

Requirements

- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Use safety relays with mechanically linked contacts.
- Hard wire with electromechanical components.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- When only a protective door is actuated during interventions in the hazardous area.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Position switches, supply conductor and command processing are redundant.
- Actuated position switch, supply conductor and command processing are self-monitoring.
- Single faults: Wire break, connection fault and cross-circuit are always reliably detected if the second guard door stays closed.

- Single-channel connection fault is not reliably detected if the second door is opened.
- A single fault does not cause the loss of safety function.
- An accumulation of undetected faults can cause a hazardous situation (connection fault with two contacts).
- Monitoring of redundant contactors/safety valves via feedback loop.
- Planned movement of the movable guard is normally detected by an N/C / N/O contact combination.

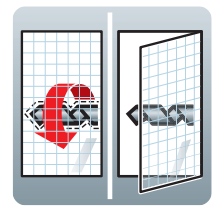
Function

After the supply voltage is applied to the safety relay (terminal A1-A2), the Power LED indicates readiness for activation of the enable paths. When the last still opened guard is closed, the N/C contacts of the feedback loop check first of all that the contactors Q1 and Q2 are in their rest position. If this state is present, the enable relays inside the ESR pick up, which is indicated via LEDs K1 and K2.

The not safety-related signalling path (terminal 41-42) is opened and contactors Q1 and Q2 can pick up via the enable paths (terminal 13-14 and 23-24).



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



→ Not all faults are reliably detected due to the series connection of the safety guards. It may be necessary to implement a justified fault exclusion to the acknowledgement of a short-circuit fault by the second safety guard. In this case, detailed documentation about the fault exclusion must be created.

→ A higher safety integrity level can be achieved by the additional monitoring of the positions of the position switches, → chapter 2.4 "Several guards with easySafety", page 42.

Condition	EN ISO 13849
Structure	Cat. 3
MTTF _d	39.34 years
B10 _d	B1, B3: 20000000, B2, B4: 1000000, Q1, Q2: 1300000
n _{op}	65000
CCF	80
DC _{avg}	83.66 %
PL	d
T10 _d	B2, B4: 15.38 years, K1: 9.6 years, all others: >20 years

Condition	IEC 62061
Structure	SS D asymmetrical
PFH _d	7.5 x 10 ⁻⁸
B10	B1, B3: 4000000, B2, B4: 500000, Q1, Q2: 975000
λ _d /λ	B1, B3: 0.2, B2, B4: 0.5, Q1, Q2: 0.75
C	11.285
β	0.05
DC	B1-B4: 60 %, K1: 99 %, Q1-Q2: 99 %
SIL	2

Safety-related switching devices



LS-11, LS-02 position switch



Safety relays ESR5-NO-21-24VAC-DC



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.4 Several guards with easySafety

Application

- For cyclical interventions in the hazardous area.
- If the stopping time is less than the entry and access time.

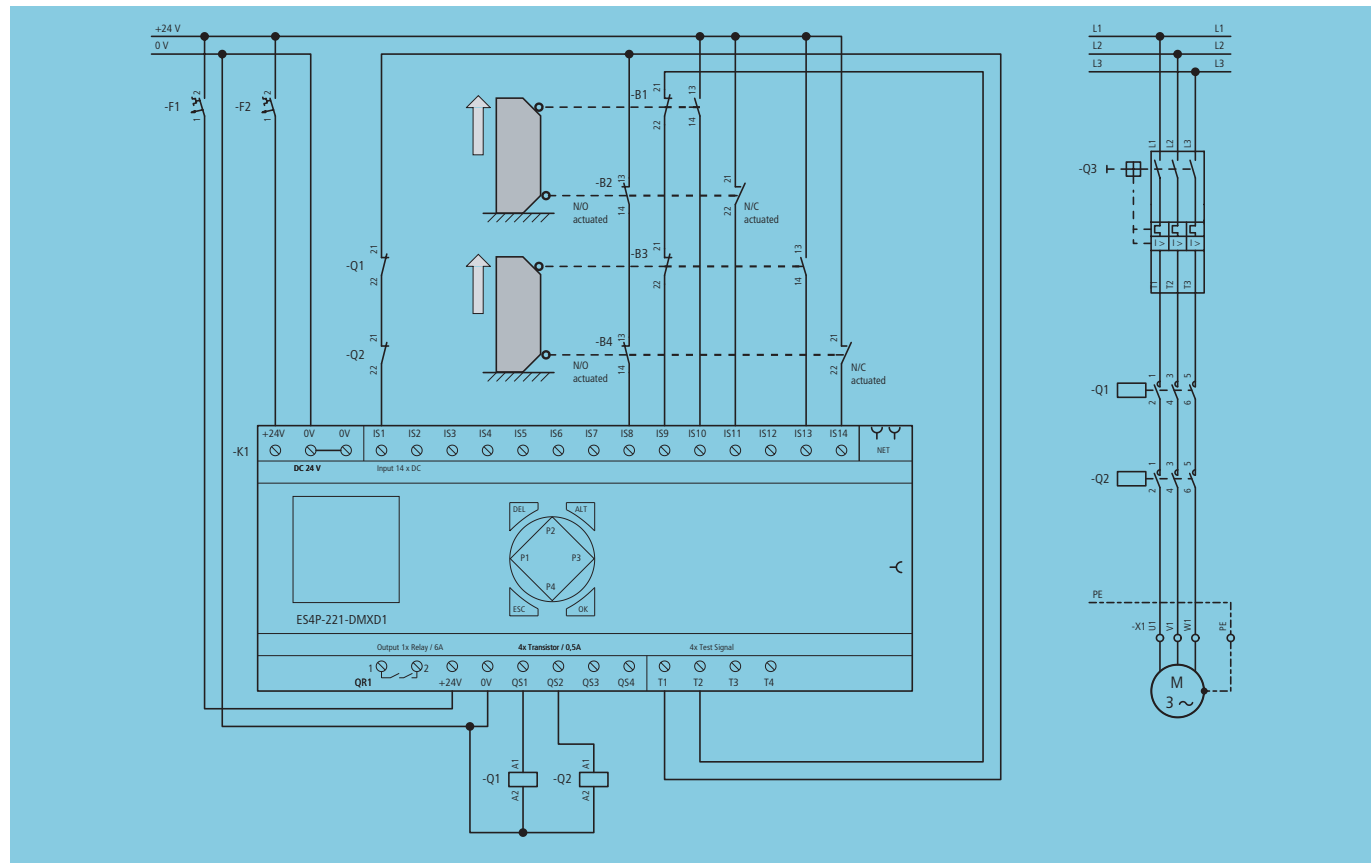


Figure 17: Guard door application with two guards on easySafety

Requirements

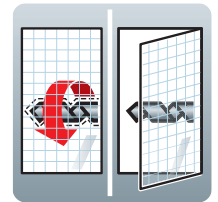
- Use positively opening position switches to IEC 60947-5-1, Annex K, and function to ISO 14119 as well as positively driven contacts.
- Use inputs of the safety guard channels (IS8 and IS9) with different test signals.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Position switches, supply conductor and command processing are redundant.
- Actuated position switch, supply conductor and command processing are self-monitoring.
- Single faults: Wire break and cross-circuit are detected reliably.
- Connection fault is covered via the diagnostics of the positively driven auxiliary contacts.
- Diagnostics of the auxiliary contacts can also be implemented in the standard circuit diagram of the easySafety.
- Planned movement of the movable guard is normally detected by an N/C / N/O contact combination.
- Category 3 system behavior allows the accumulation of undetected faults to lead to the loss of the safety function.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

When the last still opened guard is closed, the Safety Gate (SG) safety function block issues the enable to activate the device safety outputs. The feedback circuit monitoring then first checks that the contactors are in the rest position. If this state is present, the EM (External Monitor) function block issues the enable and sets device outputs QS1 and QS2. The contactors Q1 and Q2 pick up and their normally closed contacts open.



The device switches off safely if there is a connection fault across the contacts of a channel. A restart is prevented by the diagnostics device of the positively driven auxiliary contacts.

Condition	EN ISO 13849
Structure	Cat. 3
MTTF _d	58.18 years
B10 _d	B1, B3: 20000000, B2, B4: 1000000, Q1, Q2: 1300000
η_{op}	65000
CCF	80
DC _{avg}	99 %
PL	e
T10 _d	B2, B4: 15.38 years, all others: > 20 years

Condition	IEC 62061
Structure	SS D, asymmetrical
PFH _d	7.46×10^{-8}
λ_d/λ	B1, B3: 0.2, B2, B4: 0.5, Q1, Q2: 0.75
B10	B1, B3: 4000000, B2, B4: 500000, Q1, Q2: 975000
C	11.285
β	0.05
DC	B1-B4: 99 %, K1: 99 %, Q1-Q2: 99 %
SIL	3

Safety-related switching devices



LS-11 position switches



easySafety ES4P-221-DMXD1
safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.5 Two-channel with safety relay

Application

- For cyclical interventions in the hazardous area.
- If the stopping time is less than the entry and access time.

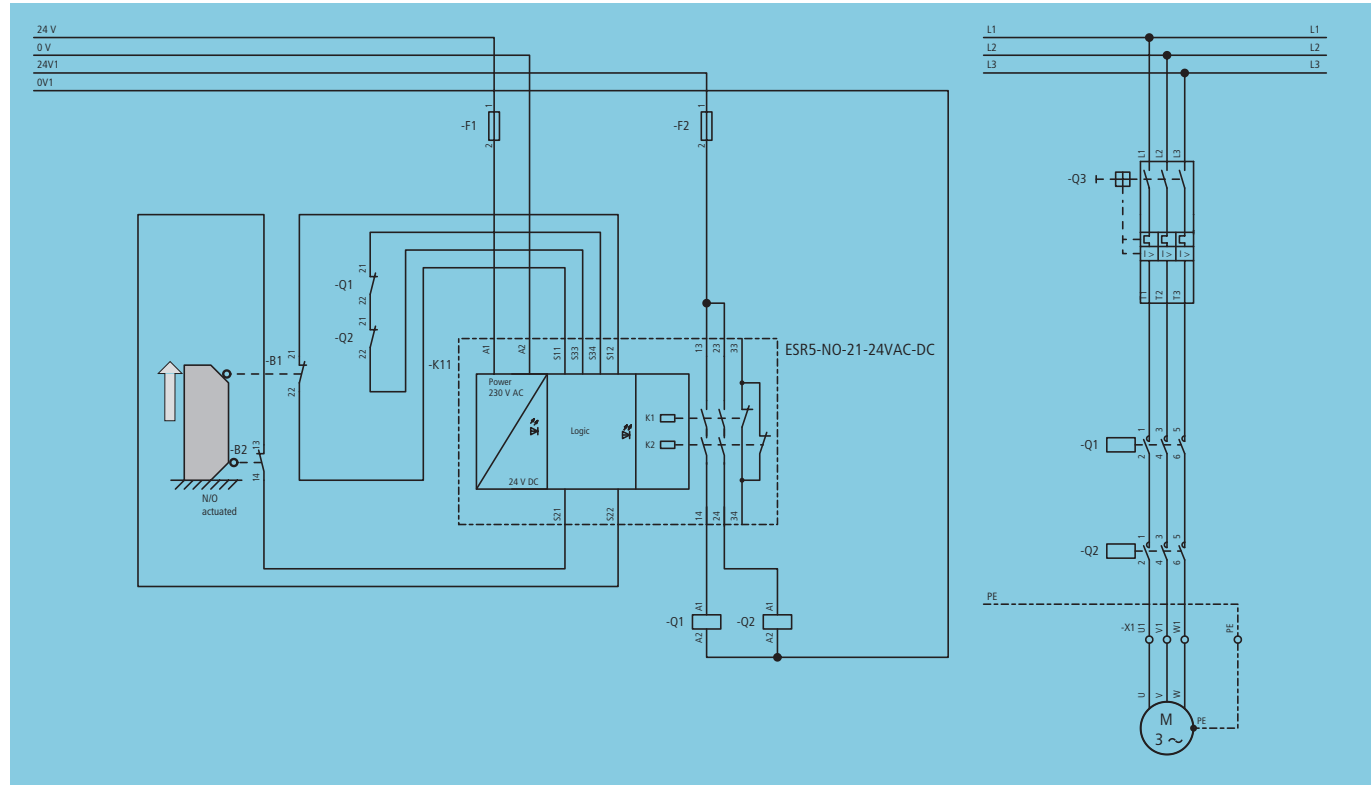


Figure 18: Two-channel guard door with ESR5

Requirements

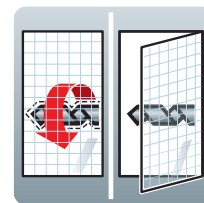
- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Use separately laid supply conductor.
- Hard wire with electromechanical components.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Position switch, supply conductor and command processing are redundant and self-monitoring.
- Monitoring of redundant contactors via feedback loop.
- Single faults: Wire break, connection fault and cross-circuit in position switch, supply conductor and safety relay are detected immediately or with the next start command.
- Planned movement of the movable guard is normally detected by an N/C / N/O contact combination.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

After the supply voltage is applied to the safety relay (terminal A1-A2), the Power LED indicates readiness for activation of the enable paths. When the guard is closed, the N/C contacts of the feedback circuit check first of all that the contactors Q1 and Q2 are in their rest position. If this state is present, the enable relays inside the ESR pick up, which is indicated via LEDs K1 and K2. The not safety-related signalling path (terminal 31-32) is opened and contactors Q1 and Q2 can pick up via the enable paths (terminal 13-14 and 23-24).

Opening the guard switches off relays K1 and K2 inside the ESR via the two position switches B1, B2. The not safety-related signal path (terminal 31-32) closes and the enable paths open. The contactors Q1, Q2 drop out and the safety relay switches to ready status via the now closed N/C contact in the feedback circuit.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 4	Structure	SS D asymmetrical, SS D symmetrical
MTTF _d	62.88 years	PFH _d	7.58×10^{-8}
B10 _d	B1: 20000000, B2: 1000000, Q1, Q2: 1300000	B10	B1: 4000000, B2: 500000, Q1, Q2: 975000
n _{op}	65000	λ_d/λ	B1: 0.2, B2: 0.5, Q1, Q2: 0.75
CCF	80	C	11.285
DC _{avg}	99 %	β	0.05
PL	e	DC	B1, B2, K1, Q1, Q2: 99 %
T10 _d	B2: 15.38 years, K1: 9.6 years, all others: > 20 years	SIL	3

Safety-related switching devices



LS-11, LS-02 position switch



Safety relays ESR5-NO-21-24VAC-DC



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.6 Two-channel with safety relay and RS2

Application

- For cyclical interventions in the hazardous area.
- If the stopping time is less than the entry and access time.

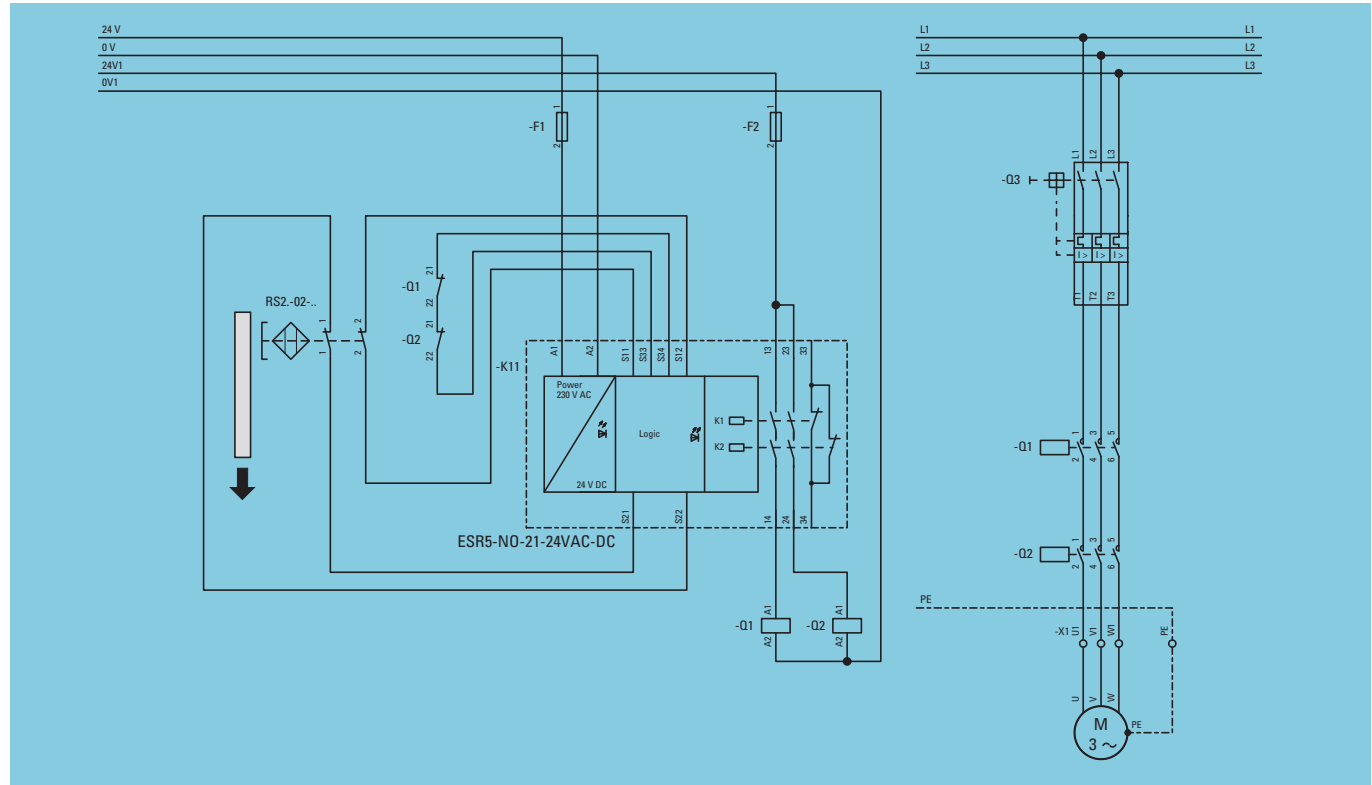


Figure 19: Two-channel guard door system with safety relay

Requirements

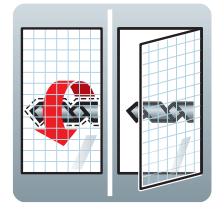
- Use non-contacting safety switches that conform to IEC 60947-5-3 and operation in accordance with ISO 14119 type 3 or 4.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Fault exclusion required for the input wiring, so the cable must be laid with shielding!
- Hard wire with electromechanical components.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tries safety principles (EN ISO 13849-1 and EN ISO 13849-2).
- Redundant, self-monitoring command processing.
- Monitoring of redundant contactors via feedback circuit.
- Single faults: Wire break, connection fault and cross-circuit in position switch, supply conductor and safety relay are detected immediately or with the next start command.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

After the supply voltage is applied to the safety relay (terminal A1-A2), the Power LED indicates readiness for activation of the enable paths. When the guard is closed, the N/C contacts of the feedback circuit check first of all that the contactors Q1 and Q2 are in their rest position. If this state is present, the enable relays inside the ESR pick up, which is indicated via LEDs K1 and K2. The not safety-related signalling path (terminal 31-32) is opened and contactors Q1 and Q2 can pick up via the enable paths (terminal 13-14 and 23-24).

Opening the guard switches off relays K1 and K2 inside the ESR via the two position switches B1, B2. The not safety-related signal path (terminal 31-32) closes and the enable paths open. The contactors Q1, Q2 drop out and the safety relay switches to ready status via the now closed N/C contact in the feedback circuit.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 3	Structure	SS D symmetrical
MTTF _d	63 years	PFH _d	4.79 x 10 ⁻⁸
B10 _d	B1: 20000000, Q1, Q2: 1.300000	B10	B1: 5000000, Q1, Q2: 975000
n _{op}	6500	λ _d /λ	B1: 0.25 Q1, Q2: 0.75
CCF	80	C	11.285
DC _{avg}	99 %	β	0.05
PL	d	DC	B1, K11, Q1, Q2: 99 %
T10 _d	20 years	SIL	2

A performance level of PL_e can be mathematically achieved, but a minimum HFT of 1 is required for PL_e, and this HFT is not achievable when using only one RS switch. Fault exclusion is not possible either - refer to ISO 14119 sec. 8.2 and ISO 13849-2, Annex D.8. Because of this, cat. 3 and PL_d are the highest achievable levels.

Safety-related switching devices



Non-contact safety switches RS2-02-C3



Safety relays ESR5-NO-21-24VAC-DC



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.7 Two-channel with safety relay and redundant RS2

Application

- For cyclical interventions in the hazardous area.
- If the stopping time is less than the entry and access time.

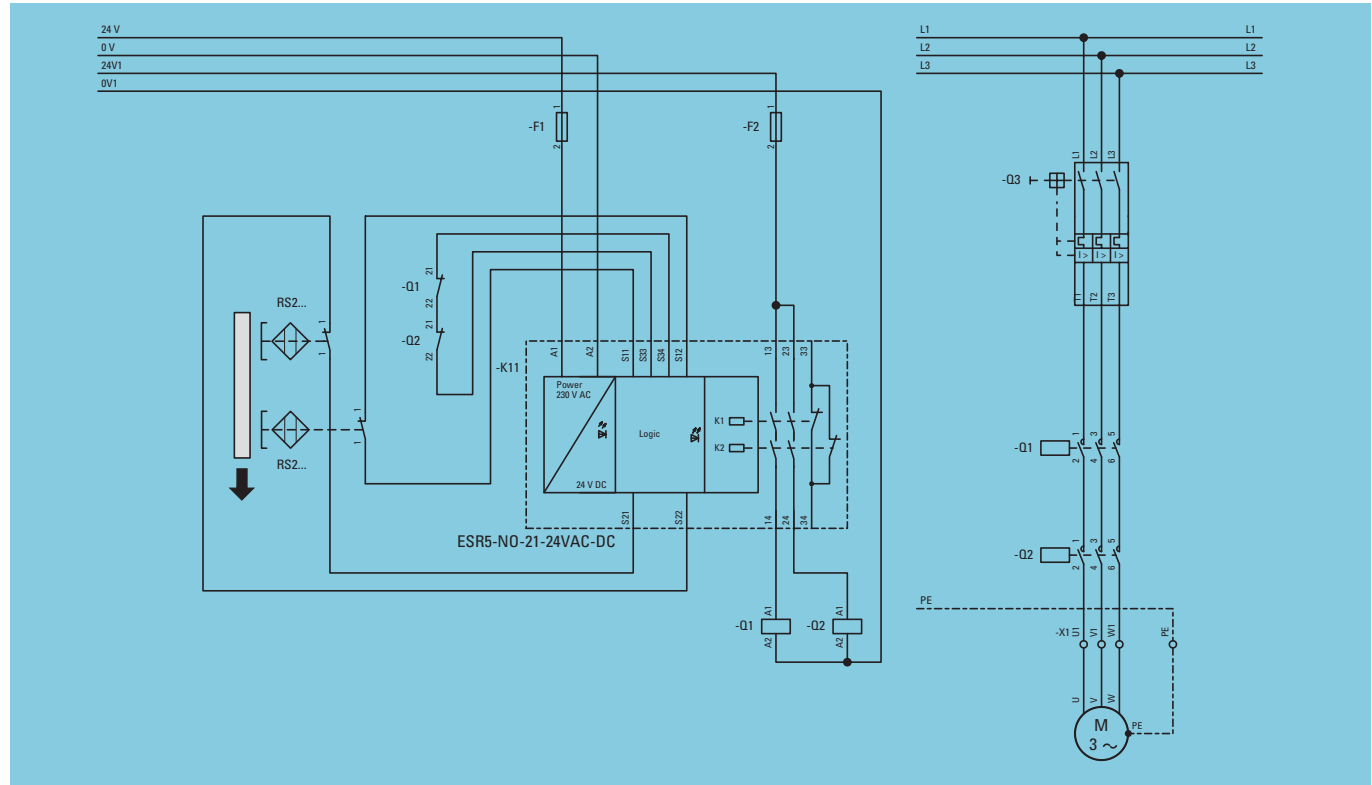


Figure 20: Two-channel guard door monitoring with redundant sensor

Requirements

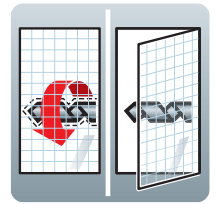
- Use non-contacting safety switches that conform to IEC 60947-5-3 and operation in accordance with ISO 14119 type 3 or 4.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Redundant, self-monitoring non-contacting safety switches, input wiring, and command processing.
- Monitoring of redundant contactors via feedback loop.
- Single faults: Wire break, connection fault and cross-circuit in position switch, supply conductor and safety relay are detected immediately or with the next start command.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

After the supply voltage is applied to the safety relay (terminal A1-A2), the Power LED indicates readiness for activation of the enable paths. When the guard is closed, the N/C contacts of the feedback circuit check first of all that the contactors Q1 and Q2 are in their rest position. If this state is present, the enable relays inside the ESR pick up, which is indicated via LEDs K1 and K2. The not safety-related signalling path (terminal 31-32) is opened and contactors Q1 and Q2 can pick up via the enable paths (terminal 13-14 and 23-24).

Opening the guard switches off relays K1 and K2 inside the ESR via the two position switches B1, B2. The not safety-related signal path (terminal 31-32) closes and the enable paths open. The contactors Q1, Q2 drop out and the safety relay switches to ready status via the now closed N/C contact in the feedback circuit.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 3	Structure	SS D symmetrical
MTTF _d	63 years	PFH _d	4.79 x 10 ⁻⁸
B10 _d	B1: 20000000, Q1, Q2: 1300000	B10	B1, B2: 5000000, Q1, Q2: 975000
n _{op}	6500	λ _d /λ	B1, B2: 0.25, Q1, Q2: 0.75
CCF	80	C	11.285
DC _{avg}	99 %	β	0.05
PL	e	DC	B1, B2, K11, Q1, Q2: 99 %
T10 _d	20 years	SIL	2

A fault exclusion is required for the input wirings, so the cable must be laid with shielding!

Safety-related switching devices



Non-contact safety switches RS2-02-C3



Safety relays ESR5-NO-21-24VAC-DC



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.8 Two-channel with easySafety

Application

- For cyclical interventions in the hazardous area.
- If the stopping time is less than the entry and access time.

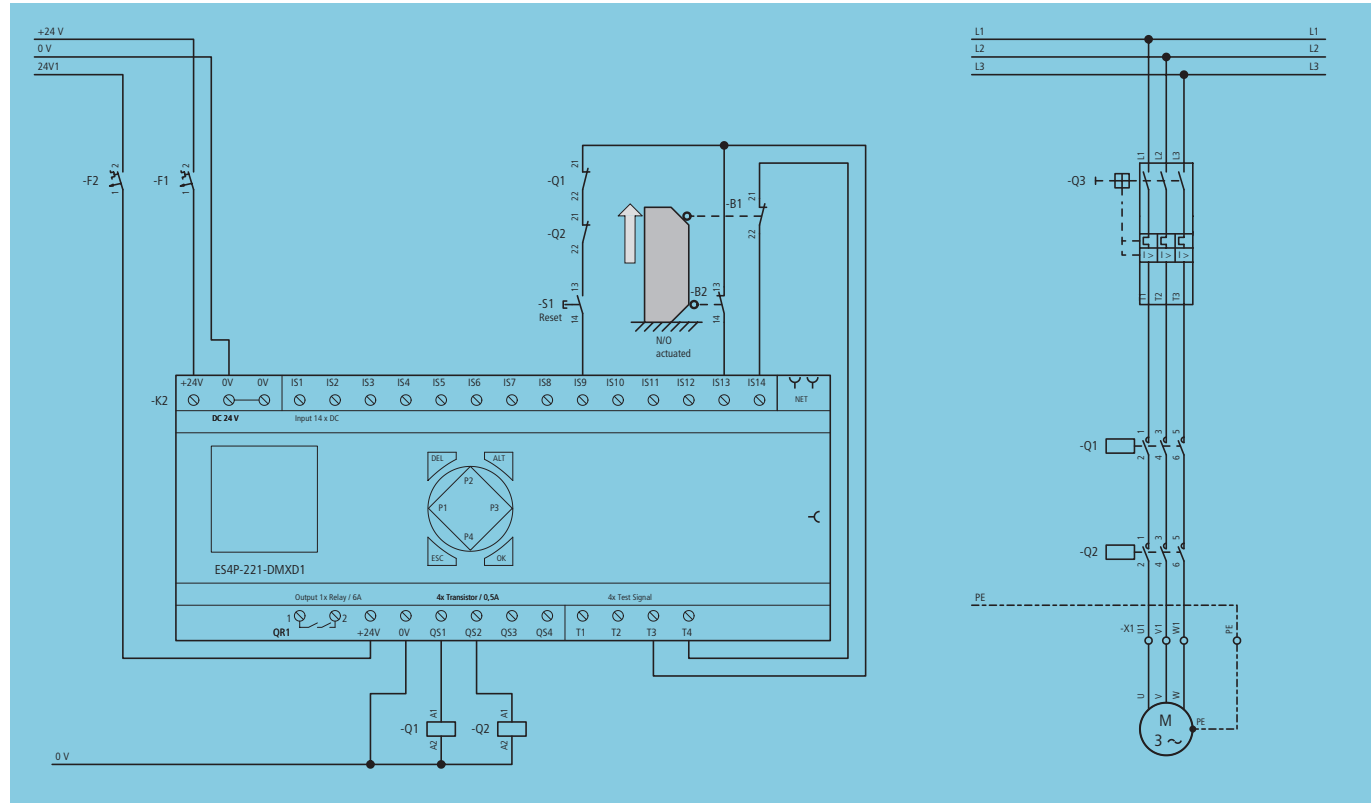


Figure 21: Two-channel guard door with **easySafety**

Requirements

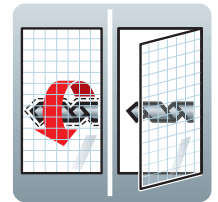
- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Use inputs with different test signals.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Lay conductor separately.
- Hard wire with electromechanical components.
- Test the mechanical functioning of the movable guard according to the specified intervals.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Position switch, supply conductor and command processing are redundant and self-monitoring.
- Monitoring of redundant contactors via feedback loop.
- Wire break, connection fault and cross-circuit in position switch, supply conductor and **easySafety** are detected immediately or with the next start command.
- Planned movement of the movable guard is normally detected by an N/C / N/O contact combination.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

The guard door must be in a closed position (N/C contact and N/O contact B1 and B2 closed), so that the enable can be issued. The feedback loop of the N/C contacts can ensure the normal position of the disconnection contactors Q1 and Q2. If the status is present, the enable can be issued by actuating the RESET button S1. The output relays of the **easySafety**

switch through, the contactors Q1 and Q2 pick up and their looped back signalling contacts open. Opening the guard causes the **easySafety** outputs QS1 and QS2 to disconnect and thus de-energize the enable paths. The **easySafety** is switched to operational readiness by the reclosed N/C contacts.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 4	Structure	SS D asymmetrical, SS D symmetrical
MTTF _d	100 years	PFH _d	7.46×10^{-8}
B10 _d	B1: 20000000, B2: 1000000, Q1, Q2: 1300000	B10	B1: 4000000, B2: 500000, Q1, Q2: 975000
n _{op}	65000	λ_d/λ	B1: 0.2, B2: 0.5, Q1, Q2: 0.75
CCF	80 pnt.	C	11.285
DC _{avg}	99 %	β	0.05
PL	e	DC	B1, B2, K1, Q1, Q2: 99 %
T10 _d	B2: 15.38 years, all others: > 20 years	SIL	3

Safety-related switching devices



LS-11, LS-02 position switch



easySafety ES4P-221-DMXD1
safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.9 With guard locking – enable via timer

Application

- When the safety interlock is not to be used for stopping the machine during normal operation.
- When the safety interlock is only to protect against minor hazards.
- For cyclical interventions in the hazardous area.
- If the stopping time is greater than the entry and access time.

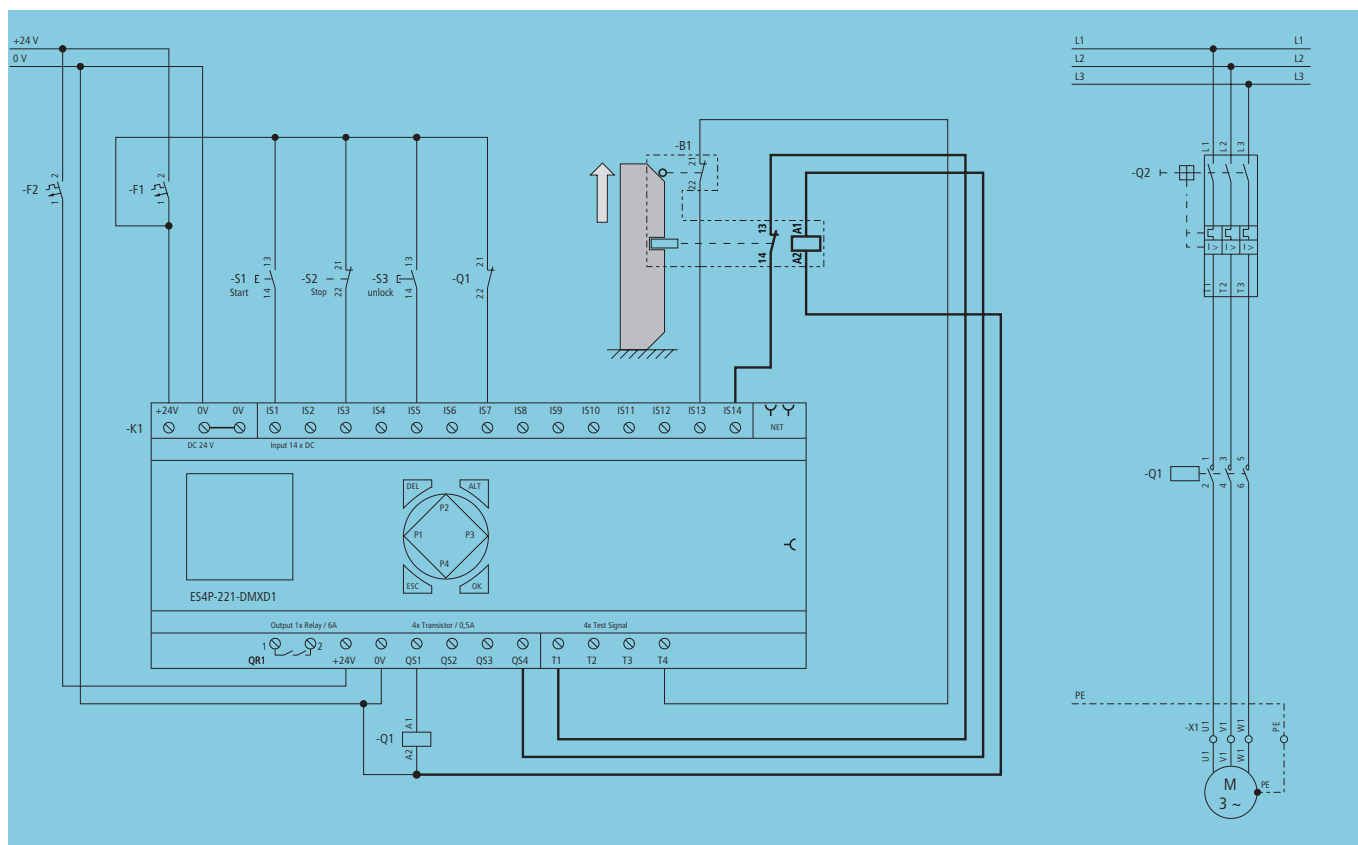


Figure 22: Safety interlock with enable via "Safety timing relay" (TS, Timing relay Safety)

Requirements

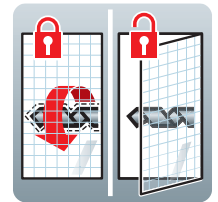
- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Safety interlock must be protected against undesired closing, i.e. the locking means cannot go to the locked position when the guard is opened.
- Hard wire with electromechanical components.
- Select safety time so that the lock does not open until after the hazardous movement has ended.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with well-tried components and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Monitoring of the guard locking via signalling contact of the safety position switch.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

When the guard is closed and the coil of the safety interlock is de-energized, the guard cannot be opened. To open the guard, the hazardous movement must first be switched off with the Stop command. The N/O contact S3 (unlatching) is then actuated. The safety timing relay first ensures that there is no hazardous movement. **easySafety** output QS4 is set when the safety time has elapsed. The actuation magnet for the lock

mechanism picks up, unlocks the guard and opens the N/C contact B1 (terminal 13-14).



Product standards may require the use of panic openers inside the doors that must open guards in any situation.

Condition	EN ISO 13849
Structure	Cat. 1
MTTF _d	100 years
B10 _d	B1 (A1-A2): 10000
n _{op}	360
CCF	not relevant
DC _{avg}	not relevant
PL	c
T10 _d	> 20 years

Condition	IEC 62061
Structure	SS A
PFH _d	6.34×10^{-7}
B10	B1 (A1-A2): 5000
λ_d/λ	B1 (A1-A2): 0.5
C	0.0625
β	not relevant
DC	not relevant
SIL	1

Safety-related switching devices



LS-S02-24DFT-ZBZ/X position switch with guard locking



easySafety ES4P-221-DMXD1 safety control relay

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

Monitoring a movable guard

2.10 With guard locking – enable via zero speed monitoring

Application

- When the safety interlock is only to protect against minor hazards and a single-channel structure is sufficient.
- For cyclical interventions in the hazardous area.
- If the stopping time is greater than the entry and access time.

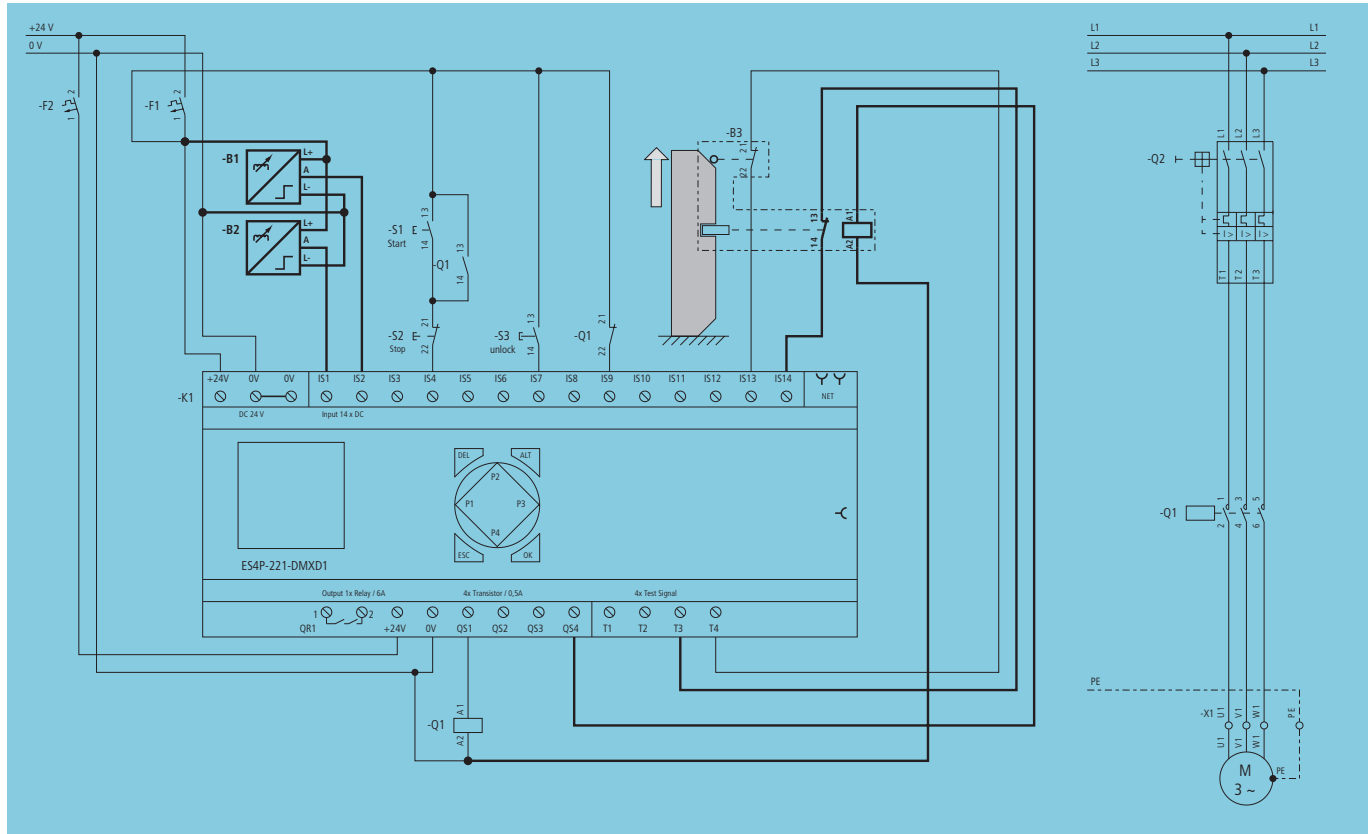


Figure 23: Safety interlock with enable via integrated "Zero speed monitoring" function block (ZM, Zero-speed monitor) in ES4P-...

Requirements

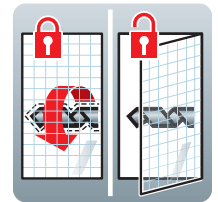
- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Safety interlock must be protected against undesired closing, i.e. the locking means cannot go to the locked position when the guard is opened.
- Hard wire with electromechanical components.
- Arrange proximity switches B1 and B2 in such a way that at least one sensor is actuated at any time. Observe mounting instructions of manufacturer!
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with well-tried components and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Monitoring of the guard locking via signalling contact of the safety position switch.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

When the guard is closed and the coil of the safety interlock is de-energized, the guard cannot be opened. To open the guard, the hazardous movement must first be switched off with the Stop command. The N/O contact S3 (unlatching) is then actuated. The zero speed monitoring first ensures that there is no hazardous movement. **easySafety** output QS4 is set when the zero speed has been reached. The actuation magnet for the lock mechanism picks up, unlocks the guard and opens the N/C contact B3 (terminal 13-14).



Product standards (C standards) may require the use of panic openers inside the doors that must open guards in any situation.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 1	Structure	TS C, SS D symmetrical
MTTF _d	43.4 years	PFH _d	7.83×10^{-8}
B10 _d	B3 (A1-A2): 10000	B10	B3 (A1-A2): 5000
n _{op}	360	λ _d /λ	B3 (A1-A2): 0.5
CCF	not relevant	C	0.0625
DC _{avg}	not relevant	β	not relevant
PL	c	DC	B1, B2: 90 %, K1: 99 %, B3 (13-14): 90 %
T10 _d	> 20 years	SIL	1

Safety-related switching devices



Proximity sensor E57-...



easySafety ES4P-221-DMXD1 safety control relay



LS-S02-24DFT-ZBZ/X position switch with guard locking

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	111
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

3 Monitoring open hazardous area

3.1 With light curtain and safety relay

Application

- For cyclical interventions in the hazardous area.
- When hazards could arise for the operator due to intervention in the hazardous area.
- If the stopping time is less than the entry and access time.

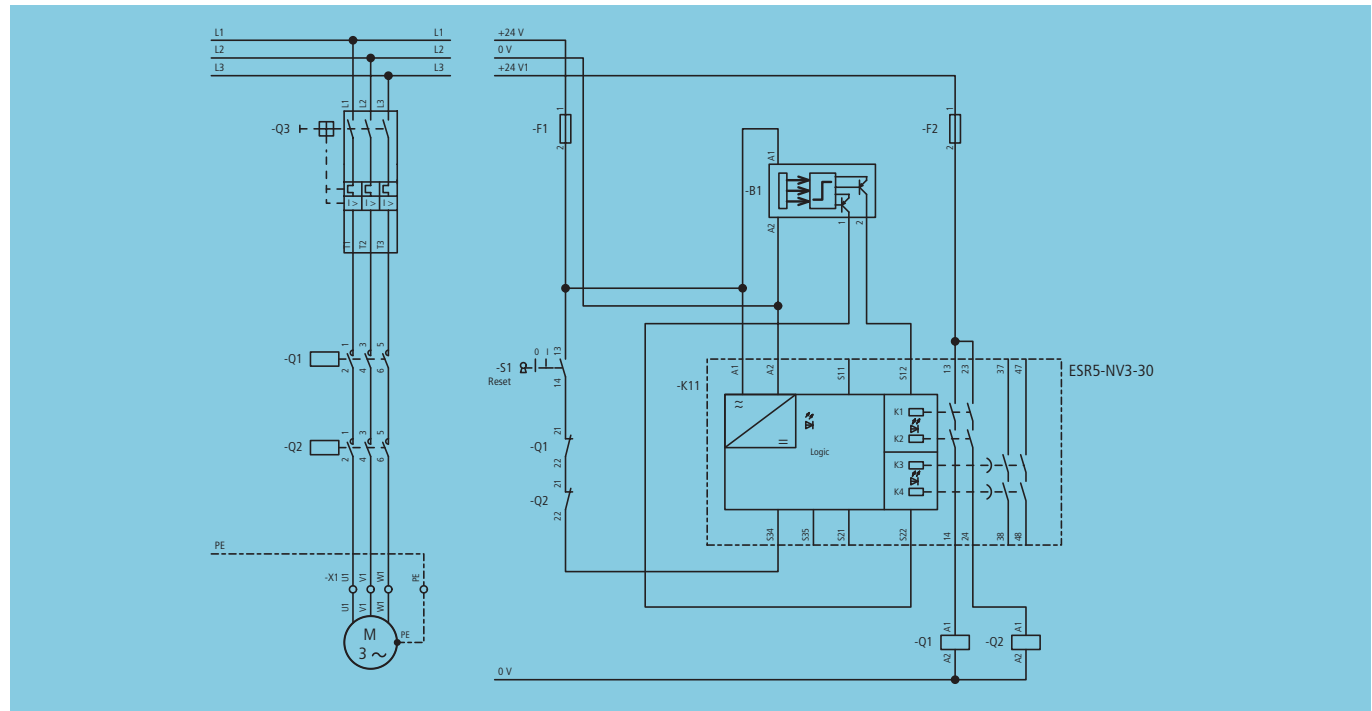


Figure 24: Electro-sensitive protective equipment on safety relay ESR5

Requirements

- Electro-sensitive protective equipment (ESPE) devices to IEC 61496-1.
- Active opto-electronic protective device (AOPDs) to IEC 61496-2.
- Immediate disconnection of all hazardous movements in the safety clearance of the ESPE. Observe mounting instructions of manufacturer!
- Do not position RESET switch S1 in the hazardous area.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Provide manual restart with self-latching.
- Case A: Unrestricted utilization period.
- Case B: Exchange contactors after 2.26 years!
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Monitoring of redundant contactors via feedback loop.
- Single faults: Wire break, connection fault and cross-circuit in control circuit device, supply conductor and safety relay are detected immediately or with the next start command.

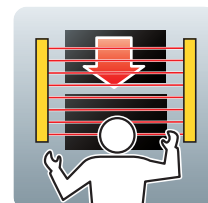


Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

After the supply voltage is applied to the safety relay K1 (terminal A1-A2), the Power LED indicates operational readiness for activating the enable paths. If there is no object in the protected field of light curtain B1, the enable relays inside the ESR are activated by means of a rising edge at input S34. LEDs K1 and K2 indicate this state. Contactors Q1 and Q2 pick up

and their auxiliary contacts open. If there is an intervention in the protected field, the OSSD outputs of the ESPE are deactivated. The enable relays inside the ESR (13-14, 23-24 non-delayed; 37-38, 47-48 with adjustable delay) drop out and thus remove the enable from contactors Q1 and Q2.

Condition	EN ISO 13849	
	Case A	Case B
Structure	Cat. 4	Cat. 3
MTTF _d	56.69 years	16.18 years
B10 _d	Q1, Q2: 1300000	Q1, Q2: 1300000
n _{op}	1800	576000
CCF	80	80
DC _{avg}	99 %	99 %
PL	e	d
T10 _d	> 20 years	Q1, Q2: 2.26 years, all others: > 20 years

Condition	IEC 62061	
	Case A	Case B
Structure	SS D, asymmetrical	SS D, asymmetrical
PfH _d	1.79 x 10 ⁻⁸	4.95 x 10 ⁻⁷
B10	Q1, Q2: 975000	Q1, Q2: 975000
λ _d /λ	Q1, Q2: 0.75	Q1, Q2: 0.75
C	0.3125	100
β	0.05	0.05
DC	99 %	99 %
SIL	3	2

Safety-related switching devices



Light curtain C4000, Manufacturer: Sick



Safety relays ESR5-NV3-30



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
IEC 61496-1/-2	Safety of machinery – electro-sensitive protective equipment Part 1: General requirements and tests Part 2: Particular requirements for active opto-electronic protective devices	–
EN ISO 13855	Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body	–

Monitoring open hazardous area

3.2 With light curtain and easy Safety

Application

- For cyclical interventions in the hazardous area.
- When hazards could arise for the operator due to intervention in the hazardous area.
- If the stopping time is less than the entry and access time.

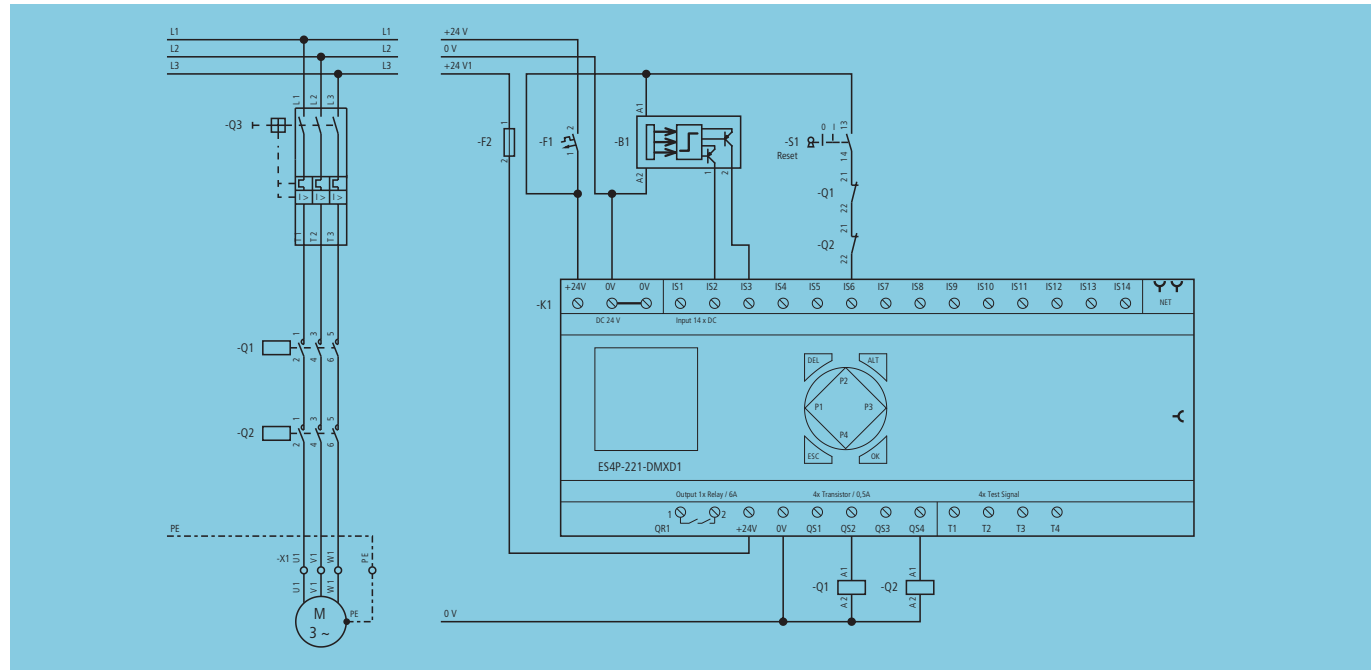


Figure 25: Electro-sensitive protective equipment on **easySafety**

Requirements

- Electro-sensitive protective equipment (ESPE) devices to IEC 61496-1.
- Active opto-electronic protective device (AOPDs) to IEC 61496-2.
- Immediate disconnection of all hazardous movements in the safety clearance of the ESPE. Observe mounting instructions of manufacturer!
- Do not position RESET switch S1 in the hazardous area.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Provide manual restart with **easySafety**.
- Case A: Unrestricted utilization period.
- Case B: Exchange contactors after 2.26 years!
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Monitoring of redundant contactors via feedback loop.
- Single faults: Wire break, connection fault in control circuit device, supply conductor and **easySafety** relay are detected immediately or with the next start command.

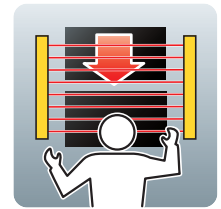


Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

There should be no object in the protected area of light curtain B1 (outputs of the light curtain uninterrupted state) so that the enable can be issued. The feedback loop of the N/C contacts can ensure the normal position of the disconnection contactors Q1 and Q2. If the status is present, the enable can be issued by actuating the RESET button S1. The output relays of the **easySafety** switch through, the contactors Q1 and Q2 pick up and their looped back signalling contacts open. An interruption in the

protected area of the ESPE stops the movements in the protection zone by disconnecting outputs QS2 and QS4 of **easySafety**. This de-energizes both enable paths. The **easySafety** is switched to operational readiness by the reclosed N/C contacts.

Condition	EN ISO 13849	
	Case A	Case B
Structure	Cat. 4	Cat. 3
MTTF _d	100 years	19.42 years
B10 _d	Q1, Q2: 1300000	Q1, Q2: 1300000
n _{op}	1800	576000
CCF	80	80
DC _{avg}	99 %	99 %
PL	e	d
T10 _d	> 20 years	Q1, Q2: 2.26 years, all others: > 20 years

Condition	IEC 62061	
	Case A	Case B
Structure	SS D, symmetrical	SS D, symmetrical
PFH _d	1.66 x 10 ⁻⁸	4.93 x 10 ⁻⁷
B10	Q1, Q2: 975000	Q1, Q2: 975000
λ _d /λ	Q1, Q2: 0.75	Q1, Q2: 0.75
C	0.3125	100
β	0.05	0.05
DC	99 %	99 %
SIL	3	2

Safety-related switching devices



Light curtain C4000, Manufacturer: Sick



easySafety ES4P-221-DMXD1
safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungsgeräte	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
IEC 61496-1/-2	Safety of machinery – electro-sensitive protective equipment Part 1: General requirements and tests Part 2: Particular requirements for active opto-electronic protective devices	–
EN ISO 13855	Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body	–

Monitoring open hazardous area

3.3 With light curtain muting and easySafety

Application

- For cyclical interventions in the hazardous area.
- If material has to be moved through the protected area of the guard without stopping the operating sequence.

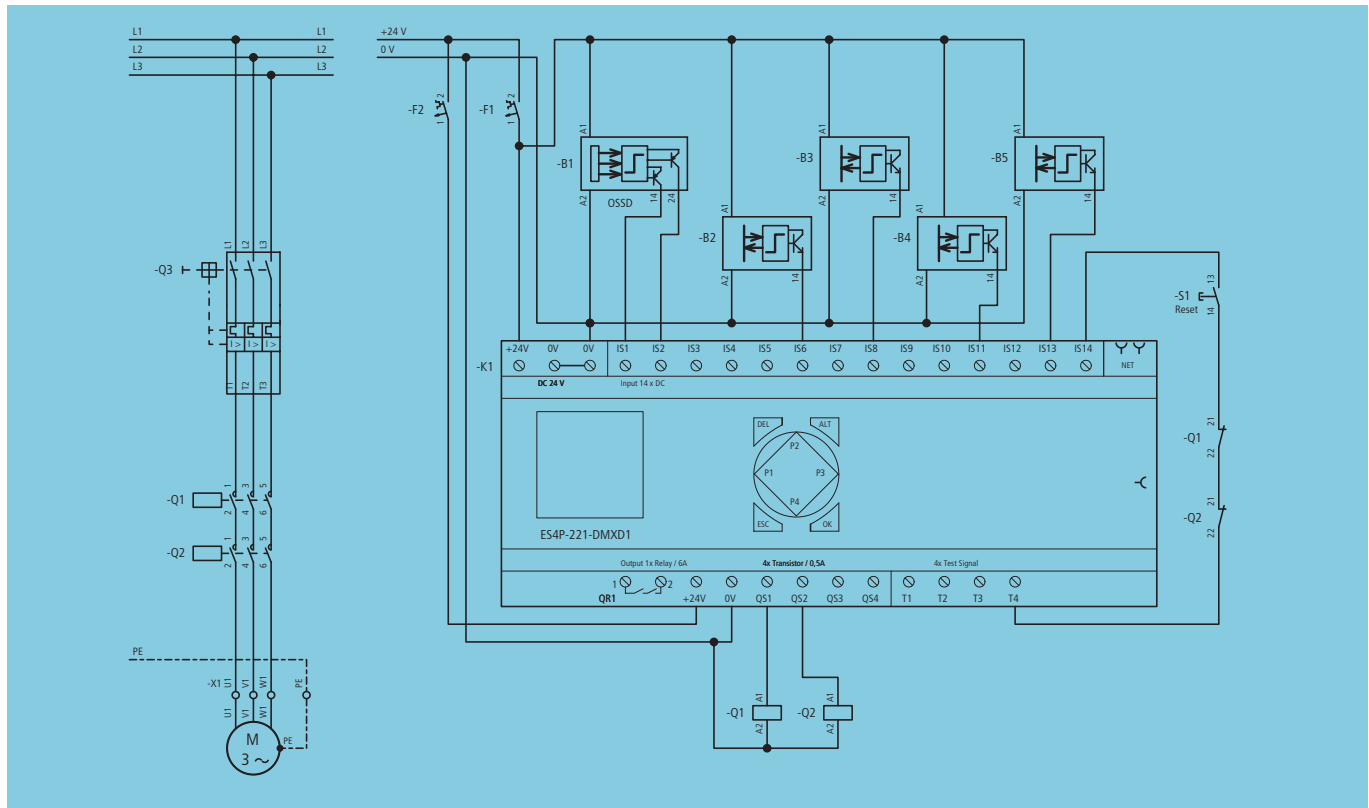


Figure 26: Electro-sensitive protective equipment with muting sensors on **easySafety**

Requirements

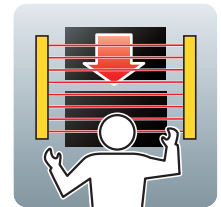
- Electro-sensitive protective equipment (ESPE) devices to IEC 61496-1.
- Active opto-electronic protective device (AOPDs) to IEC 61496-2.
- Observe positioning of safeguards with respect to the approach speeds of parts of the human body in accordance with DIN EN 999/ISO 13855
- Immediate disconnection of all hazardous movements in the safety clearance of the ESPE. Observe mounting instructions of manufacturer!
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Provide manual restart with **easySafety**.
- Position muting sensors so that only the transport conveyor pulse generates a valid muting sequence.
- Ensure during the muting state that persons cannot enter the hazardous area.
- Prevent collisions with transported goods by ensuring the protected installation of the ESPE.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Monitoring of redundant contactors via feedback loop.
- Single faults: Wire break, connection fault in control circuit device, supply conductor and **easySafety** relay are detected immediately or with the next start command.
- Distinguish between objects and persons by means of muting sensors.
- Muting sensors can be implemented with standard components.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

The muting function makes it possible to automatically bridge the safety function of the EPSE B1 for a specific time. This enables goods to be transported through the monitored area of the guard B1 without stopping the cyclical operation. Two groups of muting sensors arranged next to each other detect the beginning and the end of the movement through the protected area and start the monitoring of the maximum permissible muting time.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 4	Structure	SS D, symmetrical
MTTF _d	100 years	PFH _d	1.66×10^{-8}
B10 _d	Q1, Q2: 1300000	B10	Q1, Q2: 975000
n _{op}	1800	λ_d/λ	Q1, Q2: 0.75
CCF	80	C	0.3125
DC _{avg}	99 %	β	0.05
PL	e	DC	B1: 99 %, K1: 99 %, Q1, Q2: 99 %
T10 _d	> 20 years	SIL	3

Safety-related switching devices



Light curtain C4000, Manufacturer: Sick



easySafety ES4P-221-DMXD1
safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–
IEC 61496-1/-2	Safety of machinery – electro-sensitive protective equipment Part 1: General requirements and tests Part 2: Particular requirements for active opto-electronic protective devices	–
EN ISO 13855	Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body	–

4 Enabling safe operation

4.1 With two hand control type III C

Application

- For hazardous machine movements within reach under supervised operation: Both hands are restrained outside of the hazardous area.
- With machines with a high risk of injury, such as presses, cutting machines, manually fed punching machines.
- If the stopping time is less than the entry and access time.

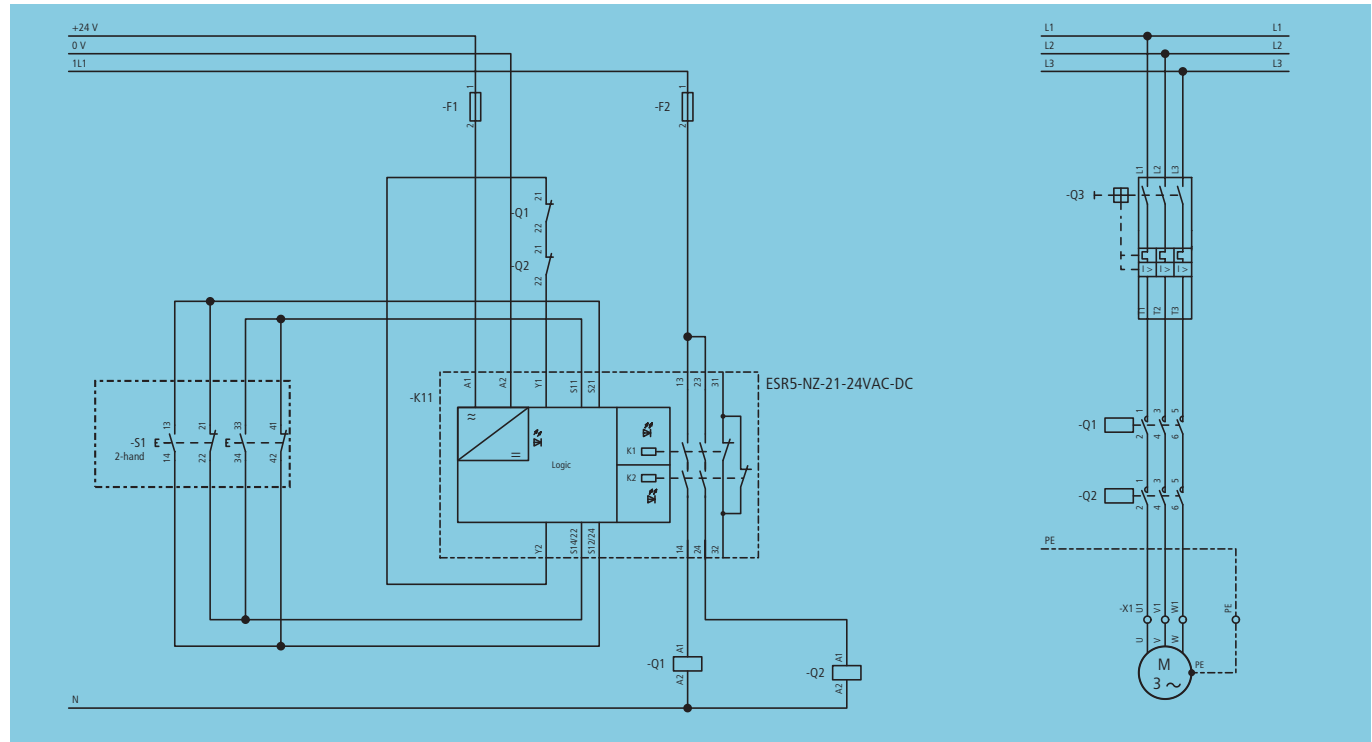


Figure 27: Two hand control type III C on ESR5

Requirements

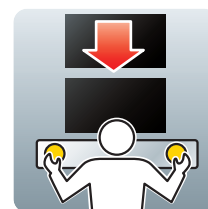
- Operation with a two-hand control device compliant with EN 574, type III C required.
- Arrange actuating devices in such a way that unintentional or intentional one-handed operation is not possible.
- Use actuating elements with positive opening to IEC 60947-5-1, Annex K.
- Two-channel circuitry must be implemented up to the operating elements (sensors/actuators) of the two-hand control station.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Sufficient clearance from the hazardous area must be ensured.

Properties

- Design with well-tried components and according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Both operating elements must be actuated within max. 0.5 seconds. If the time is exceeded, the release of both actuating elements is required before a starting is possible.
- If even one of the two actuating elements of the two-hand control is released during hazardous movement, the safety relay is de-energized and the enable paths open (uncontrolled stopping STOP category 0 to IEC 60204-1).
- Single faults: Wire break, connection fault and cross-circuit in control circuit device, supply conductor and safety relay are detected immediately or with the next start command.
- Monitoring of redundant contactors/safety valves via feedback loop.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

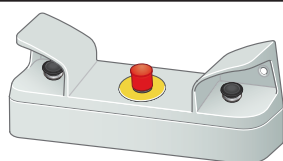
After the supply voltage is applied to the safety relay K1 (terminal A1-A2) the Power LED indicates operational readiness for activating the enable paths. Actuating the two-hand control S1 (both actuators pressed simultaneously within max. 0.5 seconds) causes first a check to be made on the rest position of contactors Q1 and Q2 via the N/C contacts of the feedback circuit. If this state is present, LEDs K1 and K2 indicate the

concurrent operation of the two-hand control. The not safety-related signal path of the safety relay is opened and the contactors are then actuated via the two closing enable paths.

Condition	EN ISO 13849
Structure	Cat. 4
MTTF _d	51.74 years
B10 _d	S1: 20000000, Q1, Q2: 1300000
n _{op}	18000
CCF	80
DC _{avg}	99 %
PL	e
T10 _d	K1: 5.7 years, all others: 20 years

Condition	IEC 62061
Structure	SS D, symmetrical
PFH _d	1.59 x 10 ⁻⁸
B10	S1: 4000000, Q1, Q2: 975000
λ _d /λ	S1: 0.2, Q1, Q2: 0.75
C	3.125
β	0.05
DC	99 %
SIL	3

Safety-related switching devices



22 mm mushroom actuator, installed in the two-hand control station to EN 574: M22-DP-Y + M22-AK11



Safety relays ESR5-NZ-21-24VAC-DC



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–
EN 574	Safety of machinery – Two-hand control devices – Functional aspects – Principles for design	114

Enabling safe operation

4.2 With two hand control type III C

Application

- For hazardous machine movements within reach under supervised operation: Both hands are restrained outside of the hazardous area.
- With machines with a high risk of injury, such as presses, cutting machines, manually fed punching machines.
- If the stopping time is less than the entry and access time.

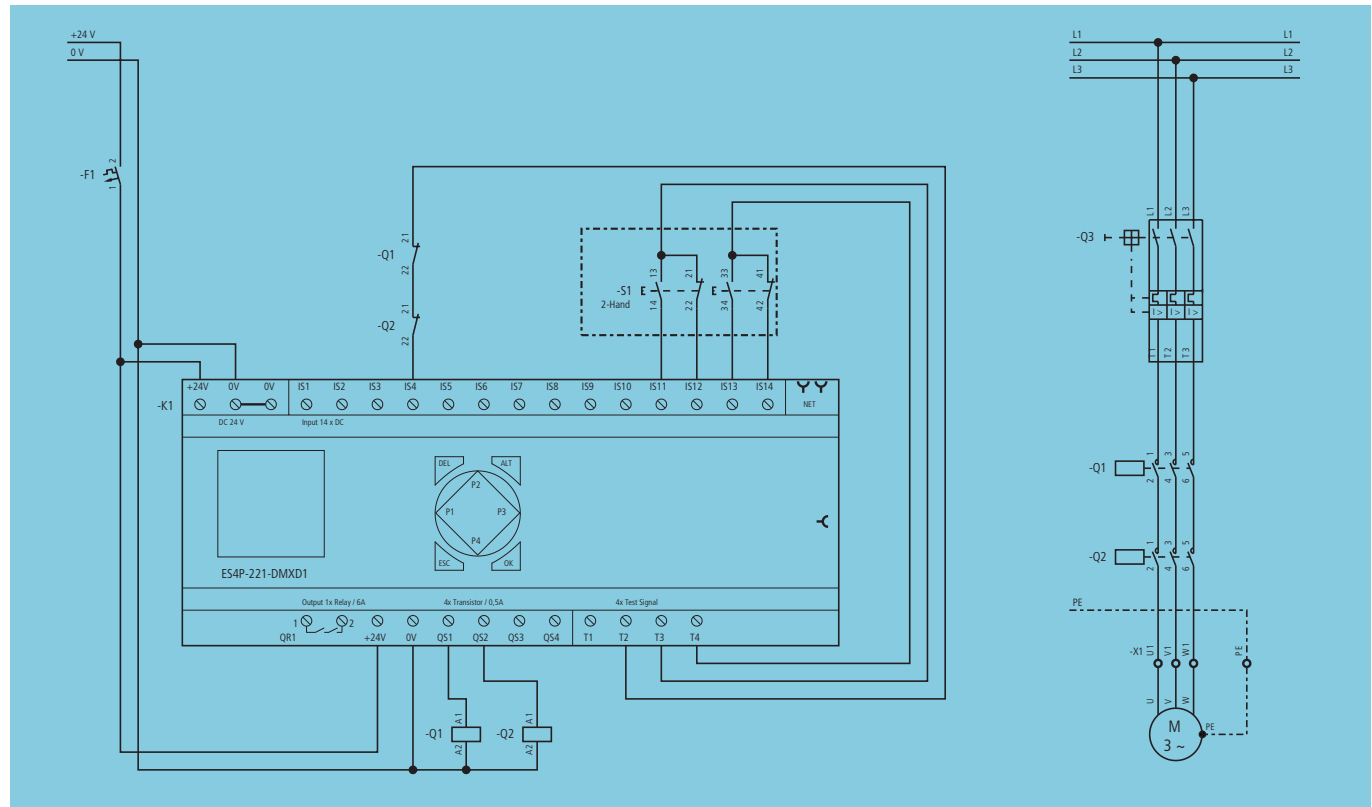


Figure 28: Two hand control type III C on **easySafety**

Requirements

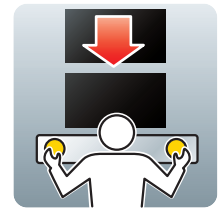
- Operation with a two-hand control device compliant with EN 574, type III C required.
- Arrange actuating devices in such a way that unintentional or intentional one-handed operation is not possible.
- Use actuating elements with positive opening to IEC 60947-5-1, Annex K.
- Two-channel circuitry must be implemented up to the operating elements (sensors/actuators) of the two-hand control station.
- Use inputs with different test signals.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Sufficient clearance from the hazardous area must be ensured.

Properties

- Design with well-tried components and according to basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Both operating elements must be actuated within max. 0.5 seconds. If the time is exceeded, the release of both actuating elements is required before a starting is possible.
- If even one of the two actuating elements of the two-hand control is released during hazardous movement, the safety relay is de-energized and the enable paths open (uncontrolled stopping STOP category 0 to IEC 60204-1).
- Single faults: Wire break, connection fault and cross-circuit in control circuit device, supply conductor and **easySafety** are detected immediately or with the next start command.
- Monitoring of redundant contactors/safety valves via feedback loop.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



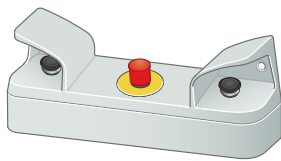
Function

Actuating the two-hand control S1 (both actuators pressed simultaneously within max. 0.5 seconds) causes the "Two-hand control Type III" (TH, two-hand button) safety function block to monitor the concurrent actuation of the two-hand control.

easySafety then checks the rest position of the two contactors Q1 and Q2 via the N/C contacts of the feedback circuit. If this state is also present, **easySafety** issues the enable signal via outputs QS1 and QS2. Both contactors pick up and switch on the hazardous drive.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 4	Structure	SS D, symmetrical
MTTF _d	100 years	PFH _d	1.33×10^{-8}
B10 _d	S1: 20000000, Q1, Q2: 1300000	B10	S1: 4000000, Q1, Q2: 975000
n _{op}	18000	λ _d /λ	S1: 0.2, Q1, Q2: 0.75
CCF	80	C	3.125
DC _{avg}	99 %	β	0.05
PL	e	DC	99 %
T10 _d	> 20 years	SIL	3

Safety-related switching devices



22 mm mushroom actuator, installed in the two-hand control station to EN 574: M22-DP-Y + M22-AK11



easySafety ES4P-221-DMXD1 safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–
EN 574	Safety of machinery – Two-hand control devices – Functional aspects – Principles for design	114

5 Enabling setting

5.1 With operating mode selector switch

Application

- For machines on which different operating modes are required, e.g.:
 - Setting operation with guard opened.
 - Jog mode
 - Free movement with light curtain muting
- On machine tools and manufacturing cells, such as presses, rotary tables and cutting machines.

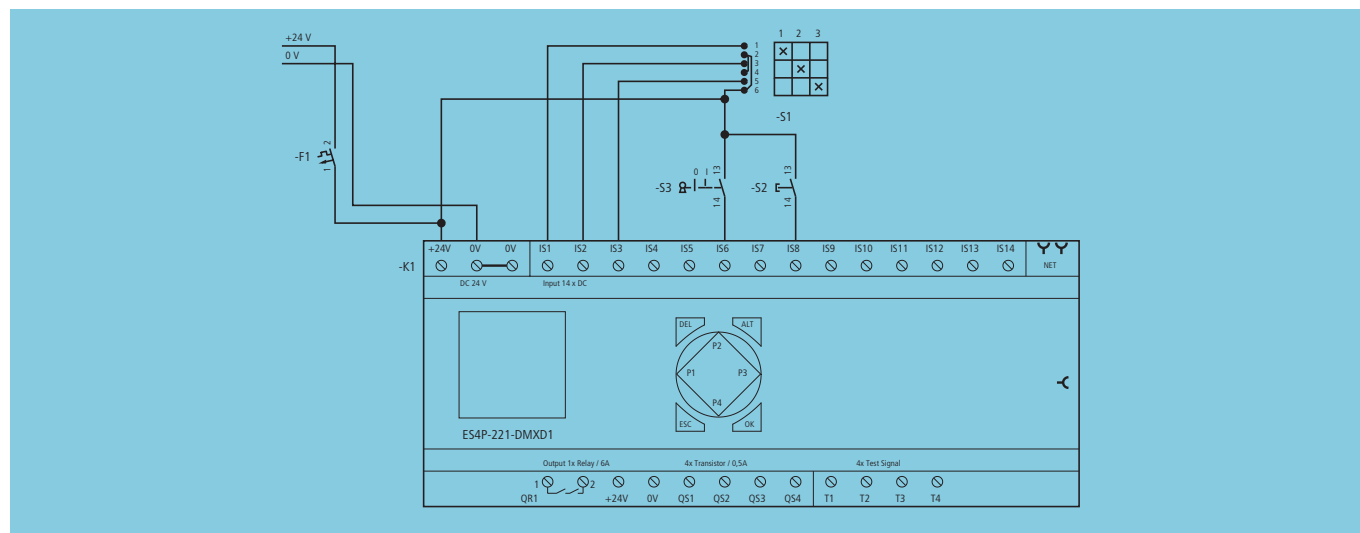


Figure 29: Safe operating mode selection with **easySafety**

Requirements

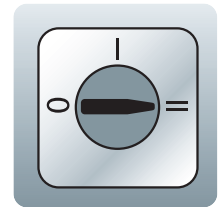
- Operating mode selection must not initiate a machine function.
- Operating mode selector switch must be protected against unauthorized, accidental actuation, e.g. by means of keyswitch (IEC 60204-1).
- Operating mode selector switch with positively opening contacts without overlapping contacting according to IEC 60947-5-1, appendix K.
- Additional measures for increasing safety must be provided, e.g.
 - Jog mode
 - Portable controlgear for setting work (dead man's switch).
 - Restricted range of movement.
 - Low speed.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- The simultaneous selection of two operating modes is excluded.
- Operating mode only accepted if the enable for operating mode change is present.



Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

Actuating the keyswitch S3 releases the "Operating mode switch" safety function block (OS, Operating mode switch) of the **easySafety**, thus allowing an operating mode change. The actual change is executed by selecting the mode on switch S1 and then accepting the mode by actuating S2.

Condition	EN ISO 13849	Condition	IEC 62061
Structure	Cat. 1	Structure	SS A, SSD symmetrical
MTTF _d	100 years	PFH _d	3.17×10^{-8}
B10 _d	2000000	B10	400000
n _{op}	3600	λ _d /λ	S1: 0.2
CCF	not relevant	C	0.625
DC _{avg}	not relevant	β	not relevant
PL	c	DC	not relevant
T10 _d	> 20 years	SIL	1

Safety-related switching devices



TO-2-8241/E operating mode selector switch



easySafety ES4P-221-DMXD1
safety control relay



M22-WRS + M22-AK10 keyswitch

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: Specification for general requirements	92
IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–

6 Combining several safety functions

6.1 Stopping in an emergency (Emergency-stop disconnection)

Application

When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).

- When hazards to the operator and the machine can occur
- requiring a performance level up to PL_r e.

→ The Emergency-stop function is an additional safety function. It is not permissible as a sole means of protection!

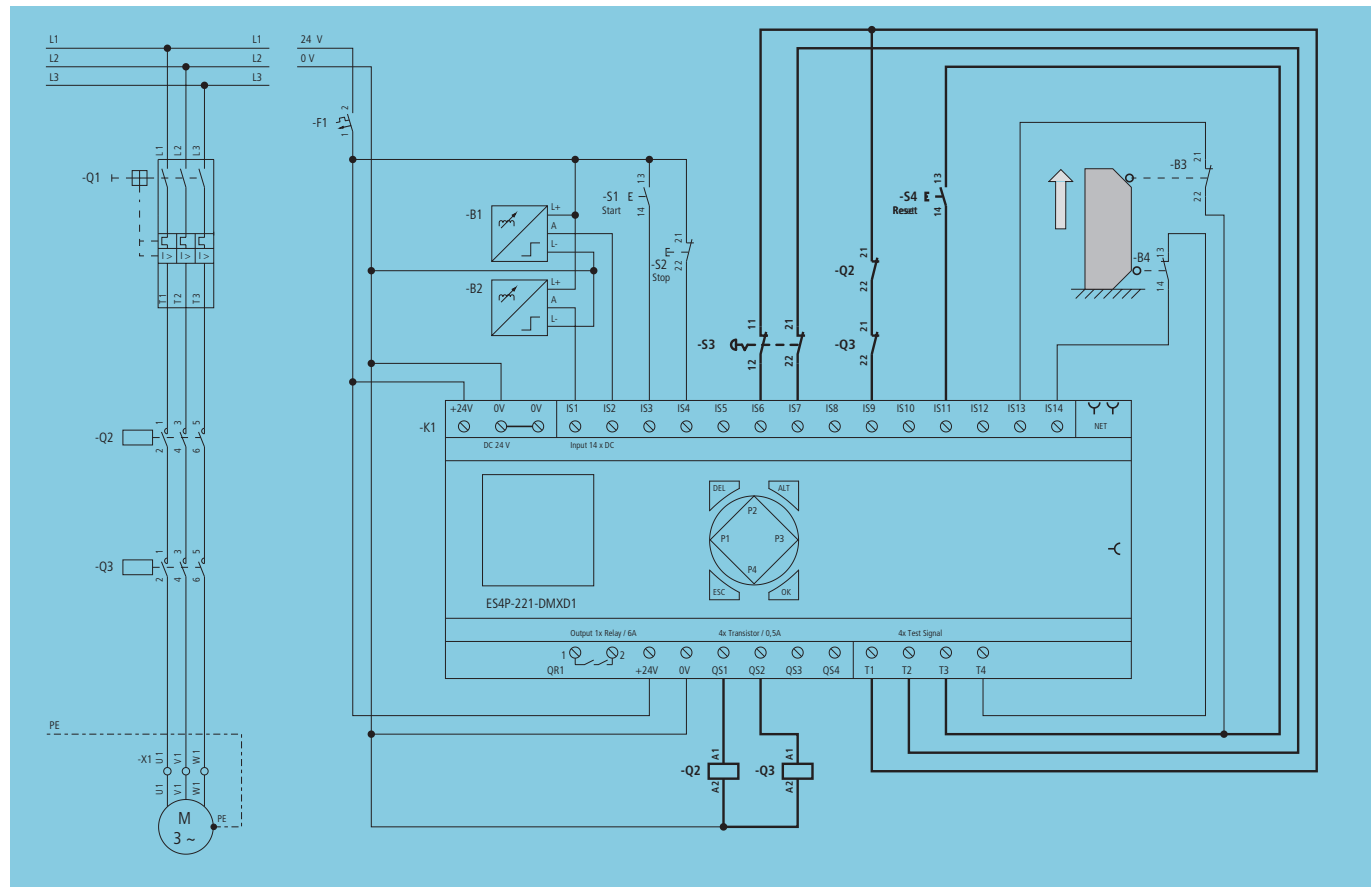


Figure 30: Two-channel emergency stop function with **easySafety**

Requirements

- Emergency-stop actuator with positive opening to IEC 60947-5-1, Annex K, and wire function with two-channel circuit and with cross-circuit detection on **easySafety** to EN ISO 13850.
- Use inputs with different test signals.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Acknowledgement required after releasing of Emergency-stop actuator.
- Activate hazardous movements after enable with separate Start command.
- Document exchange interval for contactors (case B).
- Take into account the load on the contactors, i.e. also that of the movable guard, 6.2 "Monitoring a movable guard", page 60.
- Case A: Unrestricted utilization period.
- Case B: Exchange contactors after 4.5 years.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Control circuit device, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break, connection fault are detected immediately or with the next start command.



Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

When the emergency-stop actuator S3 is actuated, the **easySafety**-outputs QS1 and QS2 are deactivated and the contactor coils Q2 and Q3 wired to them are disconnected. Acknowledgement required after Emergency-stop actuator is released by actuating pushbutton S4.

Condition	EN ISO 13849		Condition	IEC 62061	
	Case A	Case B		Case A	Case B
Structure	Cat. 4	Cat. 4	Structure	SS D, symmetrical	SS D, symmetrical
MTTF _d	100 years	40, 38 years	PFH _d	5.22×10^{-9}	2.2×10^{-7}
B10 _d	S3: 100000, Q2, Q3: 1300000	S3: 100000, Q2, Q3: 1300000	B10	S3: 20000, Q2, Q3: 975000	S3: 20000, Q2, Q3: 975000
n _{op}	S3: 360, Q2, Q3: 2520	S3: 360, Q2, Q3: 288720	λ _d /λ	S3: 0.2, Q2, Q3: 0.75	S3: 0.2, Q2, Q3: 0.75
CCF	80	80	C	S3: 0.0625, Q2, Q3: 0.4375	S3: 0.0625, Q2, Q3: 50.125
DC _{avg}	99 %	99 %	β	0.05	0.05
PL	e	e	DC	S3: 99 %, K1: 99 %, Q2, Q3: 99 %	S3: 99 %, K1: 99 %, Q2, Q3: 99 %
T10 _d	> 20 years	Q2, Q3: 4.5 years, all others: > 20 years	SIL	3	2

Safety-related switching devices



Emergency-stop actuator
M22-PVT45P-MPI + M22-A + M22-CK02



easySafety ES4P-221-DMXD1
safety control relay



DILM12 contactors

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
EN ISO 13850	Safety of machinery – Emergency-stop equipment – Principles for design	111
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1 IEC 60947-5-1 IEC 60947-5-5	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices Part 5-5: Emergency-stop devices with mechanical latching	–

Application

- When hazards could arise for the operator due to intervention in the hazardous area.
- For cyclical interventions in the hazardous area.
- If the stopping time is greater than the entry and access time.

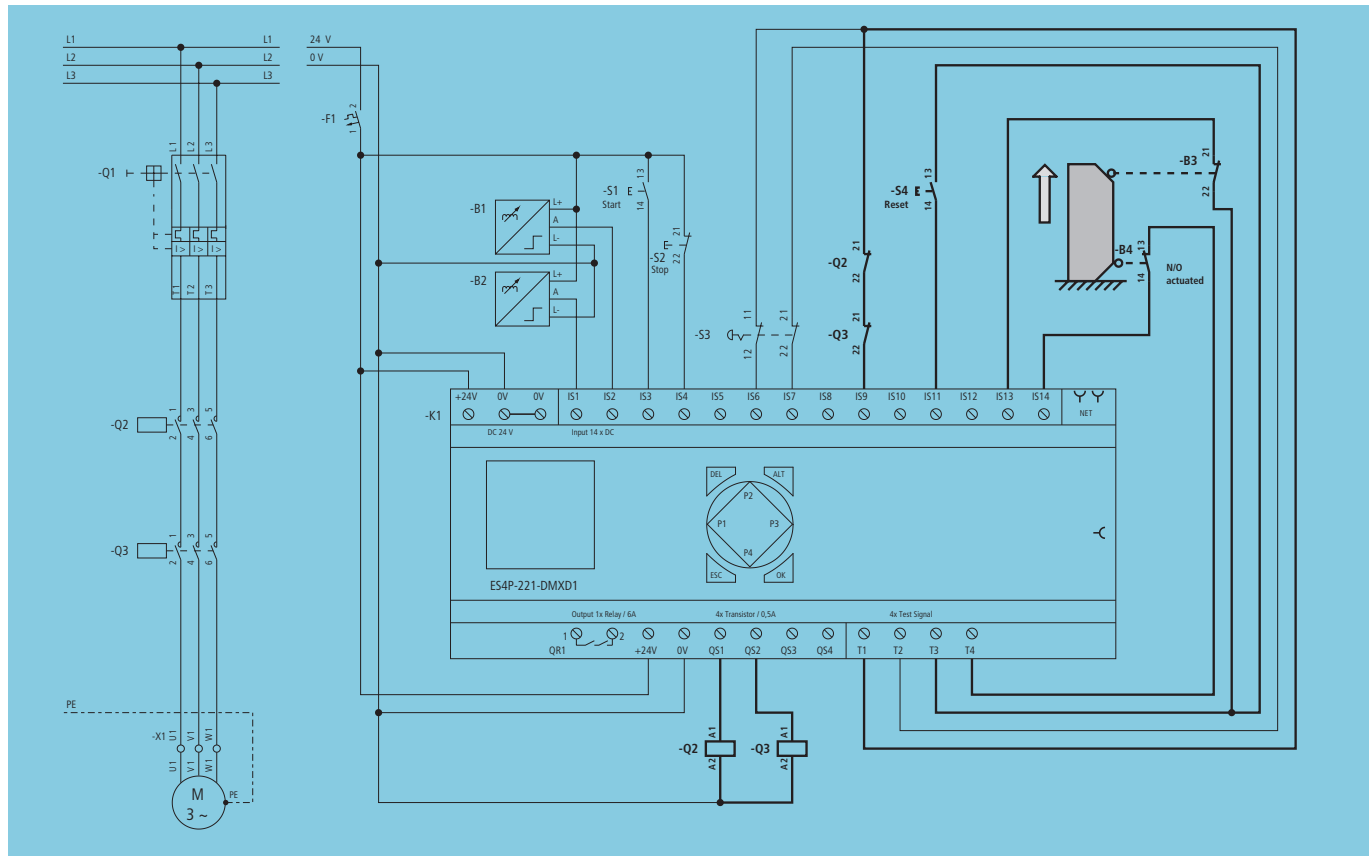


Figure 31: Two-channel safety device with **easySafety**

Requirements

- Use position switches with positive opening to IEC 60947-5-1, Annex K, and function to ISO 14119.
- Use inputs with different test signals.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Document exchange interval for contactors (case B).
- Take into account the load on the contactors, i.e. also that of the Emergency-stop function, 6.1 "Stopping in an emergency (Emergency-stop disconnection)", page 58.
- Case A: Unrestricted utilization period.
- Case B: Exchange contactors after 4.5 years, position switches with N/O contact after 3.5 years.
- Acknowledgement required after guard is closed.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Position switch, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break, connection fault are detected immediately or with the next start command.
- Only category 3 reached due to high number of switch operations (case B).

Function

The guard door must be in a closed position (N/C and N/O contact B3 and B4 closed) for the enable signal to be issued. The feedback loop of the N/C contacts can ensure the normal position of the disconnection contactors Q2 and Q3. If the status is present, the enable can be issued by actuating the RESET button S4. The QS1 and QS2 outputs of the **easySafety** switch and Q3 pick up and their looped back signalling

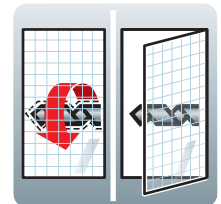


Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



contacts open. Opening the guard causes the **easySafety** outputs QS1 and QS2 to disconnect and thus de-energize the enable paths. The safety

control function is restored to operational readiness by the reclosed N/C contact.

Condition	EN ISO 13849 Case A	Case B
Structure	Cat. 4	Cat. 3
MTTF _d	100 years	29.89 years
B10 _d	B3: 20000000, B4: 1000000, Q2, Q3: 1300000	B3: 20000000, B4: 1000000, Q2, Q3: 1300000
n _{op}	B3, B4: 1800, Q2, Q3: 2520	B3, B4: 288000, Q2, Q3: 288720
CCF	80	80
DC _{avg}	99 %	99 %
PL	e	e
T10 _d	> 20 years	B4: 3.5 years, Q2, Q3: 4.5 years, alle anderen: > 20 years

Condition	IEC 62061 Case A	Case B
Structure	SS D asymmetrical and symmetrical	SS D asymmetrical and symmetrical
PfH _d	2.91 x 10 ⁻⁹	3.48 x 10 ⁻⁷
B10	B3: 4000000, B4: 500000, Q2, Q3: 975000	B3: 4000000, B4: 500000, Q2, Q3: 975000
λ _d /λ	B3: 0.2, B4: 0.5, Q2, Q3: 0.75	B3: 0.2, B4: 0.5, Q2, Q3: 0.75
C	B3, B4: 0.3125, Q2, Q3: 0.4375	B3, B4: 50, Q2, Q3: 50.125
β	0.05	0.05
DC	B3, B4: 99 %, K1: 99 %, Q2, Q3: 99 %	B3, B4: 99 %, K1: 99 %, Q2, Q3: 99 %
SIL	3	2

Safety-related switching devices



LS-11, LS-02 position switch



easySafety ES4P-221-DMXD1 safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1 IEC 60947-5-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices	–
ISO 14119	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	108

Combining several safety functions

6.3 Speed monitoring with easySafety

Application

- When the immediate disconnection of the power supply does not cause hazardous states (uncontrolled stopping – STOP category 0 to EN ISO 13850).
- When hazards to the operator and the machine occur due to overspeed.

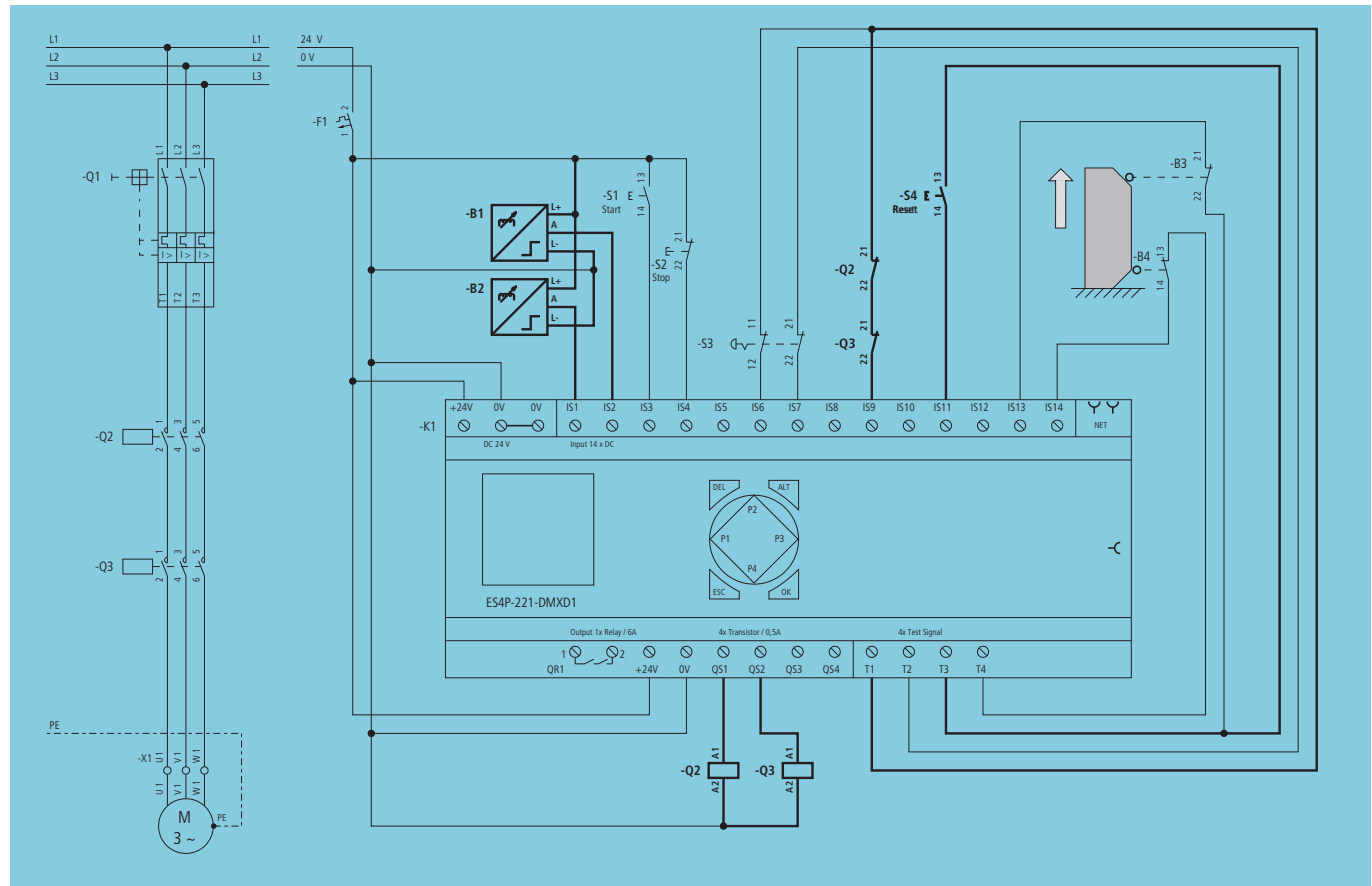


Figure 32: Speed monitoring with easySafety

Requirements

- Speed measuring with redundant safety speed sensors.
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.
- Document exchange interval for contactors (case B).
- Take into account the load on the contactors, i.e. also that of the Emergency-stop function, 6.1 "Stopping in an emergency (Emergency-stop disconnection)", page 58.
- Case A: Unrestricted utilization period.
- Case B: Exchange contactors after 4.5 years.
- Acknowledgement required after guard is closed.
- Observe additional applicable standards, e.g. IEC 60204-1.

Properties

- Design with basic and well-tried safety principles (EN ISO 13849-1 and EN ISO 13849-2)
- Proximity sensors, supply conductor and command processing are redundant and self-monitoring.
- Single faults: Wire break and connection are detected reliably by means of the measuring principle. Observe mounting instructions of manufacturer!

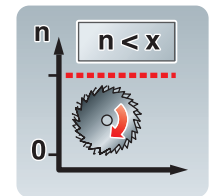


Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		



Function

When the limit speed configured in the **easySafety** is reached, the overspeed monitoring function block (OM, Overspeed monitor) removes the enable of the safety outputs QS1 and QS2 and thus de-energizes the contactors Q2 and Q3. The N/C contacts in the feedback circuit can

be used to determine whether the contactors have returned to their rest position before a renewed enable signal is issued by actuating the RESET button S4.

Condition	EN ISO 13849	
	Case A	Case B
Structure	Cat. 3	Cat. 3
MTTF _d	50.93 years	24.01 years
B10 _d	Q2, Q3: 1300000	Q2, Q3: 1300000
n _{op}	Q2, Q3: 2520	Q2, Q3: 288720
CCF	80	80
DC _{avg}	91.1 %	95.27 %
PL	e	d
T10 _d	20 years	Q2, Q3: 4.5 years, all others: > 20 years

Condition	IEC 62061	
	Case A	Case B
Structure	SS D, symmetrical	SS D, symmetrical
PFH _d	1.55 x 10 ⁻⁸	2.3 x 10 ⁻⁷
B10	Q2, Q3: 975000	Q2, Q3: 975000
λ _d /λ	Q2, Q3: 0.75	Q2, Q3: 0.75
C	Q2, Q3: 0.4375	Q2, Q3: 50.125
β	0.05	0.05
DC	B1, B2: 99 % K1: 99 % Q2, Q3: 99 %	B1, B2: 99 % K1: 99 % Q2, Q3: 99 %
SIL	3	2

Safety-related switching devices



Proximity sensor E57-...



easySafety ES4P-221-DMXD1
safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 13849-1/2	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design Part 2: Validation	106
IEC 62061	Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems	107
IEC 60947-4-1	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor starters; electromechanical contactors and motor starters	–

7 Preventing restarts

7.1 With contactors

Application

- When an automatic Restart causes hazardous conditions when the voltage is restored.
- When faulty behaviour of the electrical equipment occurs due to voltage failure.

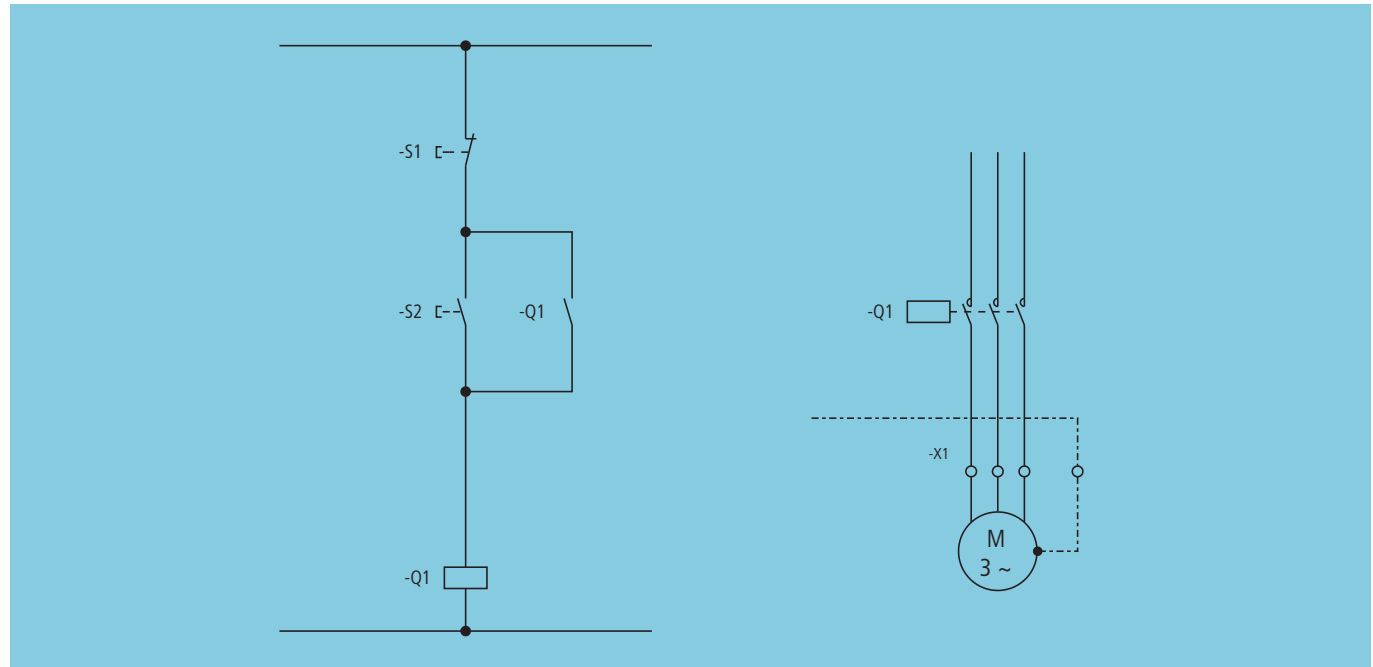


Figure 33: Contactor self-switching prevents automatic restart with voltage recovery

Requirements

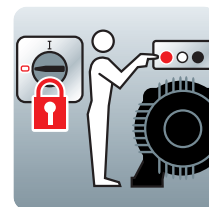
- Contactors must have an operating voltage tolerance of between 85 % to 110 % of the control voltage in accordance with IEC 60947-1.
- Power supply and protective device according to IEC 60204-1, paragraph 9.1.1.

Properties

- Control voltage dips up to -15 % do not lead to disconnection.

Function

When the voltage is restored, the machine only starts with an intentional start command.



Well-tried switchgear



DILM12 contactor



DILM25 contactor



DILM50 contactor



DILM150 contactor

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 60947-1	Low-voltage switchgear and controlgear – Part 1: General rules	–

Preventing restarts

7.2 With easySafety

Application

- When an automatic Restart causes hazardous conditions when the voltage is restored.
- When faulty behaviour of the electrical equipment occurs due to voltage failure.

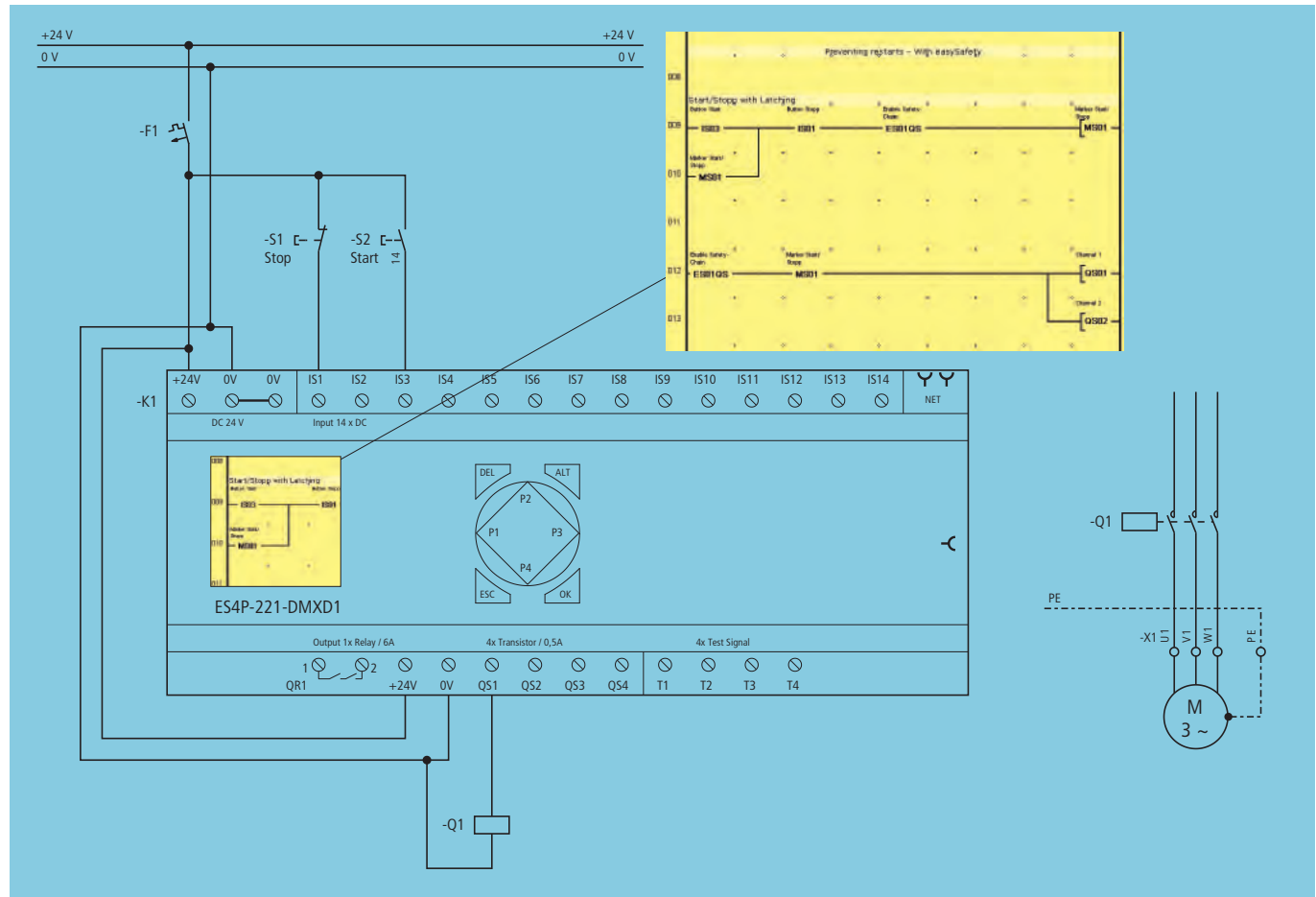


Figure 34: Self-switching with **easySafety** prevents automatic restart with voltage recovery

Requirements

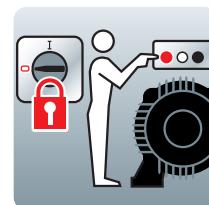
- Ensure that the AST parameter setting of a safety function block never causes the unexpected startup of the machine or an uncontrolled change in the speed of the machine.
- Contactors must have an operating voltage tolerance of between 85 % to 110 % of the control voltage in accordance with IEC 60947-1.
- Hard wire with electromechanical components.

Properties

- Control voltage dips up to -15 % do not lead to disconnection.
- Mode parameter allows the startup behaviour of each safety function block to be set: AST – automatic start, MST – manual start, CST – controlled start.

Function

The Mode parameter enables you to set the startup behaviour of the safety function block. The restart prevents uncontrolled starting after the power supply is switched on and after the protected area is enabled. If a manual restart is still required, the self maintaining function in the circuit diagram can be programmed (see programming window).



Well-ried switchgear



easySafety ES4P-221-DRXD1 safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 60947-1	Low-voltage switchgear and controlgear – Part 1: General rules	–

Preventing restarts

7.3 With feedback circuits

Application

- If a fault in disconnection circuit may cause loss of the safety function.

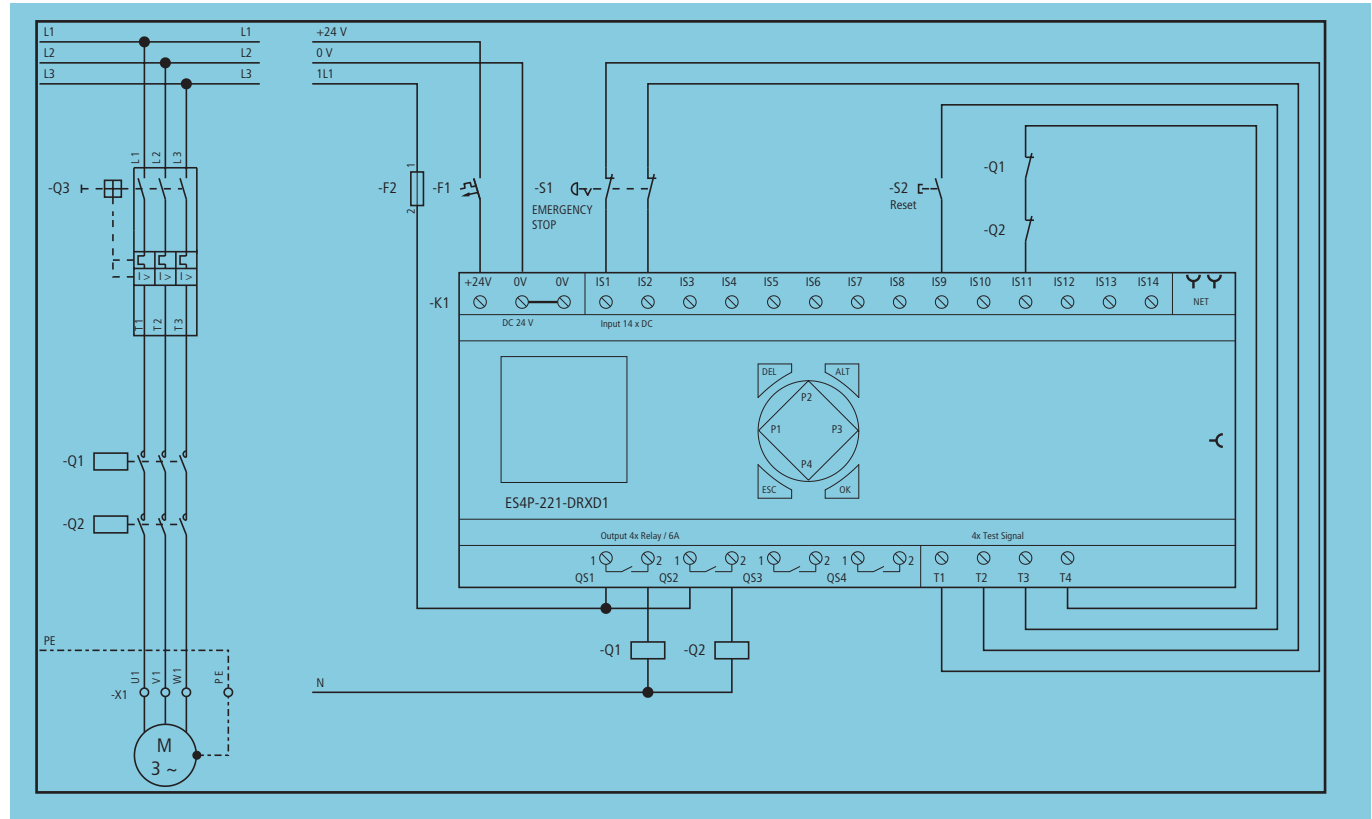


Figure 35: Feedback circuit (loop) prevents restart by open contactor contacts

Requirements

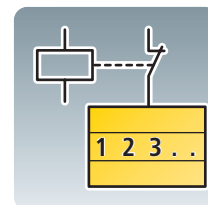
- Install redundant contactors and with mechanically linked and feedback contacts.
- Hard wire with electromechanical components.

Properties

- If the contactors are switched on, **easySafety** checks whether the feedback circuit closes within the monitoring time.
- If the contactors are switched off, **easySafety** checks whether the feedback circuit closes within the monitoring time.

Function

The EM (External Monitor) safety function block checks the signalling contacts of the contactor. If a contactor does not return to the rest position on disconnection, the function block does not issue the enable signal and prevents the restart.



Well-tried switchgear



easySafety ES4P-221-DRXD1 safety control relay



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 60947-1	Low-voltage switchgear and controlgear – Part 1: General rules	–

8.1 For short interventions

- When during maintenance an unexpected startup of the machine or part of the machine can cause a hazard.

- For switching off parts of an installation for minor work over a short time.

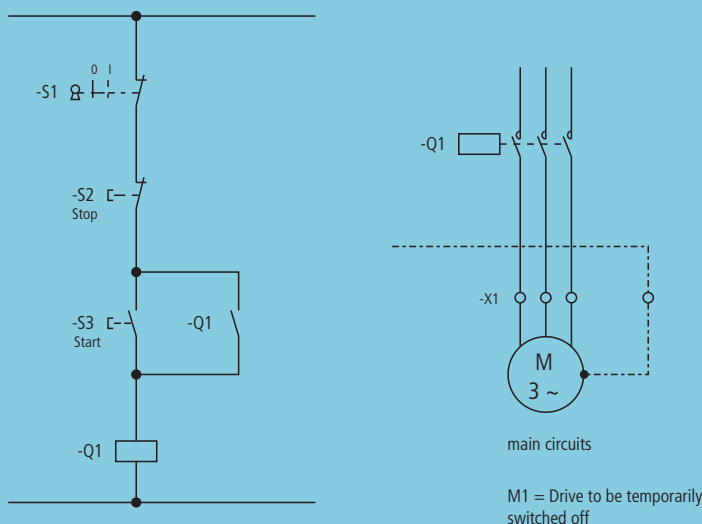


Figure 36: Prevention of unexpected startup by keyswitch

- For work without significant dismantling of the machine (IEC 60204-1)
- For adjustments requiring a relatively short time (IEC 60204-1).
- For work on the electrical equipment if
 - there is no hazard arising from electric shock or burns (IEC 60204-1).
 - the means of disconnection cannot be negated by the work (IEC 60204-1).
 - the work is of a minor nature (IEC 60204-1).
- Positively opening switch with two ON and OFF switch positions.
- Lockable in the OFF position
- Contactor must be switched in normal operation so that a failure can be detected.

- Partial disconnection that is protected against restart.

The keyswitch is locked in the OFF position for maintenance work. An unexpected starting by another person during work in the hazardous area is thus not possible.



Well-ried switchgear



M22-WRS + M22-AK10 keyswitch



DILM12 contactor

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
EN 1037 (ISO 14118)	Safety of machinery – Prevention of unexpected startup	112
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 60947	Low-voltage switchgear	–

9 For repair and maintenance safety

9.1 With power disconnecting device (main switch)

Application

- When hazards could arise for the operator or machine due to unexpected startups.
- For isolating the electrical installation.
- For circuits requiring a mains disconnection device in accordance with IEC 60204-1.

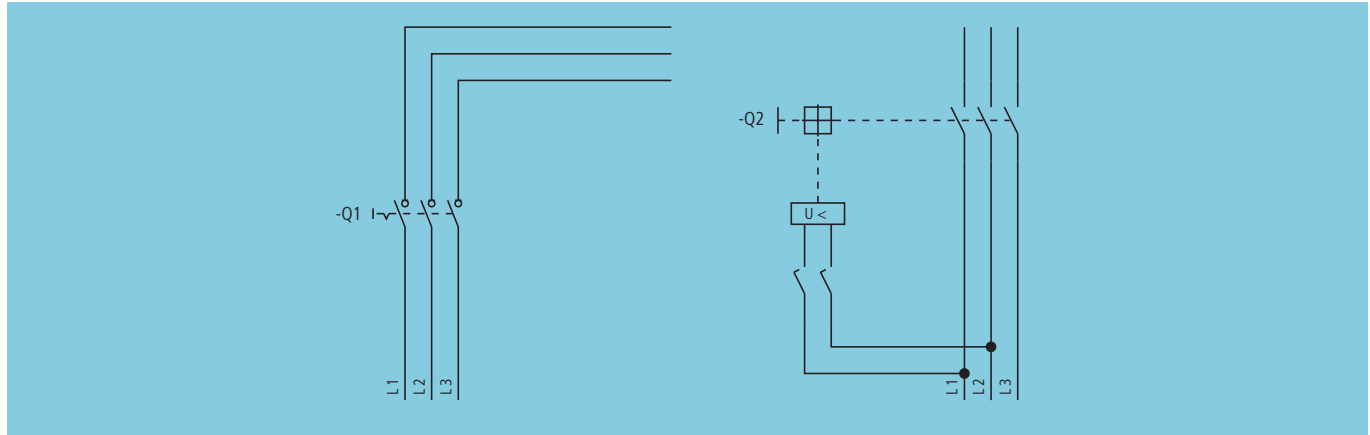


Figure 37: Switch-disconnector and circuit-breaker as power disconnecting device (main switch)

Requirements

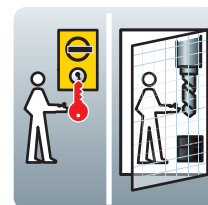
- The power disconnecting device (main switch) must be one of the following types:
 - Switch disconnector in accordance with IEC 60947-3 for utilization category AC-23B or DC-23B.
 - Circuit-breaker in accordance with IEC 60947-2, suitable for isolation.
 - Switch-disconnector in accordance with IEC 60947-3 with auxiliary contact for load disconnection before the main contacts open.
 - Plug and socket combination in accordance with IEC 60204-1 (5.3.2. e) for machines with flexible cables.
- Switch with two switch positions: ON and OFF and intermediate position TRIPPED if required.
- Lockable in OFF position, e. g. via padlocks.
- If in a multiple supply system the disconnection of only one power disconnecting device leads to hazardous conditions, the common disconnection via mechanical interlocks or undervoltage releases must be forced.
- Observe regulations concerning arrangement and assembly in accordance with IEC 60204-1 and IEC 60947!

Properties

- One power disconnecting device (main switch): Isolation of the entire system from the power supply.
- Multiple supply: Isolation of particular circuits from the power supply, e.g. automatic, central disconnection.
- Implements the first 2 of the 5 safety rules in accordance with EN 50110-1 (VDE 0105):
 - 1. Isolate.
 - 2. Secure against reclosing.
 - 3. Verify isolation from the supply.
 - 4. Short-circuit and ground.
 - 5. Cover or enclose neighbouring units that are live.

Function

The hazardous electrical installation is isolated and secured against reclosing via the main switch.



Well-tried switchgear



P1-25/E switch-disconnectors



Circuit-breaker NZMN2-A200 with toggle lever locking device

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
EN 1037 (ISO 14118)	Safety of machinery – Prevention of unexpected startup	112
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 60947-1	Low-voltage switchgear and controlgear – Part 1: General rules	–

For repair and maintenance safety

9.2 With devices for isolating the electrical equipment

Application

- For work without the risk of an electric shock.
- For prevention of unexpected startups.
- When parts of the machine must remain functional.

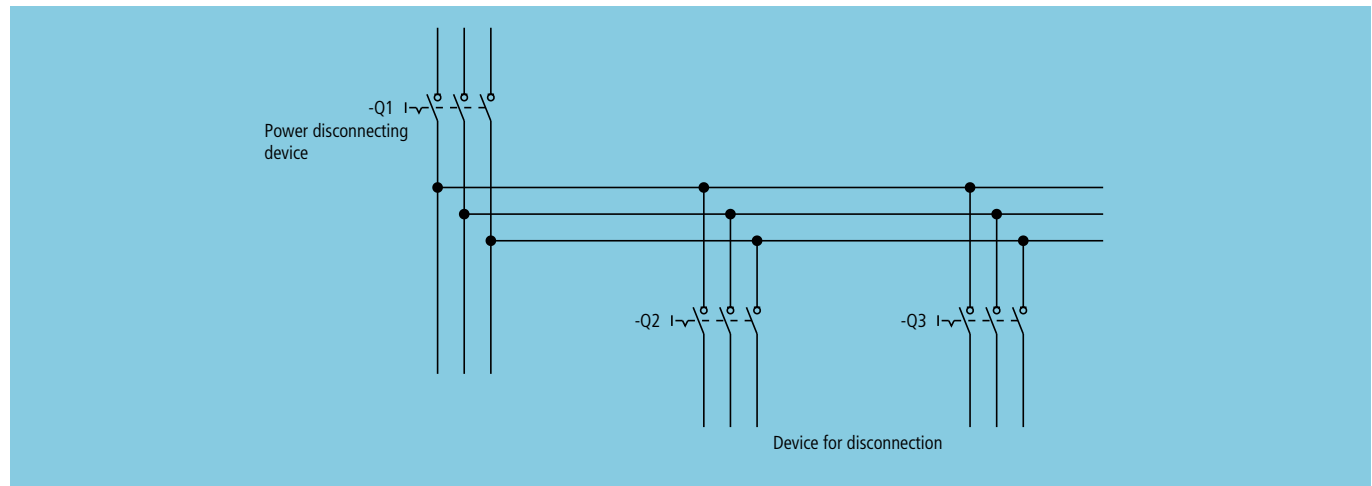


Figure 38: Devices for disconnection of allowed partial isolation

Requirements

- The power disconnecting device (main switch) must be one of the following types:
 - Switch disconnecter in accordance with IEC 60947-3 for utilization category AC-23B or DC-23B.
 - Circuit-breaker in accordance with IEC 60947-2, suitable for isolation.
 - Switch-disconnector in accordance with IEC 60947-3 with auxiliary contact for load disconnection before the main contacts open.
 - Plug and socket combination in accordance with IEC 60204-1 (5.3.2. e) for machines with flexible cables.
- Switch with two switch positions: ON and OFF and intermediate position TRIPPED if required.
- Lockable in OFF position, e. g. via padlocks.
- Observe regulations concerning arrangement and assembly in accordance with IEC 60204-1 and IEC 60947!
- Use a power disconnection with switch position indication to IEC 60947-1.

Properties

- Isolation of individual parts of the electrical equipment from the mains.
- Isolating characteristics allow unhindered work on the electrical and mechanical equipment as opposed to indirect shut-down with the aid of a contactor.
- Implements the first 2 of the 5 safety rules in accordance with EN 50110-1 (VDE 0105):
 - 1. Isolate.
 - 2. Secure against reclosing.
 - 3. Verify isolation from the supply.
 - 4. Short-circuit and ground.
 - 5. Cover or enclose neighbouring units that are live.

Function

The switch-disconnectors isolate hazardous electrical parts of the installation and prevent them from restarting.



Well-tried switchgear



P1-25/E switch-disconnectors



Circuit-breaker NZMN2-A200 with toggle lever locking device

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
EN 1037 (ISO 14118)	Safety of machinery – Prevention of unexpected startup	112
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 60947-1	Low-voltage switchgear and controlgear – Part 1: General rules	–

9.3 With repair, maintenance and safety switch

Application

- For isolating the electrical installation or parts of it.
- For prevention of unexpected startups.

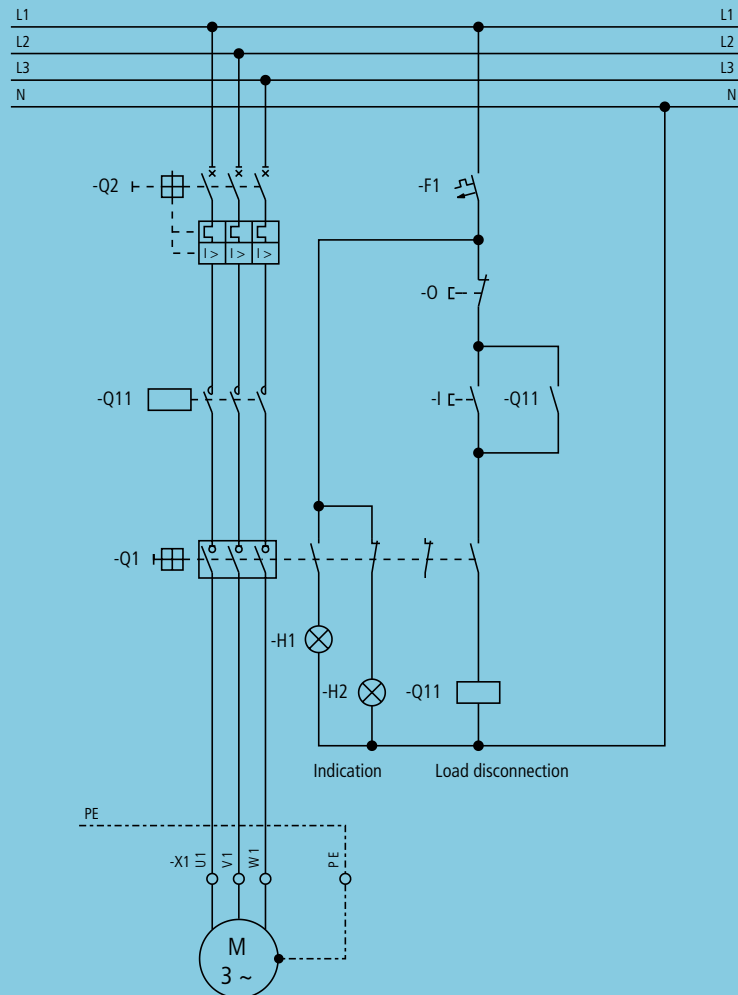


Figure 39: Switch-on prevention by safety switch

Requirements

- Observe regulations concerning arrangement and assembly in accordance with IEC 60204-1 and IEC 60947!
- Use a power disconnection with switch position indication to IEC 60947-1.



Properties

- Isolation of the entire system from the power supply
→ chapter 9.1 "With power disconnecting device (main switch)", page 82
- Isolation of individual sections of the installation from the power supply → safety switch/maintenance switch.
- Implements the first 2 of the 5 safety rules in accordance with EN 50110-1 (VDE 0105):
 - 1. Isolate.
 - 2. Secure against reclosing.
 - 3. Verify isolation from the supply.
 - 4. Short-circuit and ground.
 - 5. Cover or enclose neighbouring units that are live.

Function

The switch-disconnectors isolate hazardous electrical parts of the installation. Each electrical fitter can protect himself from unauthorized restarts by means of a padlock.

Well-tried switchgear



P1-25/I2-SI/HI11-SW

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
EN 1037 (ISO 14118)	Safety of machinery – Prevention of unexpected startup	112
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 60947-1	Low-voltage switchgear and controlgear – Part 1: General rules	–

10 Protection against electric shock

10.1 Protective isolation

Application

- Protection against indirect contact, i.e. in the event of insulation faults.
- Photoelectric circuits for maintenance work in control panels.
- Power supply for devices used in switchboards during maintenance work (e.g. meters, laptops)

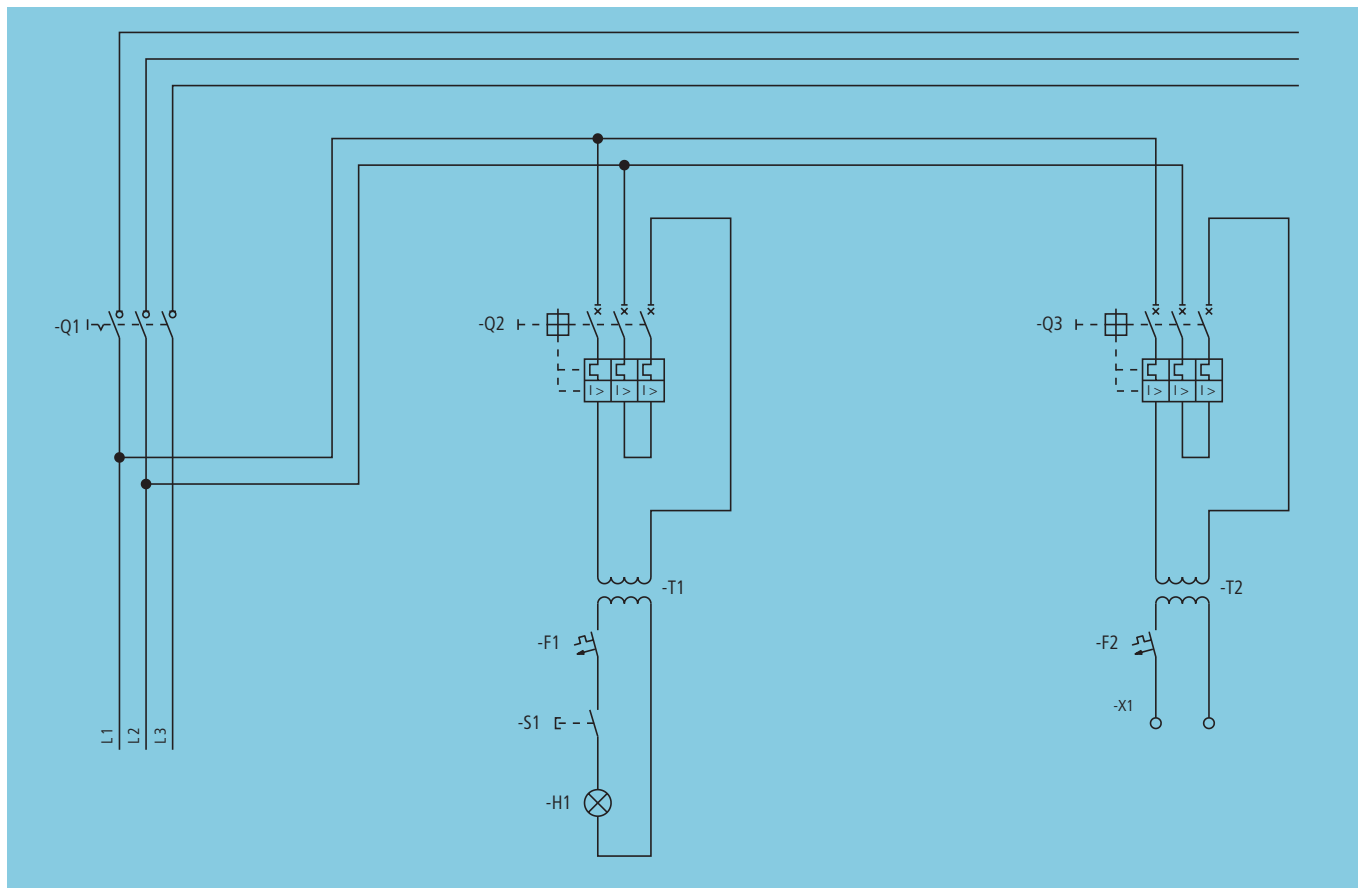


Figure 40: Protective isolation

Requirements

- Isolating transformer to IEC 61558-2-4.
- Safely insulated windings (reinforced or double insulation) to IEC 61558-2-6.
- Circuit downstream of the isolating transformer must remain ungrounded.
- Normally only for one load.
- Secondary voltage not more than 250 V.
- Observe special cabling requirements when tapping upstream of the main switch, e.g. short-circuit proof cabling, conductor colors, etc.

Properties

- Protection against electric shock with simultaneous contact with a conductive part and a grounded component.
- Protection against electric shock with simultaneous contact of the earth potential and conductive components which are live due to an insulation fault.
- Simultaneous contact of both conductors causes electric shock.

Function

The isolating transformers provide a control voltage that is galvanically isolated from the main circuit.



Well-ried switchgear



Single-phase control transformer, isolating transformer, safety transformer ST10,63(400/24)

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 61558-2-4	Safety of power transformers, power supply units and similar – Particular requirements for isolating transformers for general use	–
IEC 61558-2-6	Safety of power transformers, power supply units and similar – Particular requirements for safety isolating transformers for general use	–

Protection against electric shock

10.2 PELV extra low voltage with safe isolation

Application

- PELV extra low voltage with safe isolation

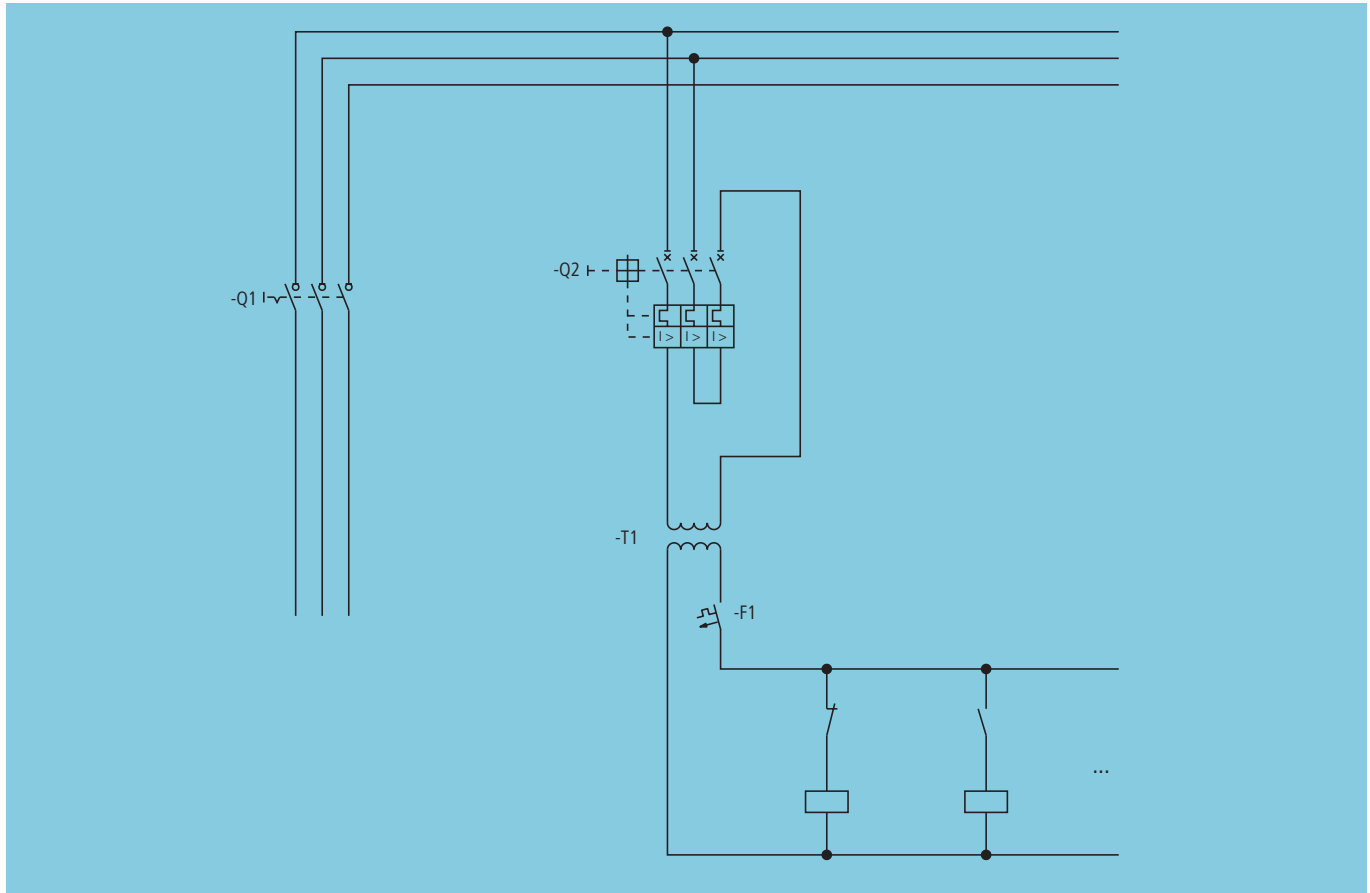


Figure 41: PELV extra low voltage with safe isolation

Requirements

- Safety transformer to IEC 61558-2-6.
- Safely insulated windings (reinforced or double insulation).
- Circuit downstream of the safety transformer must be grounded.
- Secondary voltage with AC not more than 25 V, with DC not over 60 V.

Function

The safety transformer provides a control voltage that is isolated from the main circuit.

Properties

- Protection against electric shock with simultaneous contact with a conductive part and a grounded component.
- PELV is double insulated. In the event of an insulation fault, the conductive part is not energized.
- Protection against electric shock with simultaneous contact of both conductors.



Well-tried switchgear



Single-phase control transformer, isolating transformer, safety transformer ST10,63(400/24)

Safety standards

Standard	Contents	→ page
EN ISO 12100	Safety of machinery – Basic terms, general principles for design Part 1: Basic terminology, methodology Part 2: Technical principles	103
IEC 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	92
IEC 61558-2-4	Safety of power transformers, power supply units and similar – Particular requirements for isolating transformers for general use	–
IEC 61558-2-6	Safety of power transformers, power supply units and similar – Particular requirements for safety isolating transformers for general use	–

11 Machine engineering in accordance with IEC 60204-1

11.1 Power supply and protection devices

The reliability of the protective function does not only depend on the equipment and circuitry selected. Other factors and interrelationships should also be taken into account.

Weld-free design

Open the circuit, "switch off" the hazard – this is not possible with welded contacts.

If the switching device is for safety purposes, a risk evaluation may make overdimensioning or redundancy necessary ("Feedback Circuit", page 96).

Try to ensure that the protective device trips in the event of a short-circuit or overcurrent before the contacts of the switching devices weld. The protective device should naturally also be able to withstand the motor startup or the switching on of transformers.

Design the control circuit correctly

A short-circuit in the control circuit can cause uncontrolled states. In the worst case this may cause the failure of the safety functions. This may either cause

- contacts to weld or
- the short-circuit current to cause the tripping of the short-circuit protective device.

In both cases, the correct choice of short-circuit protective device and the transformer is critical.

Section 7.2.10 in IEC 60204-1 stipulates that protective devices should be weld-free: "When selecting those protective devices, consideration shall be given to the protection of switching devices against damage due to overcurrents (for example welding of the switching device contacts).

You should therefore choose the lowest value for the maximum permissible overcurrent protective device specified for the switching devices used.

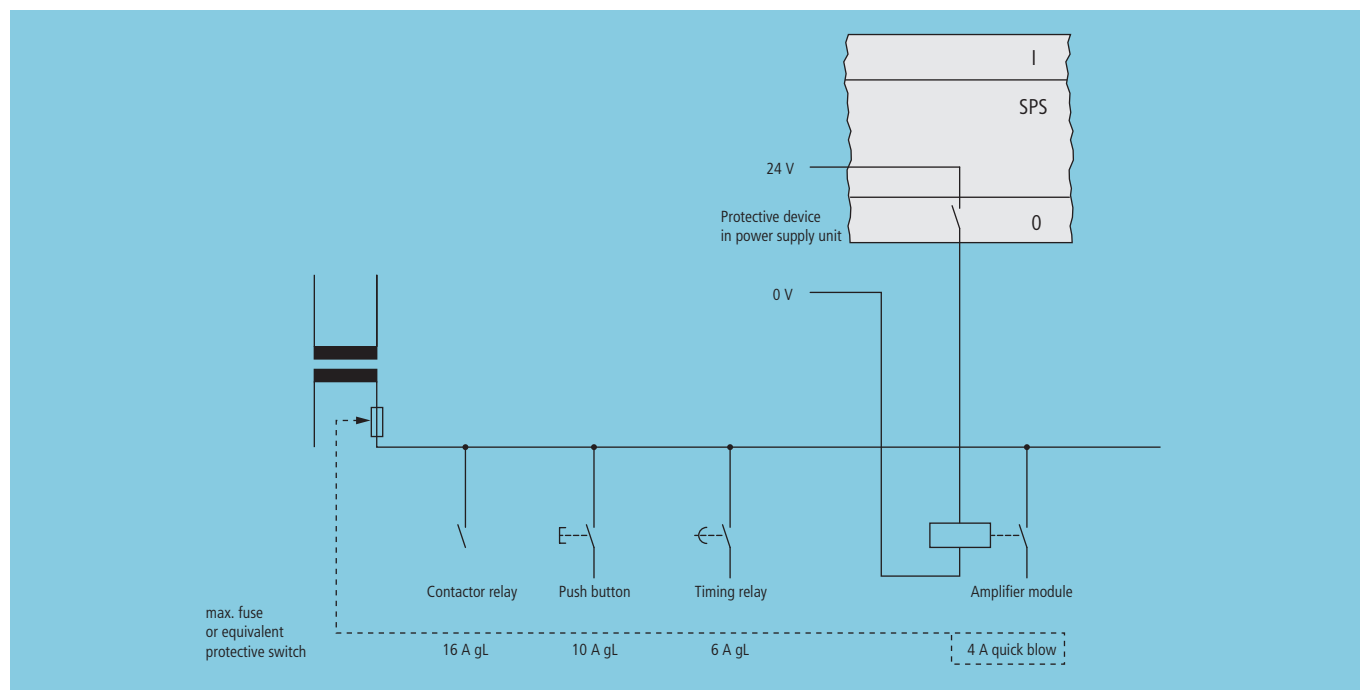


Figure 42: Use of a fuse as a protective device

Ensure that the prospective short-circuit current in your control circuits does not exceed 1000 A. Switching devices in accordance with EN 60947-5-1 are protected against welding up to this maximum value by means of the protective devices specified.

The limitation of the prospective short-circuit current can be achieved through the use of:

- Transformers
- Protective device and cable length/cross section

Using transformers

The use of transformers for the supply of control circuits is required for almost all machines. Except for the following: Machines with a single motor starter and a maximum of two external control devices.

Protective device and cable length/cross section

The protective device should respond quickly in the event of a short-circuit.

When selecting the protective device, you must ensure that in the event of a short-circuit, the breaking current is reached within 0.2 s.

- Determine therefore the short-circuit current value, taking the following factors into account:
 - Transformer.
 - Cable length.
 - Conductor cross-section.
- Then select a short-circuit protective device with a maximum response value lower than the short-circuit current value. Use the following equations for the calculation:

Calculation of the secondary short-circuit current

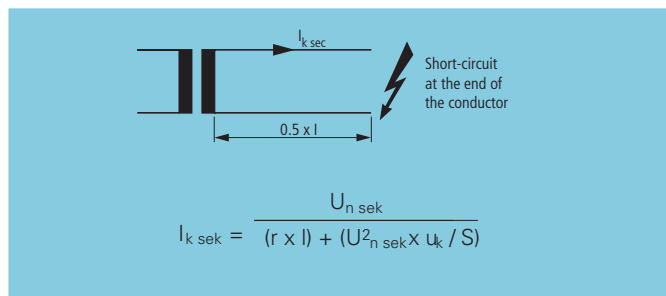


Figure 43: Calculation of the short-circuit current

Control transformer STI

- $I_{k \text{ sek}}$ = Secondary short-circuit current in A
- $U_{n \text{ sek}}$ = Rated secondary voltage of transformer in V
- u_k = Short-circuit voltage of the transformer in %
- S_n = Rated power (rating) of transformer in kVA

- l = Cable length of secondary circuit in km
- r = Resistance per unit length of the single core cable in Ω/km
- $r = 24.5 \Omega/\text{km}$ for $0.75 \text{ mm}^2 \text{ Cu}$
- $r = 18.1 \Omega/\text{km}$ for $1.0 \text{ mm}^2 \text{ Cu}$
- $r = 12.1 \Omega/\text{km}$ for $1.5 \text{ mm}^2 \text{ Cu}$

Determination of the short-circuit protective device

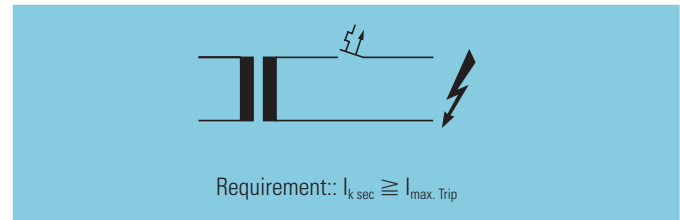


Figure 44: Determination of short-circuit devices

- Tripping values of miniature circuit-breaker for 0.2 seconds

Catalog No.	Characteristic	max. response current of short-circuit release
FAZ	B	$3 - 5 \times I_n$
FAZ	CSA	$5 - 10 \times I_n$
FAZ	D	$10 - 20 \times I_n$

- Fuse

Find the disconnection current at 0.2 seconds on the time-current characteristic curve for the fuse concerned.

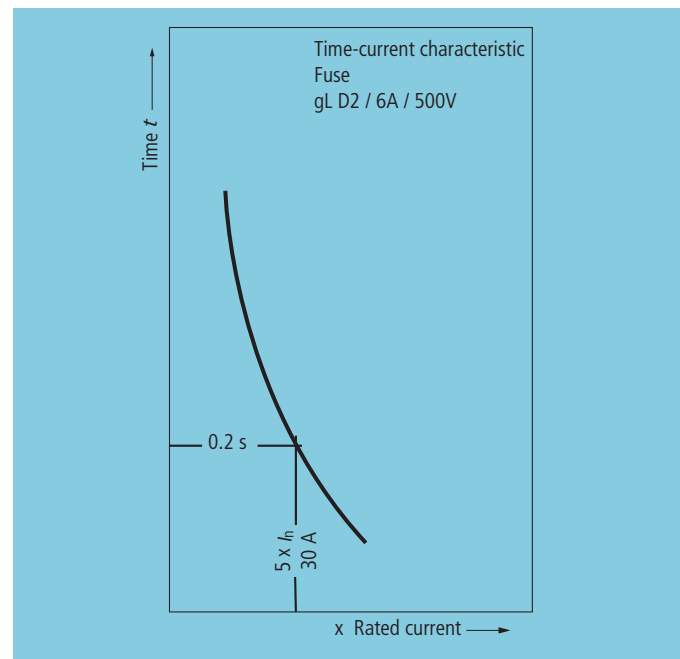


Figure 45: Example: Time-current characteristic of a 6 A fuse

Machine engineering in accordance with IEC 60204-1

11.2 Long control cables

Switching contactors over long multiple control cables

The capacitance of long control conductors in AC circuits may impede contactors from dropping out in response to an Emergency-stop command. This is particularly the case of:

- High control voltage (e.g. 500 V).
- Low contactor sealing current.
- Contactors with very low drop-out voltages U_a (IEC 60947-4-1: $10\% < U_a < 75\%$)

The control conductor must therefore not exceed a maximum length l_{\max} for a given control voltage and contactor size, otherwise the capacitance of the control conductors will prevent the contactor from switching off due to the sealing current present.

Maximum cable length l_{\max}

The actual conductor capacitance C must be less than C_{\max} in order to ensure trouble-free switching of a contactor. With continuous contacts the capacitance C must be expected and with pulse contacts $2 \times C$. In the latter case, the maximum length of the control conductor l_{\max} is therefore only half the length as for continuous contact.



Figure 46: Two-wire control (left) and three-wire (pulsed) control

Using a guide value for the specific cable capacitance of $0.3 \text{ } 0.3 \text{ } \mu\text{F/km}$ of a 2-core control cable, the maximum permissible control cable length at 50 Hz is:

Two-wire control:

$$l_{\max} = 1.7 \times 10^6 \frac{P_H}{U_c^2} [\text{m}]$$

Three-wire (pulsed) control:

$$l_{\max} = 0.85 \times 10^6 \frac{P_H}{U_c^2} [\text{m}]$$

P_H = Rated sealing power in VA

U_c = Rated operating voltage in V

The following table shows the maximum single control conductor length for Eaton contactors. Rated operating voltage: 230 V and 120 V (max. $1.1 \times U_c$).

Table 2: Control conductor length for Eaton contactors

Contactor type	Maximum permissible cable length in m for ...			
	Two-wire control 50 Hz	Three-wire control 50 Hz	Two-wire control 60 Hz	Three-wire control 60 Hz
$U_c = 230 \text{ V}$				
DILE(E)...; S(E)00	148	74	118	59
DILM7 - DILM15; DILA	129	64	103	51
DILM17 - DILM32	257	129	206	103
DILM40 - DIL65	514	257	411	206
DILM80; DILM95	836	418	668	334
DILM115; DIL150	112	56	90	45
DILM185 - DILM250	138	69	111	55
DILM300 - DILM500	138	69	111	55
$U_c = 120 \text{ V}$				
DILE(E)...; S(E)00	543	272	434	217
DILM7 - DILM15; DILA	472	236	378	189
DILM17 - DILM32	944	472	756	378
DILM40 - DIL65	1889	944	1511	756
DILM80; DILM95	3069	1535	2456	1228
DILM115; DIL150	413	207	331	165
DILM185 - DILM250	508	254	406	203
DILM300 - DILM500	508	254	406	203



Remedy if the contactor does not drop out

If during the engineering phase or during commissioning it is determined that the contactors do not drop out due to the long control conductor lengths involved, use the following methods to solve the problem:

- Use a larger contactor (higher sealing power)
- Reduce the control voltage (allow for voltage drop).
- Use a DC actuated contactor.
- The coil is shorted by means of an additional N/C contact for two-wire control and N/O contact for three-wire control. An additional cable is required for this. The disconnection times of the contactors will increase considerably.

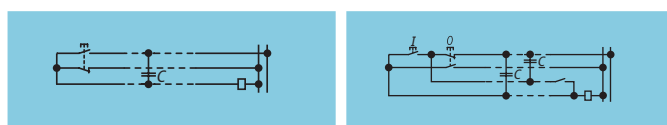


Figure 47: Increasing the disconnection times with two-wire control (left) and three-wire control.

- Parallel connection of a resistive load to the contactor coil. The resistance is determined with the following equation:

$$R = \frac{1000}{C} [\Omega]$$

The rating for the resistor is:

$$P = \frac{U_C^2}{R} [W]$$

Remember that the resistor contributes to the total heat dissipation of the circuit.

Use well-tries circuit designs and components.

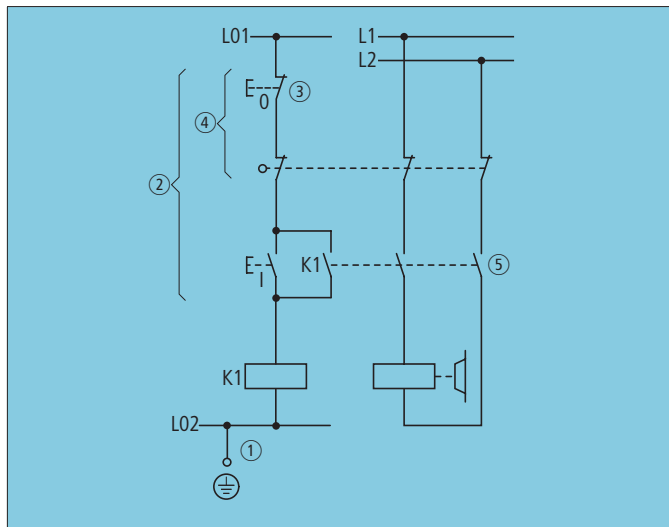


Figure 48: Proven circuit design

- ① Ground the control current circuit.
- ② Connect all switch functions to the ungrounded end.
- ③ Disconnect by de-energizing to ensure fail-safe operation.
- ④ Use switches with positively opening contacts (do not confuse with positively driven operation).
- ⑤ Switch all active cables to the controlling device.

Feedback Circuit

Insert an N/C contact for each of the subsequent contactors at the location of the “feedback circuit” for additional enable paths or for monitoring redundant contactors. The N/C contacts must be suitable as mirror contacts in accordance with IEC 60947-4-1, Annex F. If one of these contactors welds, the circuit stays in the rest state with the next ON command until the fault is rectified. See circuits on page 22, 56 and 78.

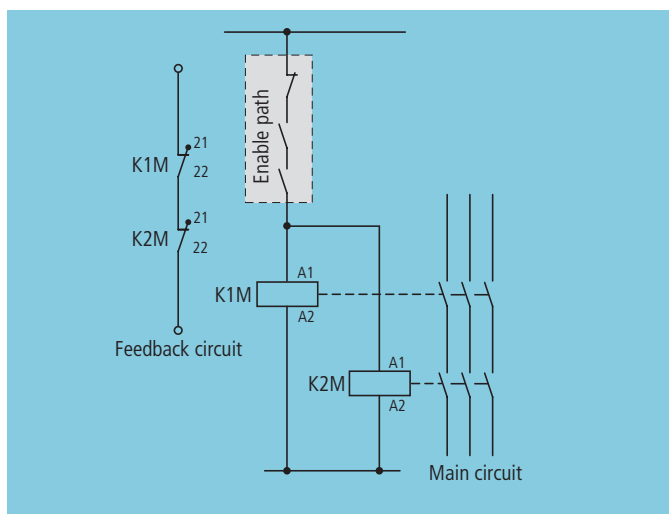


Figure 49: Feedback circuit, monitor external contactors

Provide redundancy

Redundancy means that more components than required for normal operation are provided. A typical form of redundancy is the double provision of contactor relays in the Emergency-stop combination, such as → chapter 1.7 “With electronically controlled drives”, page 24

If one of the devices fails because it is not energized or is blocked, the other device establishes the safe condition and the fault is detected. This, however, can only be carried out with positively driven auxiliary contacts.

Ensure diversity

This involves the design of control circuits using different function principles or with different types of components, such as the combination of N/C and N/O contacts that are actuated by the protective devices → chapter 2.5 “Two-channel with safety relay”, page 44.

Carry out function tests

The control system should carry out the function tests automatically in the best case. Many functions cannot be tested automatically. For example, an Emergency-stop actuator is only actuated in the event of an emergency. Carry out individual function tests at appropriate intervals.

Arrange devices effectively

Refer to the requirements of “ISO 14119”, page 108 concerning the arrangement of position switches.

Use safety switching devices and programmable electronic safety control relays

Safety switching devices are components of the protective equipment on machines and plants. Their use reduces the risk for the protection of persons, material and machines.

The decision whether to use a conventional or an electronically programmable safety device depends on the application at hand. A conventional safety switching device is an effective solution for simple applications. Contact expansion modules enable safety-related enabling paths to be reproduced cost effectively (→ figure 50, page 97).

With complex tasks, an electronically programmable control relay can offer an extensive range of functions. The flexible programming allows you to implement different safety-related functions and safety categories.

The entire machine or system control is normally implemented separately in a non-safety section with conventional PLC technology and a safety-related section with safety switching devices or control relays.

Prevent foreseeable misuse

Machines are reset for operation as soon possible after malfunctions.

Example: Packages, pallets or machine parts jam inside a palletizing machine. After an Emergency-stop the machine should restart. The operator therefore goes to the danger zone and tries to rectify the fault. For this situation, the drive may possibly have to start in the opposite direction.

If this is only possible by manually operating the contactors, there is a high risk of danger. The wrong drive may be started or the wrong rotation direction may be selected.

The implementation of the features required by the standards is not enough. More foresighted planning in cooperation between machine designers and electrical engineers is required.

Possible measures are:

- Consideration of the environmental conditions with the placement of control panels, operating elements and indication elements.
- Extended functions with the setting mode:
 - Jog operation for the operation of drives.
 - With additional selection of the direction of rotation.
 - Startup function with incorrect start position.
- Marker function for continued unhindered operation after stop.
- Display of the stored actual situation.
- Faults should be detectable from a safe location: Extended indication functions.
- From a safe location, it must be possible to simultaneously observe the critical machine movements and the indicating instruments while being able to operate the control elements.
- After reset of an action in an emergency (emergency-stop command), the machine must not restart automatically. The Start command must occur via a separate pushbutton.

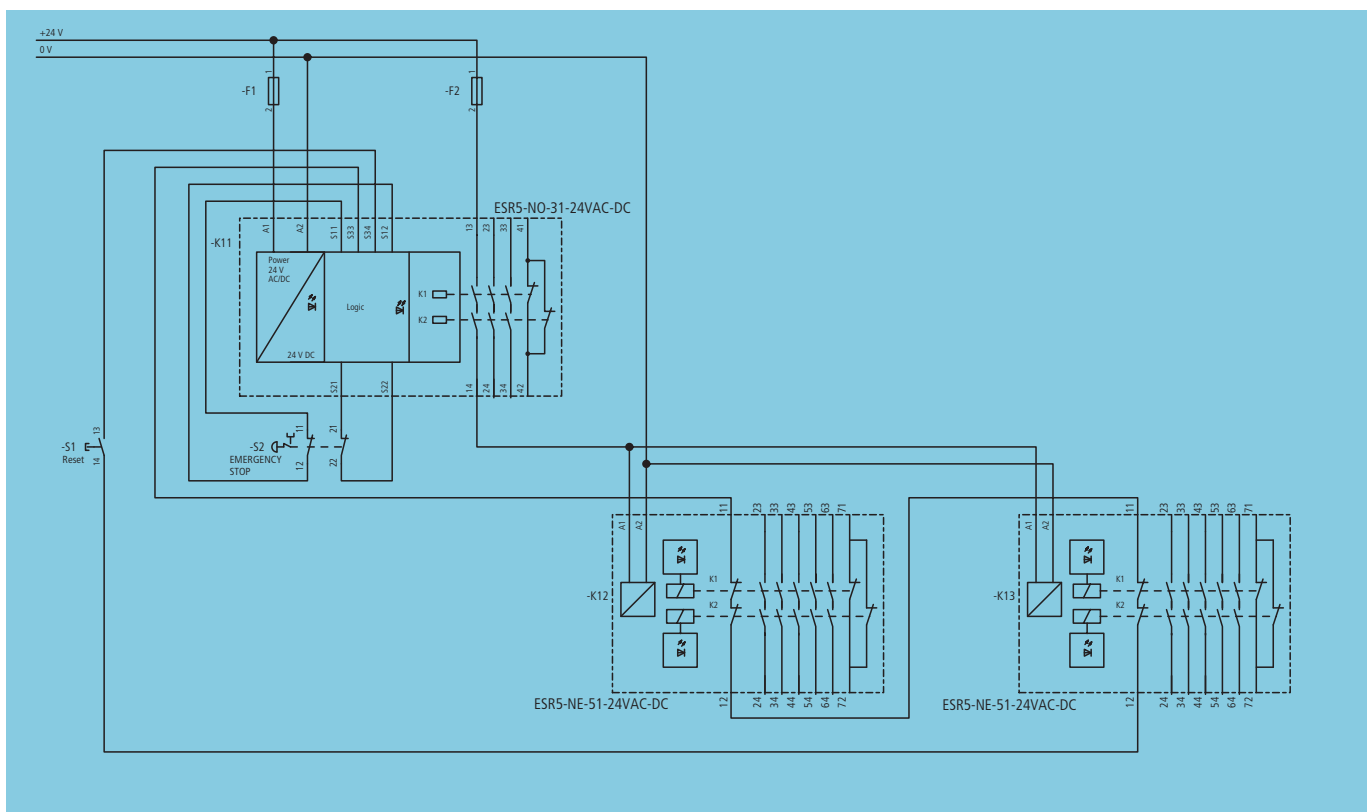


Figure 50: Feedback Circuit, safety relays with contact expansion modules

12 The way to a safe machine

12.1 Schedule

The way to a safe machine

Your machine must be demonstrably safe, i.e. it must perform its functions without causing injury or damage to health. As a rule you are permitted to provide self-certification and to refer to the "responsible authorities" in special cases. This should also be certified externally by affixing the CE mark.

Hazard detected, hazard excluded

A risk estimation must be made for the entire machine as well as for its associated parts. If the conclusion is reached that a circuit or component failure in protective devices may cause danger, then additional measures must be taken to avoid the risks in the event of a fault. This procedure must be executed carefully and documented in every case.

Create a factory standard

- Identify the relevant directives.
- Research the standards.

→ chapter "The European safety concept", page 100

Prepare technical documentation

- List the basic requirements.
- Carry out a hazard and risk analysis.
- Describe solutions.
- Specify test criteria.

If a relevant type C standard does not exist, the machine engineer must evaluate the risk by means of a hazard analysis, implement measures to minimize risks, carry out tests and record results.

The type B standards EN ISO 12100, EN ISO 13849-1 and IEC 62061 will help the engineer in the assessment and reduction of risks.

Integrate a safety concept

- Inherently safe design.
- Technical safety measures and additional protective measures.
- User information concerning residual risk
 - on the machine
 - in the user manual

The protective measures to be taken must have the objective of excluding the risk of accidents during the machine lifetime, from manufacture to decommissioning, dismantling and disposal, in all operating situations.

Prepare operating instructions

- Basic safety chapter
- Special danger warnings
- Translate operating instructions

The operating instructions with the description of "intended use" and "warnings" are important for the user. The completed risk evaluation is of use here: "Warning of residual hazards that cannot be excluded".

Create a declaration of conformity

The manufacturer must prepare a declaration of conformity for each machine in which the relevant EN standards are mentioned and the conformity of the machine is declared. If compliance with these standards is ensured, it can be assumed that the requirements of the Machinery Directive are also fulfilled.

If a machine is listed in Annex IV and V of the Machinery Directive, special conformity assessment procedures must be applied in accordance with clause 12. A list of the machines in accordance with Annex IV and V is shown on page 150.

Annex II of the Machinery Directive stipulates two different declarations of conformity:

1. Annex II A for machines.
2. Annex II B for incomplete machines.

In addition to the declaration of conformity, the manufacturer must document all relevant hazards/risks and counter measures with test results. This documentation is not written for customers but must be presented to a "responsible authority" if this is "requested on justifiable grounds".



Affix CE mark

The manufacturer and the authorized agent in the EU (licensee/contract partner) must declare the conformity of products with the safety requirements of the relevant directives and EN standards. This is documented by the issuing of an EU declaration of conformity.

The manufacturer takes full responsibility for the affixing of the CE marking after prototype testing. The CE mark is a compulsory condition of sale since from the date of compulsory CE marking onwards, products/components/devices/systems may not be sold without the CE mark.

The CE marking should be considered like a passport within the European single market. It must not, however, be confused with a quality mark or seal since it is only intended as an administrative marking. The CE marking mainly is designed for the competent body. It indicates to purchasers and end users that it can be "assumed" that the product meets the requirements of the directive or the applicable legislation.

The CE marking must be carried out before putting the product onto the market, i.e. before selling and commissioning. Putting into circulation as defined by the directive applies to any transfer of technical devices, products or other goods to others. Importation into the EU is also considered as putting into circulation, and so imported goods must also be provided with the CE marking if they are required to comply with a directive. Technical equipment includes working equipment that is ready for use, devices, tools and machines. Technical equipment includes working equipment that is ready for use, devices, tools and machines. Working equipment is ready for use when it can be used for the intended purpose. No other parts are required.

Putting into circulation, and thus CE marking, applies to the following machines:

- New machines produced for the first time in the EU.
- Existing machines which must be retrofitted and/or modified.
- All machines (new ones and existing machines) which are imported from a non-EU country and which are sold and/or used in the EU.
- New or modified machines which are provided free of charge.



The way to a safe machine

12.2 Directives important for machines

The European safety concept

There are several different directives with compulsory marking requirements and a large and rapidly growing number of EN standards (harmonized European standards). Their aim and purpose is to assist the free movement of goods within the European Union on the basis that each member state will have similar requirements for ensuring that minimum safety levels for users are met.

EU directives = national legislation

EU directives are a type of blanket directive. The directives must be implemented by all member states into national legislation.

The EU directives are primarily there to ensure a standard and binding legal framework.

However, only the basic requirements are specified without technical details so as not to impair technological developments.

The European standards

The European standards (EN standards) are implemented into the national standards of each member state within the European Union.

National standards with contents not complying with EN standards are withdrawn.

This applies to DIN/VDE standards as well as to work safety standards VBG..., ZH... etc. (in Germany) By complying with the EN standards, it can be "assumed" that the requirements of the directives are fulfilled. These EN standards are listed in the "Report of the commission in the scope of the execution of the guideline".

Can EN draft standards be used?

Only the valid (white paper) EN standards are to be used.

As long as there are no EN standards for a particular field, or only drafts, then the national standards can and should be used.

In practice, the draft standards (prEN...) published in the EC Official Journal are also used by the responsible authority as the basis for conformity assessment.

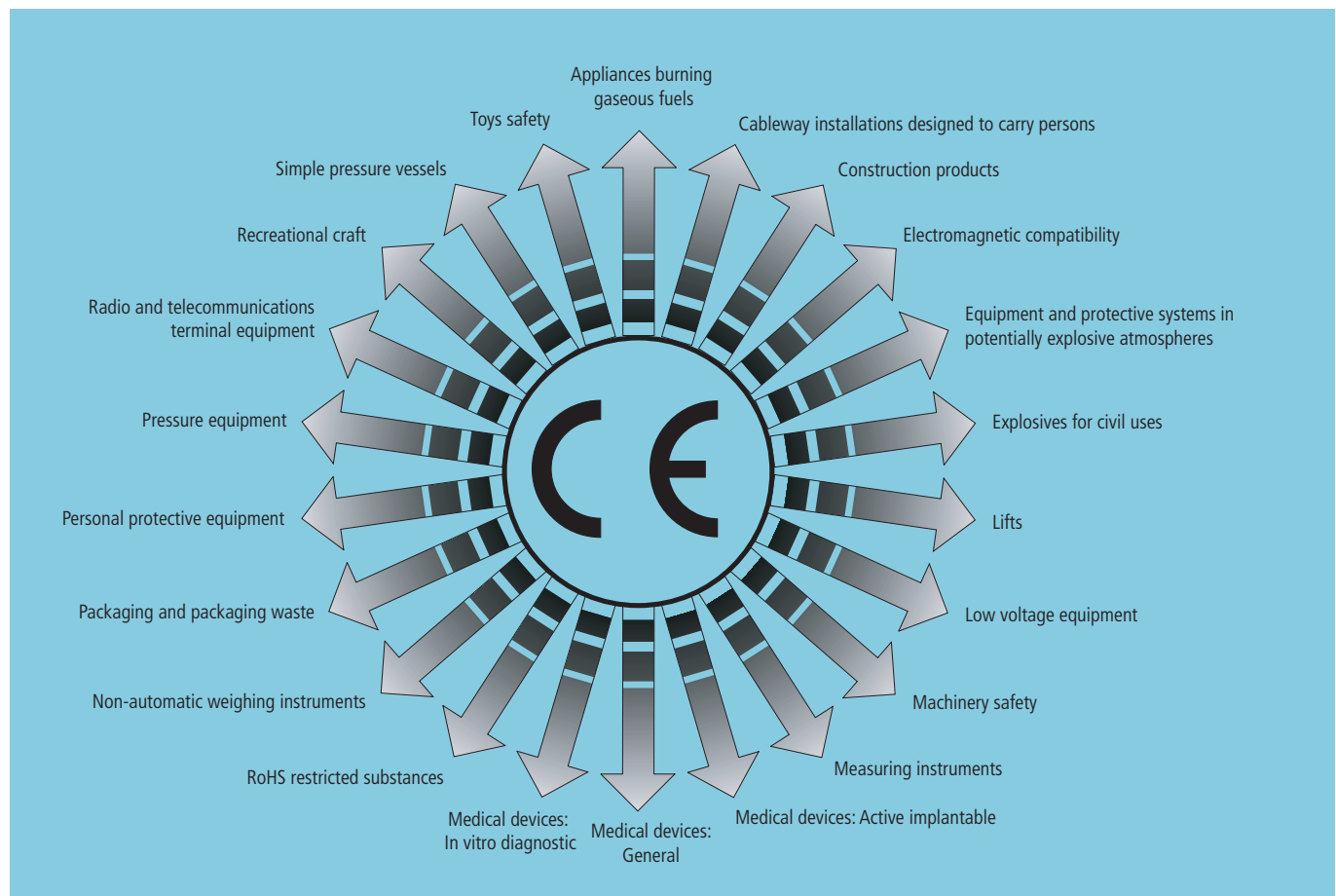


Figure 51: EC/EU Directives concerning the CE marking



Low-voltage Directive

The Low-Voltage Directive 2006/95/EC requires the mandatory CE marking of electrical equipment. The fulfillment of safety objectives is meant to ensure protection from hazards caused by electrical current in low-voltage devices. Important basic requirements in the form of safety objectives are described in Annex I of the directive.

Low-voltage devices include electrical switching devices, conductors, cables, wires and installation components with a voltage range of 50 – 1000 V AC and 120 – 1500 V DC (see EN 50110-1).

EMC Directive

The marking of products compliant with the EMC Directive 2004/108/EEC has been compulsory since 1996. The EMC Directive stipulates two basic requirements placed on the electromagnetic compatibility of devices:

- IEC 61000-6-1 – Immunity, i.e. the appropriate immunity of devices to electromagnetic interference.
- IEC 61000-6-3 – Emission, i.e. the highest value of electromagnetic interference emitted by devices (radiation, emission).

Different requirements are placed on industrial applications on the one hand, and home, business, trade, light industry, small companies, offices and laboratories on the other.

Machinery Directive

Since the beginning of 1995 CE marking has been made obligatory for compliance with the Machinery Directive 89/392/EC. The new Machinery Directive 2006/42/EC has been in force from 29.12.2009 and thus replaces the previously valid 98/37 EC. It stipulates the general requirements placed on the safety of machines and the health the user/operator.

What is a “machine”?

In accordance with this directive, a machine means an “assembly of linked parts or components, at least one of which moves, with the appropriate actuators, control and power circuits etc., joined together for a specific application.”

It also includes the actuating devices as well as the control and power circuits which are added for a particular application (such as the processing, treatment, moving or packaging of a material).

However, the Machinery Directive only contains basic requirements whilst there are many different types of machines available. The question therefore arises: “How can I prove that my machine is safe?”

The EN standards consequently stipulate requirements that can be tested and are therefore certifiable for this purpose.

The EN “Safety for Machines” standards are divided into three main groups:

- Type A: Basic standards defines requirements which apply to all machine types and are basic safety requirements.
- Type B: Group standards deal with design aspects such as distances, surface temperatures, ... or functional aspects such as Emergency-stop, two-hand control, ... These aspects apply to different machine groups.
- Type C: Product standards are “product standards” that stipulate specific requirements placed on individual machine types. The type C standard enables the safety of the machines to be tested and certified.

Type A

EN ISO 12100

Safety of machinery
Basic terms, general principles for design

Type B

EN ISO 13849-1

Safety of machinery
Safety-related parts of control systems

IEC 62061

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

IEC 60204-1

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

Type C

Machine safety standards with detailed safety requirements for specific machines or a group of machines.

→ The product standard must first be observed for the relevant machine type. This normally refers to the relevant group standards. If the C standard contains requirements that are different, the C standard applies.

The safety requirements stipulated in the Machinery Directive and in EN standards depend on the risk of accident involved. Most type C standards take into account the specific risks of the machine type concerned. The degree of safety required therefore tends to depend on the particular standard concerned.

Old machines

Information on machines put into circulation on the market and commissioned before 12-29-2009 is provided in section 13.5 “Requirements for existing machines”, page 152.

The way to a safe machine

12.3 Overview of relevant safety standards

The contents of standards have been laid out and structured on the following pages for practical use. Please refer to the standard concerned directly for binding or detailed information.

The order addresses for EN standards are provided in section 13.6 “Reference sources for regulations, bibliography”, page 148.

Information on the Internet at: www.vdma.org

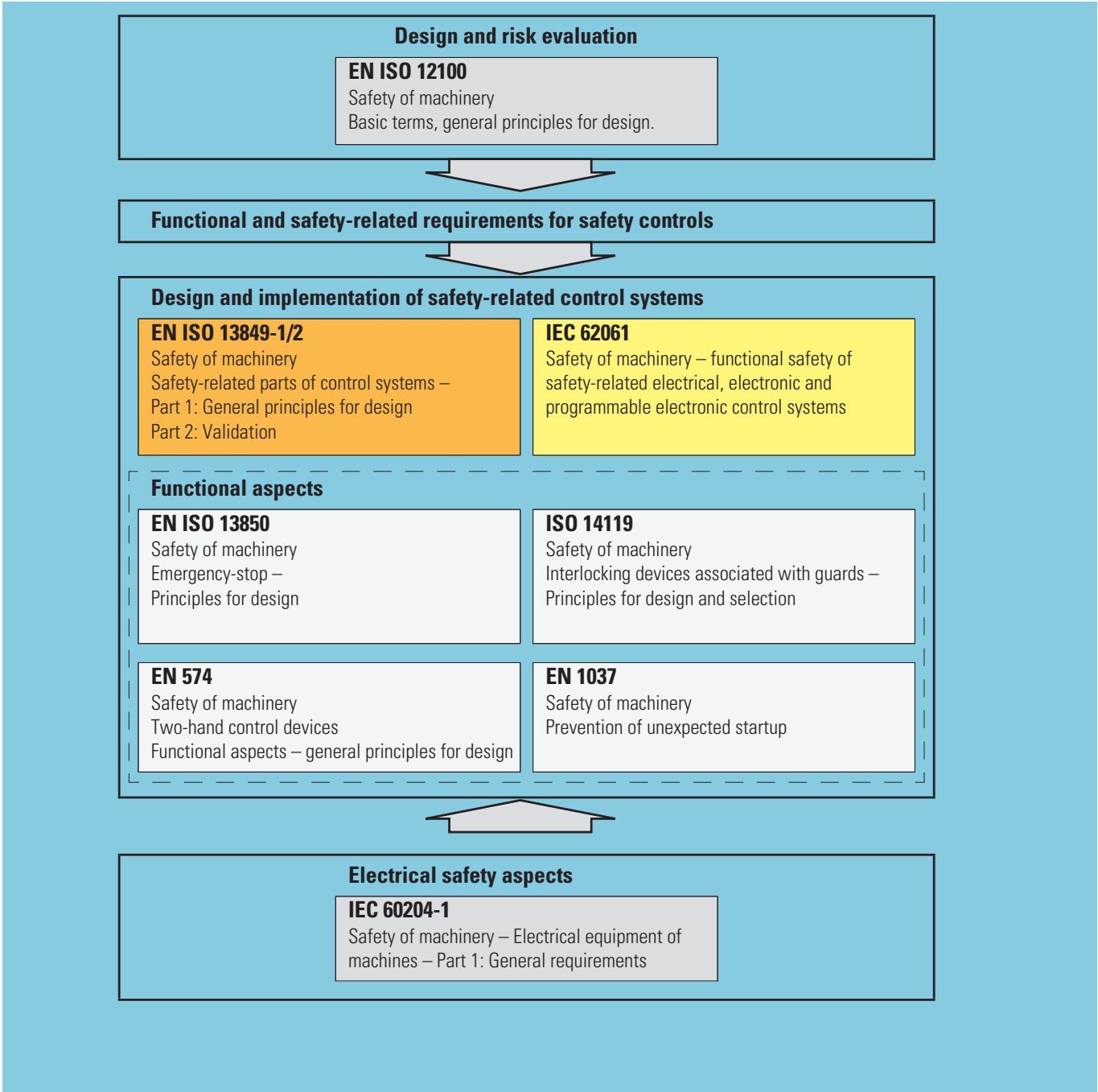


Figure 52: Standards and directives for the design of safety-related parts of control systems



Design and risk evaluation

EN ISO 12100

Safety of machinery; Basic terms, general principles for design
Part 1: Basic terminology, methodology
Part 2: Technical principles

Purpose

By which basic and pragmatic methods can machines of all types be designed in compliance with European legislation?

If no product standard exists for your machine, important guidance is provided here. This Type A standard forms the basis for Type B and C standards.

Target group

Machine designers B and C standards makers and creators of factory standards.

Essential points in brief

The strategy for risk reduction is specified as follows:

Perform a risk assessment by carrying out the following steps in the order given:

- Determine limits and intended use of the machine.
- Identify possible hazards and hazardous situations.
- Assess the risk for every hazard or hazardous situation.
- Evaluate risk and make decisions on the necessity of risk reduction.

If the result of the risk assessment shows that risk reduction is necessary, protective measures must be taken according to the following “3-step method”.

1. Inherently safe design

Choose suitable design features as principal measures for hazard removal:

- No sharp corners or edges.
- Observe minimum clearances from hazards.
- Reduce forces, speeds and weights to safe values.
- Design parts within the load limits.
- Use intrinsically safe technologies such as safety extra-low voltage, non-toxic fluids in the hydraulics etc.
- Mechanical restraint devices shall be given preference over solutions dependent on power when the transfer of movement is involved.
- Ensure ergonomic features such as sufficient lighting and ergonomic operation.
- Exclude hazardous behaviour of the machinery such as unexpected startups or uncontrolled speed changes by means of safe control system design.
- Fault detection by means of redundant design
- Minimize the work required in the danger zone through:
 - Reliability of machine functions – this reduces the frequency of the interventions required.

- No manual loading and unloading of the machinery.
- Setting and maintenance locations outside the danger zone.

Take into account all “phases of the working life” of the machine: Construction, transport and commissioning, operation and implementation, decommissioning, dismantling and, when necessary, disposal.

2. Risk reduction by means of technical safeguards

Technical protection measures must be applied if it is not possible to reduce the potential hazards by means of appropriate design features.

Example 1:

If access to the danger zone is not necessary during operation, close this area off by means of mechanical covers. EN 953 describes the requirements placed on “guards”.

Example 2:

Ensure the following measures if the user must work in the danger zone:

- Movable guard with monitoring feature.
- Electro-sensitive protective equipment.
- Two-hand control.

The guards should remain functional when possible during maintenance and setting operations. If this is not possible, a lockable operating mode selector switch must be used. This should enable an operating mode of “reduced risk” such as creep speed to be selected manually.

3. User information concerning residual risk

You were not able to remove all hazards satisfactorily by means of design measures or technical safeguards? Warn the user directly by means of clear indications in the operating instructions at the location of danger!

Risk estimation and evaluation must be carried out after each of the three stages for risk reduction → figure 53, page 104.

The way to a safe machine

Overview of relevant safety standards

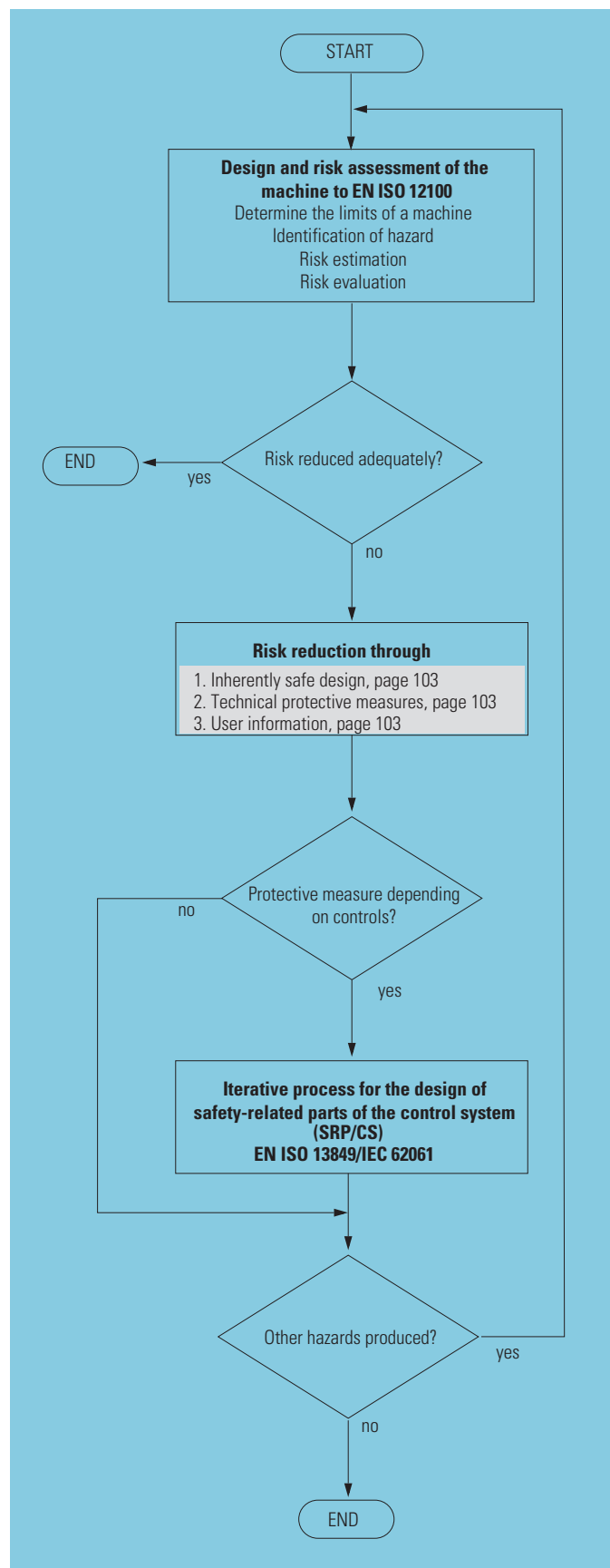


Figure 53: Risk reduction strategy

Additional precautionary measures

In the event of an emergency one or several Emergency-stop devices must be provided. This is not necessary for:

- Portable handheld or manually operated machines.
- Machines where the risk is not reduced by an Emergency-stop.

The Emergency-stop function must not be regarded as a substitute for protective measures. It must be designed so that the hazardous movement can be stopped by suitable means according to the risk assessment (see EN ISO 13850).

Energy isolation and dissipation are required for repair and maintenance work. For this use for example lockable main switches with isolating function.

Furthermore:

- Provide connection possibilities for transport with lifting gear.
- Ensure that all work such as operation, maintenance etc. can be carried out on the floor or on non-slip platforms.
- Ensure static and dynamic stability.

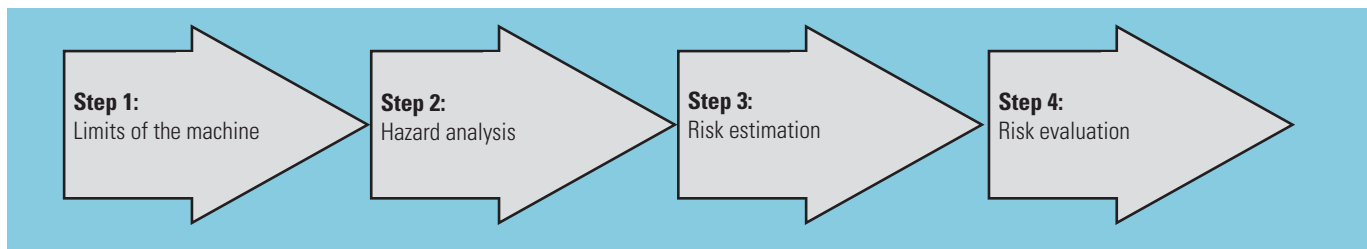


Figure 54: Risk assessment in 4 steps

Step 1: Limits of a machine

Define first of all the limits of the machine.

- Which functions are to be fulfilled by the machine and which not? Proper usage and foreseeable faults and misuse.
- Who should use the machine and who not? Qualification and experience of the personnel in all areas from development to maintenance.

Step 2: Hazard analysis

Identify the hazards:

- Which kind of hazards are present on the machine? Use the tables in EN ISO 12100 as a check list. This table indicates possible electrical, mechanical, chemical and physical dangers
- Assess the ambient and operating conditions of the machine.
- Which events can cause damage? Manual material supply or removal, service, maintenance, human behaviour, influence by persons that are not operating personnel, failure of safety-related components.

Step 3: Risk estimation

Estimate the risk for each hazardous situation by determining the following factors:

- Severity of damage (slight, serious, fatal)
- Probability of occurrence of the damage depending on:
 - Exposure to the hazard by one or several persons.
 - Occurrence of a hazardous incident.
 - Possibility to reduce or limit the damage.

Assess the risk for every hazardous situation taking the following factors into account:

- Take all affected persons into account.
- Type, frequency and duration of stay in the hazardous area.
- Relationship between exposure to the hazard and effects.
- Human factors: risk awareness, training, time pressure.
- Suitability of the protective measures.
- Possibility of defeating the implemented safety measures.
- Combination and interrelationship of hazardous situations (complexity).

Step 4: Risk evaluation

A risk evaluation must be carried out after the risk estimation in order to assess the necessity of risk reduction. If risk reduction is required, refer to the risk reduction points stated in EN ISO 12100. The risk assessment must then be repeated.

- Has the necessary level of safety been achieved?
- Have hazards been removed/reduced?
- Do the technical protective measures offer sufficient protection and can they be used in practice?
- Is the category selected in accordance with EN ISO 13849 or IEC 62061 correct?
- Are instructions for the intended use clearly formulated and understandable?
- Are the safe working procedures described properly?
- Is the user informed of the necessity of the personal protective equipment?
- Is the user warned sufficiently of residual risks?

The certification of the hazard analysis is a check that all significant hazards have been identified and appropriate precautions have been taken, such as the selection of the suitable category in accordance with EN ISO 13849 or subsystem architecture in accordance with IEC 62601. Protective measures and the objectives achieved through them must be documented.

The way to a safe machine

Overview of relevant safety standards

Design and implementation

EN ISO 13849-1

Safety of machinery
Safety-related parts of control systems
General principles for design

Purpose

- Design and assessment of a safety-related control system.
- Determine and assess the degree of resistance to faults, depending on the risk of hazard.
- Check and document the requirements stipulated and achieved.

Target group

- Machine designers
- Design engineers
- Independent test institutes
- "C" standard makers
- Creators of factory standards

Essential points in brief

EN ISO 13849 stipulates safety requirements and provides a guide to the principles for designing and integrating safety-related parts of control systems (SRP/CS) and software.

Properties are defined for these parts of the SRP/CS that are required for the implementation of the corresponding safety functions.

The probability of failure must be estimated for each SRP/CS and/or combination of SRP/CS that represents a safety function. This value is expressed as the performance level (PL a to e).

The technologies and energies (electrical, hydraulic, pneumatic, mechanical etc.) used for a machine are not considered in the design of an SRP/CS.

The PL of the SRP/CS is determined by estimating the following parameters:

- MTTFd value of each component
- DC
- CCF
- Architecture of the category
- Behaviour of the safety function under fault condition(s)
- Systematic failures
- The ability to perform a safety function under foreseeable environmental conditions.

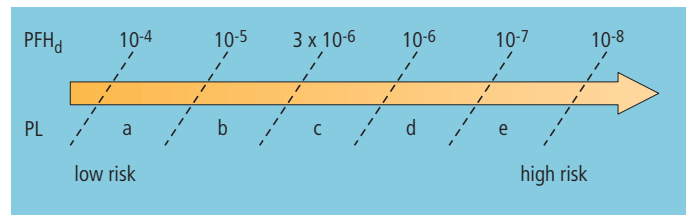


Figure 55: Average probability of failure

PFH_d = Average probability of dangerous failure per hour

PL = Performance Level

→ Other measures are required to achieve the PL in addition to the average probability of dangerous failure per hour.



Design and implementation

IEC 62061

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

Purpose

Examination and assessment of the performance level (PL) and the safety integrity level (SIL) of a safety-related control system.

Target group

- Machine designers
- Design engineers
- Independent test institutes
- "C" standard makers
- Creators of factory standards

Essential points in brief

This standard specifies the requirements and gives recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control system (SRECS) of machines.

It is restricted to risks that arise directly from the hazards of the machine itself or a group of machines in coordinated operation.

It does not specify requirements for the performance of non-electrical (e.g. hydraulic, pneumatic) control elements for machines.

The safety integrity requirements of the safety-related control function must be derived from the risk assessment. This can ensure that the necessary level of risk reduction is achieved. This standard expresses the safety integrity as a failure limit value for the probability of a dangerous failure per hour for each safety function. This value is divided into three safety integrity levels (SIL).

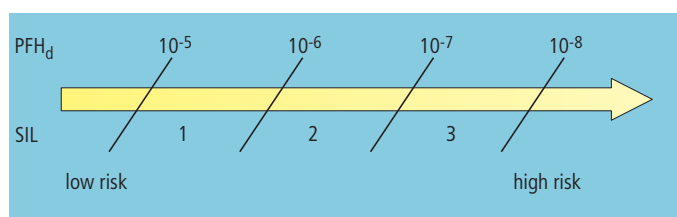


Figure 56: Average probability of failure

PFH_d = Average probability of dangerous failure per hour

SIL = Safety Integrity Level

An example in section 12.6 "Steps to SIL safety integrity level according to IEC 62061", page 126 further explains the design and integration of a safety-related control system.

Recommended application and selection of standard

Fulfillment of the relevant basic safety requirements can be assumed if both EN ISO 13849 and IEC 62061 are applied.

When should I use which standard?

Refer to the following table comparing the application areas of both standards to select the appropriate standard.

Table 3: Recommended application of EN ISO 13849-1 and IEC 62061

	EN ISO 13849-1	IEC 62061
Non-electric, e.g. hydraulic	Included	Omitted
Electromechanical, e.g. relay and/or simple electronics	All architectures and up to PL e	All architectures and up to SIL 3
Complex electronics, e.g. programmable	All architectures and up to PL e	Up to SIL 3 with development according to IEC 61508
Combination of different technologies	Restrictions as above	Restrictions as above, non-electrical parts to EN ISO 13849-1

Revised source: BGIA Report 2/2008, Figure 3.3

The way to a safe machine

Overview of relevant safety standards

Functional aspects

ISO 14119

Safety of machinery – Interlocking devices associated with guards – Principles for design and selection

Purpose

How should movable guards be monitored?

The standard describes the principles for the selection and design of interlock devices and their connection to the guard door (→ EN 953) or to the control system (→ EN ISO 13849, IEC 62061).

Target group

Machine designers and Type C standard makers.

Essential points in brief

This standard describes the basic terms and general design principles for interlock devices and guards.

Select and design the type of interlock device for your application so that the basic EU safety requirements are fulfilled.

Important selection criteria for a suitable interlock device in special applications are:

- The application conditions and the intended use.
- The hazards present at the machine.
- The severity of the possible injury.
- The probability of a failure of the interlock device.
- The stopping time and entry or access time.
- The duration by which a person is exposed to the hazard.

Some of these criteria have already been covered in EN ISO 12100, EN ISO 13849 and IEC 62061.

Designs are still grouped as with and without guard locking.

ISO 14119 distinguishes between four different types of interlocking devices:

- Type 1: Mechanical actuation principle, contact, force / uncoded actuator, e.g., rotary cams, linear cams
- Type 2: Mechanical actuation principle, contact, force / coded actuator, e.g., tongue (shaped actuator)
- Type 3: Non-contact actuation principle, e.g., magnetic / uncoded actuator, e.g., magnet
- Type 4: Non-contact actuation principle, e.g., RFID / coded actuator, e.g., coded RFID tag

Type 3 and type 4 interlocking devices usually feature a high degree of protection (e.g., IP67, IP69K), are affected less by soiling, and are more tolerant to guard misalignments.

If a type 3 or type 4 interlocking device is the only interlocking device, it must meet the requirements in IEC 60947-5-3.

Designs are still grouped as with and without guard locking.

Interlocking devices with and without guard locking

An interlocking device **without guard locking** is a mechanical or electrical device that only allows the operation of a machine if the guard door is closed (e.g. safety position switch with separate actuating element).



Figure 57: LS-ZB safety position switch with separate actuating element

This protective measure prevents the hazardous machine functions if the guard is not closed. Opening the guard during operation triggers a Stop command. It has the same meaning as a Stop command (EN ISO 13 850, Emergency-stop devices). Closing the guard switches the machine to operational readiness. The Start signal must be made separately.

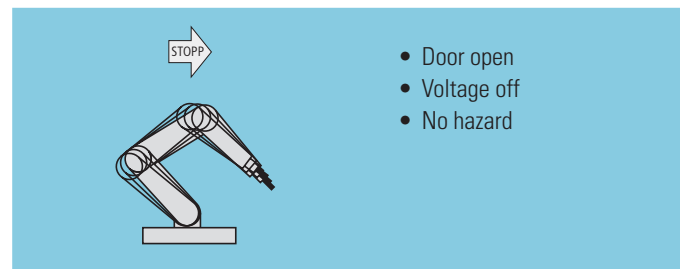


Figure 58: Interlock equipment without guard locking for personnel protection

An interlocking device **with guard locking** is a mechanical or electrical device that only allows the operation of a machine if the guard door is closed and locked (e.g. safety position switch with separate actuating element and guard locking).



Figure 59: Safety position switch with separate actuating element and LS-ZBZ auxiliary release mechanism



The hazardous machine functions are made safe by means of a closed and locked guard. The guard stays closed until the risk of injury by the hazardous machine function is excluded (e.g. by means of speed or zero speed monitors).

The machine is made operational by closing and locking the guard. The Start signal must also be issued here separately.



Figure 60: Interlock equipment with guard locking for increased personnel protection

Which type should be used when?

Stopping time > entry or access time

→ Interlock device with guard locking

Stopping time > entry or access time

→ Interlock device without guard locking

Example:

An operator opens the guard door of a lathe and thus switches off the drive energy. He then reaches into the hazardous area to retrieve a workpiece.

The hazardous movement must be finished before the operator reaches these parts of the machine. Otherwise an interlock device with guard locking must be used.

The stopping time of the machine can be determined very easily.

The entry or access time is determined by the parameters "Clearance", "Approach speed" and machine-specific factors such as "Type of accessibility".

You can calculate this time using DIN EN 999/ISO 13855 "The positioning of protective equipment in respect of approach speeds of parts of the human body".

Type of actuation of mechanical position switches

Always viewed with opened protection door.

- A position switch:

A position switch must always be actuated with positive operation.

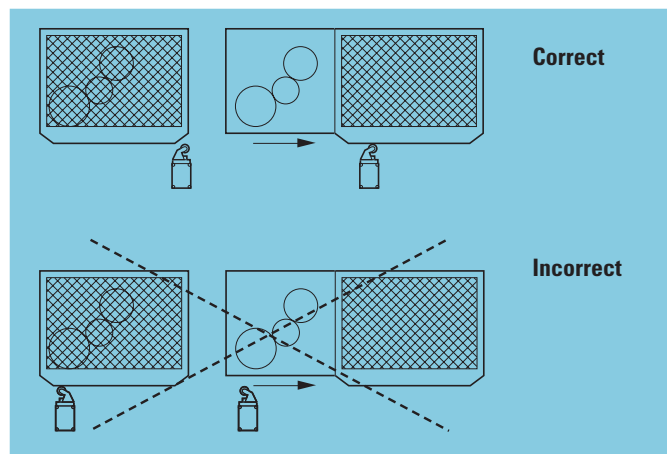


Figure 61: Type of actuation of mechanical position switches – one position switch

- Two position switches::

One must be operated positively and one may be operated via a return spring → Prevent faults with the same cause.

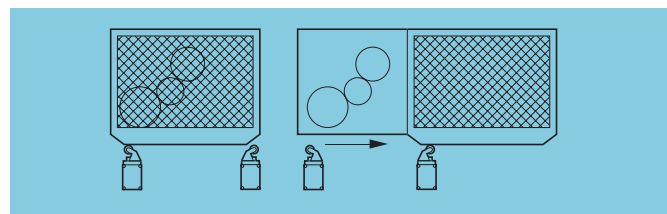


Figure 62: Type of actuation of mechanical position switches – two position switches

The way to a safe machine

Overview of relevant safety standards

Arrangement and fixing of position switches

Position switches and actuators must be protected against change of position:

- Only use fixing elements that are reliable and which can only be undone with a tool.
- Protect against self-loosening.
- Use oblong holes only for initial setting.
- Ensure mechanical restraint by means of bolts, pins, mechanical stops etc.
- Switch must not be used as a mechanical stop.
- Observe the paths specified by the switch manufacturer (figure 63, page 110).
- Ensure that the switch is protected so that external influences cannot cause any damage.
- Fit the switch so that it is accessible for maintenance and function testing.
- When the guard door is opened, ensure that intervention in the hazardous area is not made until the hazardous movement has stopped.

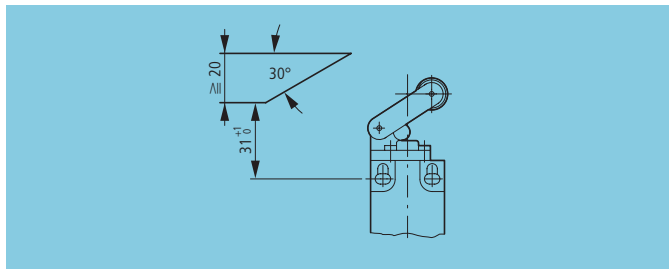


Figure 63: Travel diagram for a position switch

Bypassing the safety function should be made more difficult by separate switch actuators (safety position switches).

- The switch must be fitted with a cover.
- The actuator should be fitted as a captive part.

Requirements for position switches

- N/C contacts must be \ominus positive opening in accordance with IEC 60947-5-1 Annex K.
- Enclosed devices must have at least degree of protection IP54.

Guard locking devices must meet the following conditions:

- Be form-fit by means of two rigid parts.
- Normally assume the locked position by means of spring force and must be unlocked by means of energy.

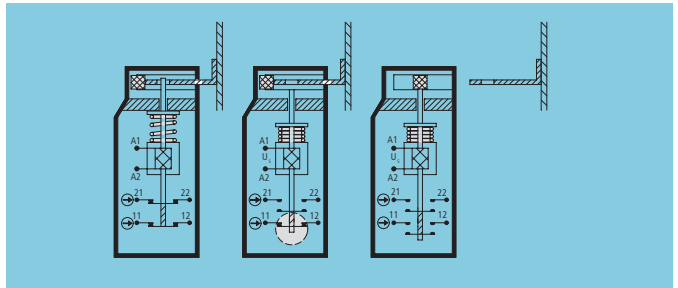


Figure 64: Spring force locking device

- Have a manual auxiliary unlocking function which can only be operated by means of a tool (only for spring-force locked devices),

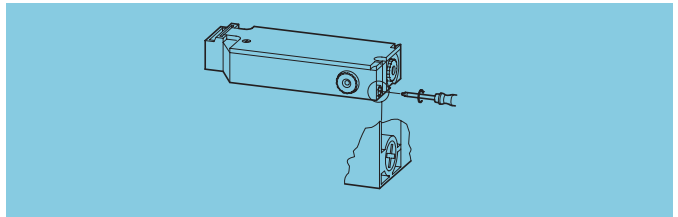


Figure 65: Manual auxiliary unlocking

- Be totally in the locked position before the machine movement is enabled.
- Withstand the forces expected.



Functional aspects

EN ISO 13850

Safety of machinery
Emergency-stop equipment – Principles for design

Purpose

Function requirements of devices for stopping in an emergency (Emergency-stop equipment).

Target group

Machine designers and Type C standard makers.

Essential points in brief

The Emergency-stop function should prevent or reduce arising or existing hazards to personnel and damage to machines or to the working material. Hazards may, for example, be functional irregularities, malfunctions of the machine, unacceptable properties in the processed material and human errors.

Emergency-stop is required

This standard stipulates the mandatory use of Emergency-stop devices for each machine with the following exceptions:

- Machines on which Emergency-stop devices do not reduce the risk.
- Hand-held and manually operated machines.

Emergency-stop is a supporting measure and not a substitute for missing protection measures!

Emergency-stop devices must be provided on all operating panels and other working stations in accordance with IEC 60204-1.

Emergency-stop operation

The Emergency-stop function is activated by a single manual operation of a person. It must always be available and functional (→ EN ISO 13849-1). The particular operating mode is not important.

Design the Emergency-stop devices in such a way that the user is not forced to consider the consequences of operating the device. This prevents delays up to the point of activating the device when the system is disconnected.

The efficiency of safety devices and devices with safety-related functions must not be impaired by the Emergency-stop function. This also includes the rescue of persons from hazardous situations.

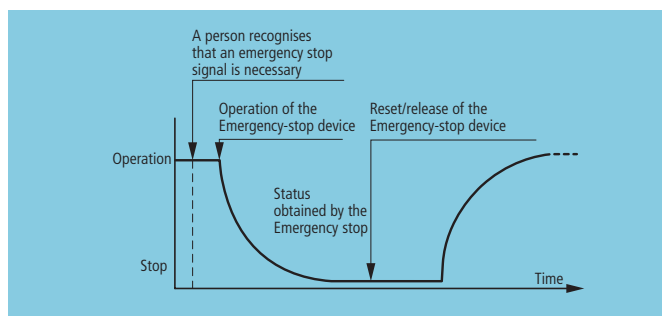


Figure 66: Function sequence emergency stop

The reaction of the machine to the Emergency-stop command must not cause any additional hazards.

Check what the minor risk represents:

- Immediate disconnection = STOP category 0.
- Controlled stopping = STOP category 1.

STOP category 0

The system is disconnected by immediate disconnection of the supply to the drive element or by mechanical interruption (disconnection) of hazardous elements and their drive elements.

Application example: main switch with Emergency-stop function or Emergency-stop switching device in conjunction with undervoltage release.

STOP category 1

A controlled stop with power to the drive element available to achieve the stop. Once the stop has been achieved, the supply must be disconnected.

Application example: Motor with a DC brake or controlled drive.

The way to a safe machine

Overview of relevant safety standards

Emergency-stop actuators

Emergency-stop actuators must ensure positive opening operation.

Emergency-stop actuators with positive opening operation \Rightarrow in accordance with IEC/EN 60 947-5-1 Appendix K, open the contacts with a rigid link between the actuating section and the contact set. Furthermore, it must be ensured that devices are tamper-proof.

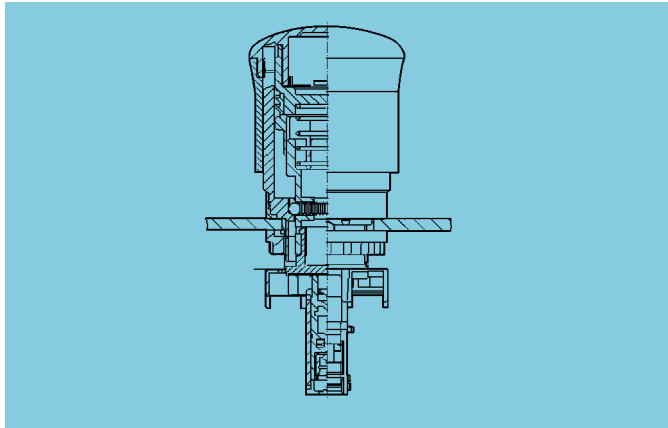


Figure 67: Positive opening with emergency stop actuators

Emergency stop contact monitoring with SMC (self-monitoring contact) if the actuation unit is particularly at risk

Function:

The SMC system is a contact element consisting of an N/C contact element connected in series with an N/O contact element. The dual-channel solution consists of two N/C contact elements. In this case, there is also a series connection between an N/C contact element and an N/O contact element. The SMC's design has its N/O contact connected to the actuator in such a way that it will only close if a proper connection is established between the actuator and the contact element. If the contact element block is not installed correctly or becomes detached, or if a surface mounting enclosure's cover becomes detached, the N/O contact will open with the SMC only, triggering the safety function.

Safety technical assessment:

Dual-channel emergency stop devices in the RMQ series without an SMC have a B10d value of 2,000,000. This makes it possible to implement a safety configuration with up to SIL3 / PLe.

Example:

If, for example, there are fewer than 660,000 actuations per year - which is always the case with emergency stop functions -, a high MTTFd value will be achieved. A high DC will then be achieved with measures in the connected decision logic. If the configuration still conforms to cat. 4, this means that all requirements for SIL3 / PLe are being met.

Application of the SMC:

If the risk analysis or validation for an emergency stop button reveals that it is particularly at risk, additional fault detection measures may be absolutely required in addition to verifying that the required PL or SIL is being conformed to. This risk could be, for example, a mechanical risk

to the contact element due to impact or mechanical shock, or the risk of the actuator being sheared off by moving parts in the surroundings. In these cases, there are stricter requirements for the safety function, and the company or entity operating the units is under the obligation of meeting these requirements. The SMC is used for these types of cases (in which the unit is particularly at risk), and can minimize the corresponding risk as required.

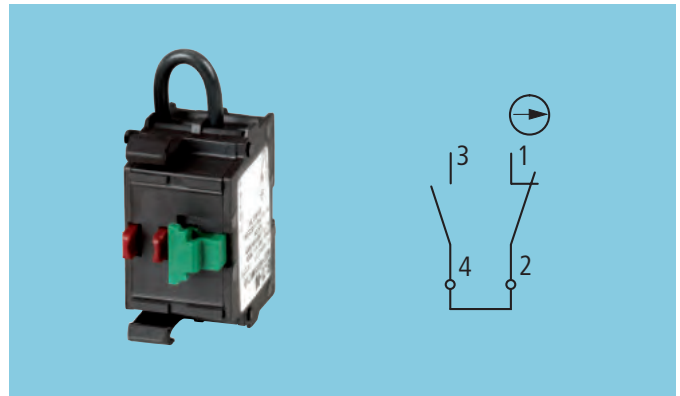


Figure 68: Single-channel configuration with monitoring contact

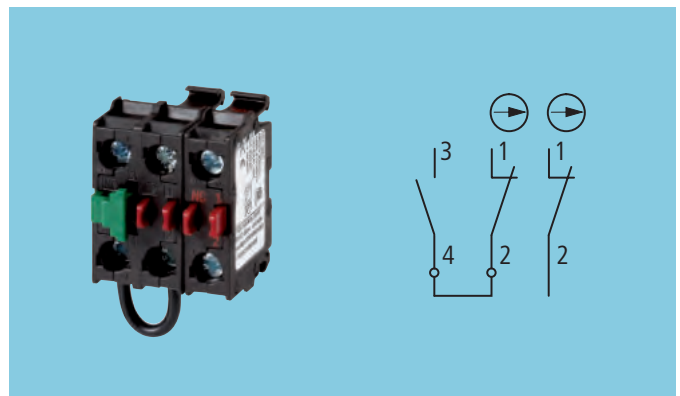


Figure 69: Two-channel configuration with monitoring contact

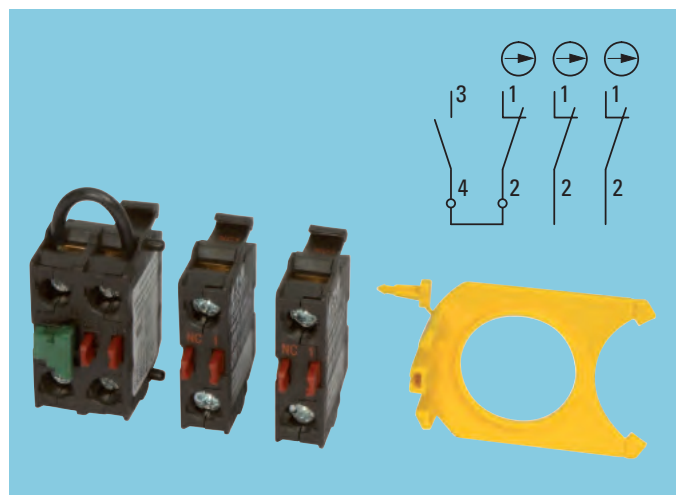


Figure 70: Two-channel configuration with monitoring and signaling contact (on a single installation level)



Functional aspects

EN 1037

Safety of machinery
Prevention of unexpected startup

Purpose

A machine must be protected against unexpected startups during the actions of a person in the danger zone. This standard stipulates design safety measures to protect against unexpected startups.

Target group

Machine designers and Type C standard makers.

Essential points in brief

The increasing level of automation in machines has increased the possibility of unexpected startups.

There are a considerable number of accidents in which machines have been stopped for fault finding or setting and which have started up unexpectedly.

Not only mechanical dangers due to movable parts must be taken into account, but also, for example, danger from radiation emitted by lasers.

Isolating and dissipating energy

Provide your machine with devices for isolation and energy dissipation.

Decommissioning, major maintenance work and work on power circuits must be carried out safely.

Devices for isolation

Devices for isolation must have the following characteristics:

- Isolate reliably.
- Transfer the operation of the actuator to the isolating element via a mechanically reliable connecting link.
- Indicate the switch position of the isolating element clearly, e.g. via the position of the operating element.
- Be lockable in the isolated position, for example with one or several padlocks. (A locking feature is not required if the restoration of the connection does not cause danger to persons.)

Main switches in accordance with IEC 60204-1 clause 5.3 meet these requirements.



Figure 71: Main switches in accordance with IEC 60204-1 clause 5.3., such as Eaton P3-100

Determine the arrangement and number of such devices according to:

- The design of the machine.
- The necessity of the presence of persons in the danger zone.
- The risk assessment carried out in accordance with EN ISO 14121.

Also observe "Devices for switching off for prevention of unexpected startup", clause 5.4 of IEC 60204-1.

Devices for the dissipation of stored energy or its retention

Devices for the dissipation of stored energy or its retention are, for example, brakes for movable parts, circuits for discharging capacitors, valves for pressure tanks.

Dissipation devices must be provided if stored energy can cause hazardous conditions.

Ensure that the energy dissipation or retention

- Occur at the same time as energy isolation.
- Do not cause hazardous conditions by themselves.
- Are described in the operating instructions.
- Can be checked for efficiency by the user (e.g. manometer).

Further measures

If the isolation/dissipation of energy is not appropriate for all operations, you can apply the following measures:

- Prevention of accidentally generated start command (example: Control circuit device with flush operating surface).
- Accidentally generated start commands must not cause an unexpected startup. STOP shall override START function. (Examples: Latched Emergency-stop actuator, key-operated actuator, opened movable protection door).



Figure 72: RMQ-Titan M22 keyswitches

- Automatic stop before a hazardous situation can occur. (example: A drive is only stopped with power electronics = Stop category 2 to IEC 60204-1. A zero speed monitoring function causes a disconnection via a contactor at the start of an unintentional movement.)



Danger!

These measures are not a substitute for energy isolation and dissipation. They may only be used after a thorough risk assessment.

The way to a safe machine

Overview of relevant safety standards

Functional aspects

EN 574

Safety of machinery – Two-hand control devices – Functional aspects; Principles for design

Purpose

The two-hand control is a safety device. A design in compliance with the standard prevents access to the danger zones during hazardous processes.

Target group

Machine builders, manufacturers of two-hand controls and type C standard makers.

Essential points in brief

The standard specifies requirements and instructions for the design and the selection of two-hand controls. The appropriate type C standard and the risk evaluation (→ EN ISO 12100 / EN ISO 14121).

The suitable two-hand control

Select the type and design of the two-hand control, depending on:

- The hazard concerned.
- The risk evaluation.
- The state of the application technology.
- Further influences such as prevention of accidental operation or bypassing of the safety feature.

No simple bypassing of the protection function or accidental actuation

Arrange the operating elements of the two-hand control so that the protection function cannot be bypassed easily. The possibility of accidental operation should also be reduced to a minimum.

The types of bypassing to be considered depend on:

- The design of the two-hand control.
- The actuation conditions.
- The type and location of mounting.
- The specified safety distances.

The standard shows some special procedures on how to prevent bypassing and accidental operation. The following examples are possible for different types of bypassing:

- Operation with one hand
 - Inside distance between the operating elements ≥ 260 mm

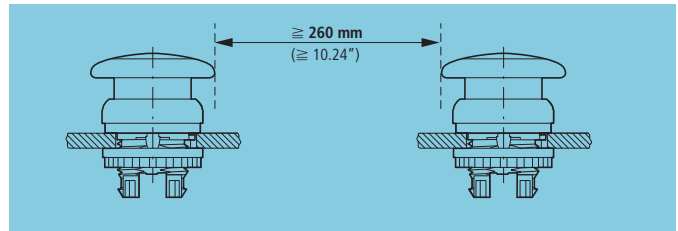


Figure 73: Prevent bypassing of guard: Inside distance

- Operation with hand and elbow of the same arm
 - Inside distance between the operating elements min. 550 mm (Φ 600 mm)
 - Operating elements with different operation directions
- Operation with forearm and elbow
 - Use of covers or collars

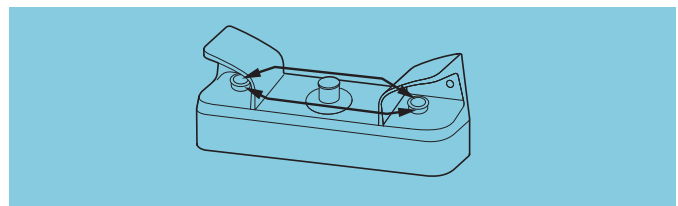


Figure 74: Prevent bypassing of the guard: Covers or collars

- Operation with one hand and any part of the body.
 - Operating elements on horizontal area min. 1100 mm above servicing level.
- Operation by blocking an operating element.
 - Use type II or type III.

These measures may not be compatible with ergonomic requirements. Make a careful decision here and take into account the "Safety first" principle!



Requirements	Types				
	I	II	III		
			A	B	C
Use of both hands	●	●	●	●	●
Output signal only if both input signals are present	●	●	●	●	●
Releasing one or both actuating elements ends the output signal	●	●	●	●	●
Prevent accidental actuation when possible	●	●	●	●	●
No simple bypass of the protection function possible	●	●	●	●	●
New output signal only after release of both operating elements		●	●	●	●
Output signal only after synchronous actuation within max. 0.5 seconds			●	●	●
Complies with category 1 in accordance with EN 954-1 ¹⁾	●		●		
Complies with category 3 in accordance with EN 954-1 ¹⁾		●		●	
Complies with category 4 in accordance with EN 954-1 ¹⁾					●

1) The versions of the EN 574 standard refer to EN954-1. A revision is in preparation.

What else must be observed?

Ensure the functioning in all operating and ambient conditions. Accidental START signals must not be generated in particular by impact, shock, falling etc. Provide two differently functioning operating elements on hand-held machines, preferably with a locking device. Portable two-hand controls in separate housings should be stable and secured against changes in their location. Protect the supply lines from damage.

Calculate the safety distance between two-hand controls and danger zone by means of the following points:

- Hand-arm speed rate (DIN EN 999/ISO 13855).
- Design and arrangement of the two-hand control.
- Response time of the two-hand control.
- Stopping time: Time between the termination of the output signal and the ending of the hazard.
- Intended use in accordance with EN ISO 12100.
- Relevant Type C standards.

Tests and information for use

Do the two-hand controls meet the requirements specified in the risk evaluation? This must be validated by means of a theoretical assessment as well as empirical tests. Table 2 of the EN 574 standard provides detailed requirements.

Provide additional information for the installation, operation and service preferably in the official language of the designer/operator.

Mark the two-hand control with at least the type and the standard concerned.

The way to a safe machine

12.4 Machine-related product standards

Subject	Standard
General	
Basic terms, general principles for design	
Basic terminology, methodology	EN ISO 12100
Technical principles	EN ISO 12100
Risk assessment	EN ISO 12100
Electrical equipment of machines – General requirements	IEC 60204-1
Safety-related parts of control systems	
General principles for design	EN ISO 13849-1
Reduction of risks to health from hazardous substances emitted by machinery.	
Principles and specifications for machinery manufacturers	EN 626-1
Methodology leading to verification procedures	EN 626-2
Safety features	
Interlocking devices associated with guards	
Principles for design and selection	ISO 14119
Electro-sensitive protective equipment	EN 61496-1
General requirements for the design and construction of fixed and movable guards	EN 953
The positioning of protective equipment in respect of approach speeds of parts of the human body parts	DIN EN 999/ ISO 13855
Clearances, surface temperatures	
Minimum gaps to avoid crushing of parts of the human body	EN 349
Safety distances to prevent danger zones being reached by the lower limbs	EN ISO 13857
Safety distances to prevent danger zones being reached by the upper limbs	EN ISO 13857
Temperatures of touchable surfaces – Ergonomics data to establish temperature limit values for hot surfaces	EN ISO 13732
Displays, control actuators, signals	
Ergonomics requirements for the design of displays and control actuators	
Displays	EN 894-2
Control actuators	EN 894-3
Visual, auditory and tactile signals	EN 61310-1
Requirements for marking	EN 61310-2
Humans	
Dimensions of human body parts	
Principles for determining the dimensions required for openings for whole body access into machinery	EN 547-1
Principles for determining the dimensions required for access openings	EN 547-2
Human body measurements	EN 547-3
Human physical performance	
Terms	EN 1005-1
Emergency-stop, two-hand control, energy isolation and dissipation	
Emergency-stop, principles for design	EN ISO 13850
Two-hand control devices – Functional aspects – principles for design	EN 574
Prevention of unexpected startup	EN 1037



Type B safety group standards

The type B safety group standards deal with design aspects such as clearances, surface temperatures, or functional aspects such as Emergency-stop, two-hand control,...

They apply to different machine groups. If there is no type C product standard for the machine, or if it does not deal with significant hazards of the machine, the specifications of the relevant type B group standards provide help with decision making.

The way to a safe machine

12.5 Steps to the Performance Level PL in accordance with EN ISO 13849-1

The necessary risk reduction is achieved by the ability of safety-related parts of a control system (SRP/CS) to perform a safety function under foreseeable conditions. The iterative process in accordance with EN ISO 13849-1 should be used for the design of the SRP/CS. After the necessary safety functions are identified and their properties defined, the required PL is determined. The following example is designed to guide you in stages through the iterative process for determining the PL.

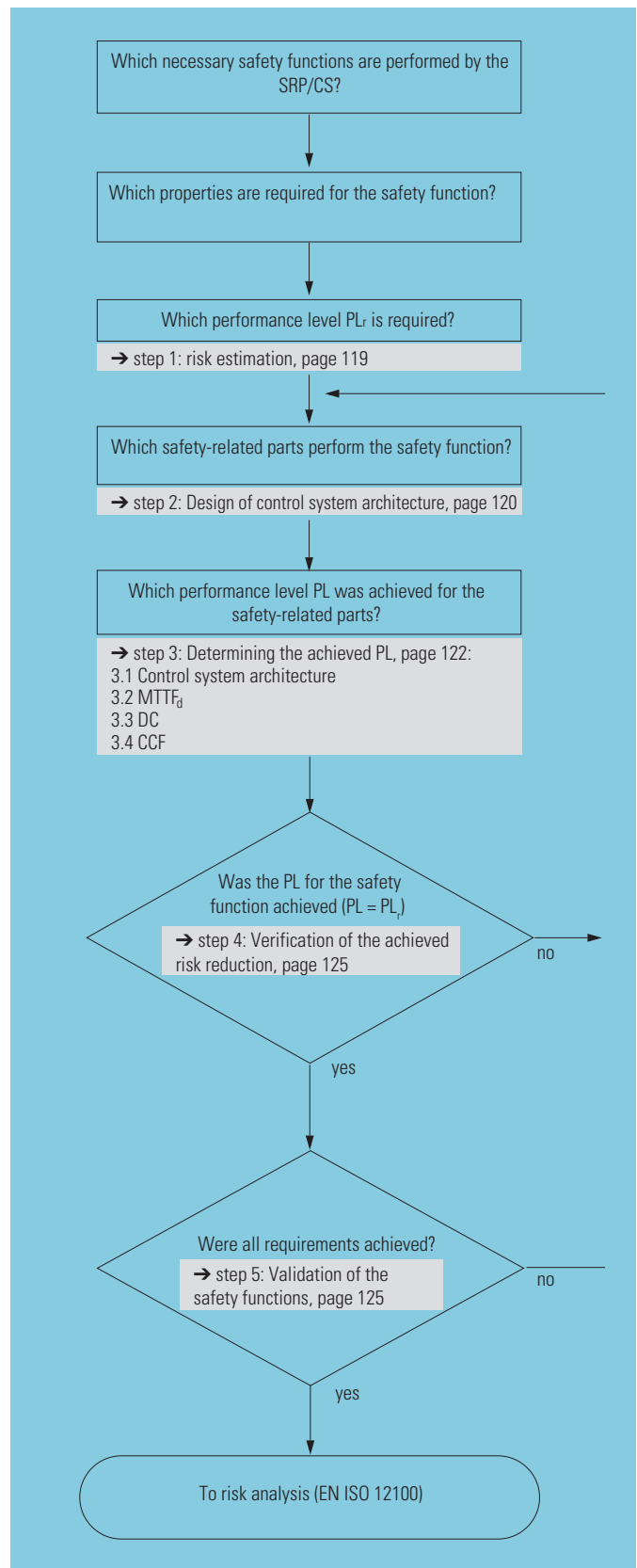


Figure 75: Design process for safety-related control functions



Step 1: Risk estimation

The degree of risk reduction determined by the risk estimation is stated as the required performance level PL_r .

The risk estimation to determine the required performance level PL_r assesses the machine without the safety functions provided.

The PL_r is determined according to the EN ISO 13849-1 risk graph. The S, F and P parameters used are the same as those of the previously used standard EN 954-1 and determine the degree of risk reduction.

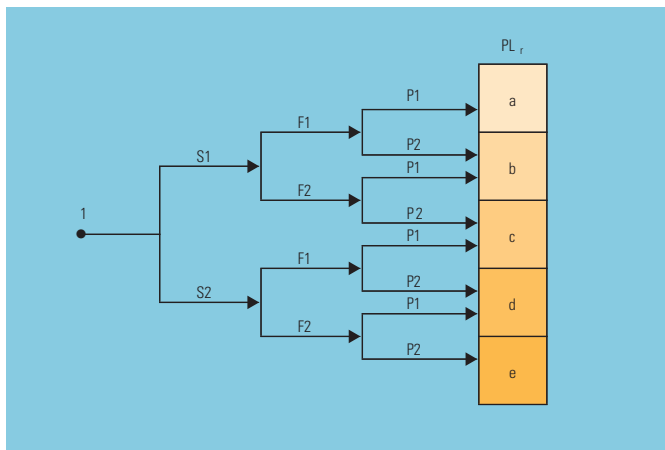


Figure 76: Risk graph from EN ISO 13849-1

Example

An additional protective measure in the form of an emergency-stop function is required for a hazardous area. This should enable the hazardous movement to be stopped in the event of an emergency, → page 20.

1.1 Estimation of the severity of injury S

Assuming the Emergency-stop device does not yet exist. What is the potential severity of injury?

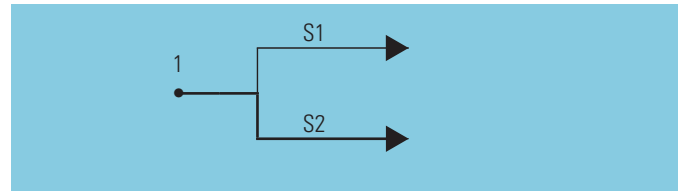


Figure 77: Estimation of the severity of harm

If injuries are reversible, such as bruises or cuts without complications choose S1. Irreversible injuries such as the loss of limbs or even fatal injuries must be categorized as S2. For our example, we will select P2.

Risk assessment also includes the frequency and/or duration of time a person is in the hazardous area.

1.2 Estimation of the frequency and/or time of exposure to hazard F

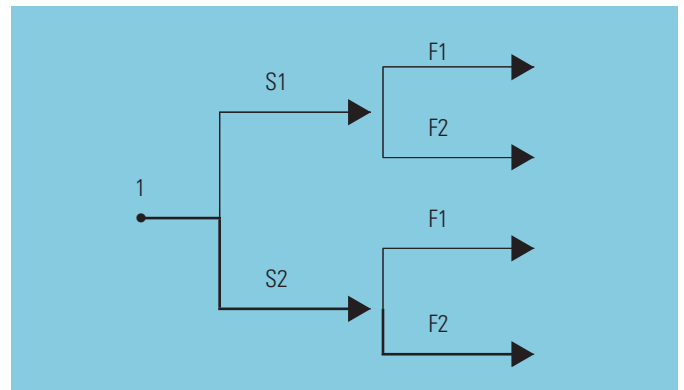


Figure 78: Frequency and time of exposure to hazard

If this is only seldom and/or for a short period, choose F1 (maximum 1 x hour). Long or frequent exposure is assessed as F2 (more than 1 x hour). For our example we choose F2.

A typical case of F2 is the intervention between the tools at regular intervals in order to remove or insert workpieces during cyclical operation. If access is only required from time to time, choose F1.

The last step deals with the question "What possibilities are there of avoiding the accident?"

The way to a safe machine

Steps to the Performance Level PL in accordance with EN ISO 13849-1

1.3 Estimation of the possibility of avoiding a hazard

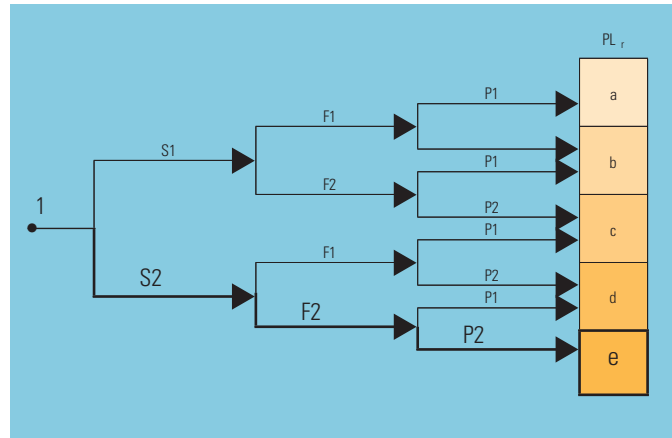


Figure 79: Possibility of hazard avoidance

P1 should only be selected if there is a realistic chance of avoiding the accident or of significantly reducing its effects. P2 should be selected if there is almost no chance of avoiding the hazard. For our example we choose P2.

An accident is especially avoidable if the hazard can be detected.

Use the following points as a guide:

- Can the hazard be determined directly on account of its physical features or only by technical means such as indicators etc.?
- Does the hazard occur suddenly, quickly and unexpectedly or slowly and visibly?
- Can the accident be avoided by escaping or by the intervention of third parties?
- Are non-professionals or experts operating the machine?
- Is operation carried out with or without supervision?
- What practical safety experience relating to the process is available?

Result

The risk estimation results in a required performance level $PL_r = PL_e$.

This procedure is not mathematically exact but is accurate in terms of quality. An estimation process that usually provides an adequate degree of accuracy with little effort. Consider it as part of the risk evaluation in accordance with EN ISO 12100 and not as a replacement for it.

Step 2: Design of control system architecture

The EN ISO 13849-1 standard provides architectures, thus providing assistance in evaluating the structure of a safety-related control system and assigning a particular category.

• Category B (basic category)

The safety-related parts of the control system shall, as a minimum, be designed in accordance with the current state of the art. They shall withstand the influences which are to be expected.

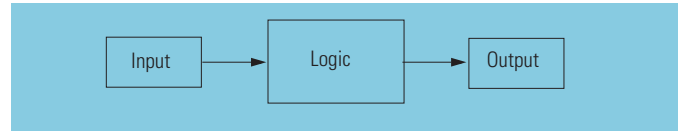


Figure 80: Structure for category B

• Category 1

The safety-related parts of the control system must be designed and constructed using well-tried components and well-tried safety principles. A well-tried safety principle is, for example, the use of position switches with positively opening contacts. Normally, the category cannot be implemented with electronic components.

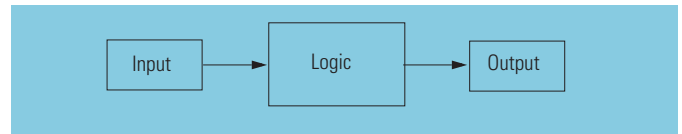


Figure 81: Structure for Category 1

• Category 2

The safety functions of the safety-related parts of a control system must be checked at suitable intervals. The check can be performed automatically or manually and at least with each startup and before a hazardous situation occurs. The check can also be carried out periodically during operation as determined by the risk analysis. A hazardous situation may occur on the machine between the checks.

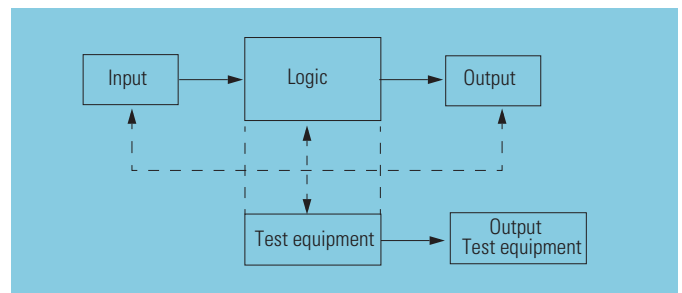


Figure 82: Structure for Category 2



• Category 3

A single fault in a safety-related part of the control system does not lead to the loss of the safety function. An accumulation of undetected faults may cause a hazardous situation on the machine, since not all faults must be detected. An example of this is the use of a redundant circuit without self monitoring.

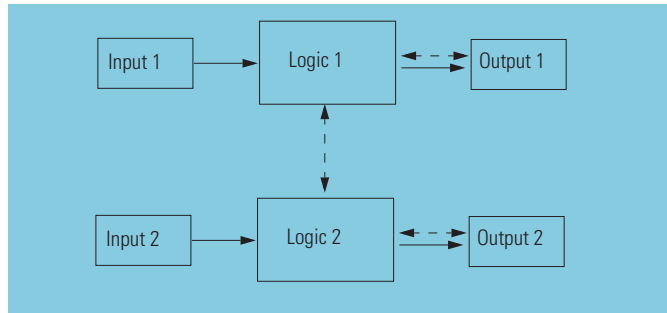


Figure 83: Structure for Category 3

• Category 4

A single fault in a safety-related part of the control system does not lead to the loss of the safety function. This fault must be detected immediately or before the next potential danger, e.g. when closing the door before a restart of the machine. If this is not possible, the accumulation of faults must not lead to the loss of the safety function.

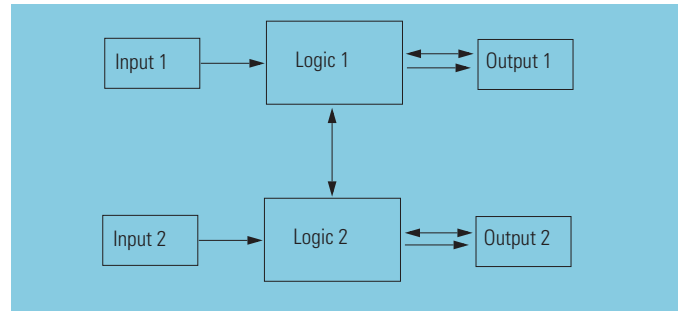


Figure 84: Structure for Category 4

Observe the following principle:

The more that risk reduction depends on the safety-related parts of the control system, the higher the resistance to faults must be.

Table 4: Summary of requirements for categories

Category	Requirements Summary	MTTF _d per channel	DC _{avg}	Common Cause
B	<ul style="list-style-type: none"> Compliance of safety-related components with the relevant standard. Withstand the factors expected. Application of basic safety principles. 	Low to medium	None	not relevant
1	<ul style="list-style-type: none"> Requirements of B category. Use of well-tried components. Use of well-tried safety principles. 	Extended	None	not relevant
2	<ul style="list-style-type: none"> Requirements of B category. Use of well-tried safety principles. Testing of the safety function at suitable intervals. 	Low to high	Low to medium	min. 65 points
3	<ul style="list-style-type: none"> Requirements of B category. Use of well-tried safety principles. A single fault does not cause the loss of safety function. Single fault must be detected in a suitable manner. 	Low to high	Low to medium	min. 65 points
4	<ul style="list-style-type: none"> Requirements of B category. Use of well-tried safety principles. A single fault does not cause the loss of safety function: <ul style="list-style-type: none"> Single fault must be detected at or before the next request, or Accumulation of undetected faults must not lead to the loss of the safety function. 	Extended	Extended	min. 65 points

The way to a safe machine

Steps to the Performance Level PL in accordance with EN ISO 13849-1

Example

Let us look at our example again. Which category must I ensure in order to achieve a performance level PL e?

View the following diagram from the standard:

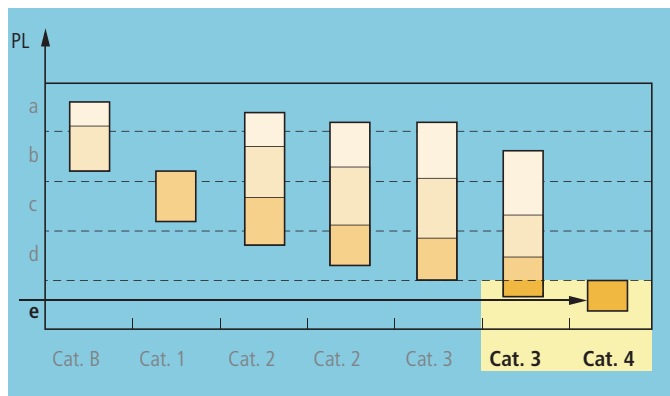
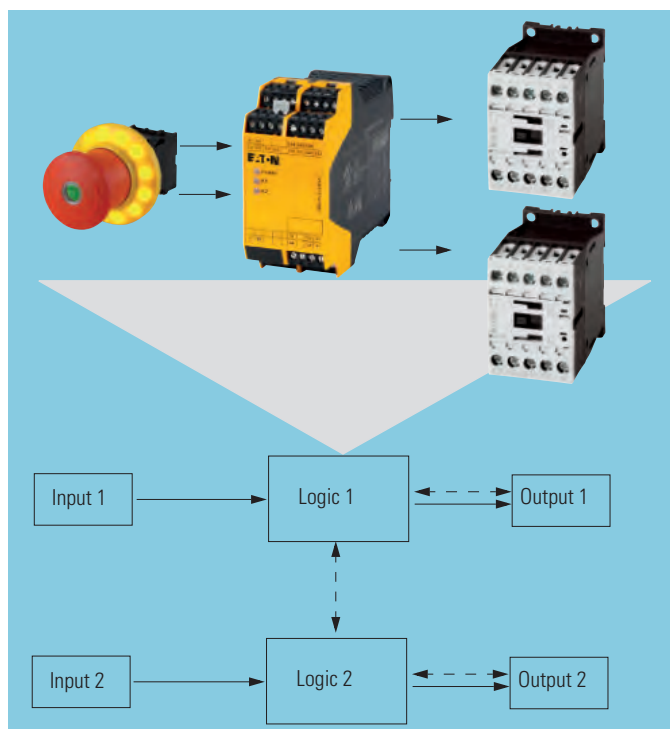


Figure 85: Possible categories for performance level PL e

Result

A performance level e is only achievable with a category 3 or 4 structure. For our example let us select a category 4 structure.

The selected example architecture corresponds to the circuit in section 1.5 "Two-channel with safety relay", page 20.



Step 3: Determining the achieved PL

Now determine the achieved performance level PL by assessing the following parameters:

Step 3.1: Control architecture (category)

Step 3.2: $MTTF_d$ – mean time to dangerous failure

Step 3.3: DC – diagnostic coverage

Step 3.4: CCF – common cause failure

Step 3.5: Relationship between the categories, $MTTF_d$, DC, CCF and PL

Let us now carry out the evaluation on the basis of our example.

3.1 Assignment of control architecture (category)

First assign the selected safety function, Emergency-stop, to the control category created in step 2.

Now assign the individual function blocks input unit, logic unit and output unit to the elements of the block diagram.

Example

For our example: The input units 1 and 2 are formed by means of the Emergency-stop device M22-PVT (→ chapter 1.5 "Two-channel with safety relay", page 20), that has the following characteristics in conjunction with the logic unit:

- Reliable detection of open circuits on the cable and in the contact.
- Reliable detection of connection faults via the contact of a channel (fault on connection cable, short-circuit to 24 V).
- Reliable detection of cross-circuits between both input channels.

The ESR safety relay represents the logic function block. It provides diagnostics functions that also act on the input and output unit.

The output units Q1 and Q2 are formed by two DILM12 and DILM25 contactors that are connected redundantly with cross-circuit detection to the logic unit (→ chapter 1.5 "Two-channel with safety relay", page 20).



3.2 Determining the MTTF_d

The MTTF_d value represents the statistical mean value until the expected dangerous failure of the components. For electromechanical components, the MTTF_d value depends primarily on the number of actuations. EN ISO 13849-1 provides the following calculation equation for this purpose:

$$MTTF_d = \frac{B10_d}{0.1 \times n_{op}}$$

B10_d: Mean number of operating cycles up to 10% of the components have failed dangerously.

n_{op}: Mean number of annual operations.

We will assume for our Emergency-stop safety function an operating frequency of 5 operations per day. The system is required to be in operation 360 days a year and two shifts per day, i.e. 16 hours per day.

This results in an n_{op} of 1800 operating cycles.

The B10_d value is specified by the component manufacturer. If no manufacturer specifications are available, Annex C EN ISO 13849-1 provides an overview with typical values as a substitute.

Example

In our example we will set a B10_d value for the Emergency-stop device of 100000 cycles (manufacturer specification) a B10_d value of 1.3·10⁶ cycles (manufacturer specification).

This results in the following values for the individual subsystems:

- Input Unit: MTTF_{d, Input} = 555.5 [years]
- Logic Unit: MTTF_{d, Logic} = 358 [years] (manufacturer specifications)
- Output Unit: MTTF_{d, Output} = 4858.6 [years]

Once all values of the individual components have been determined, determine the overall MTTF_d value for each channel.

$$\frac{1}{MTTF_{d, channel\ 1/2}} = \frac{1}{MTTF_{d, Input}} + \frac{1}{MTTF_{d, Logic}} + \frac{1}{MTTF_{d, Output}} ;$$

$$MTTF_d = 208.3 \text{ [years]}$$

If the values of both components are different, symmetrization by means of the equation D.2 from standard EN ISO 13849-1, Annex D. Symmetrization is not necessary for our example, since the structure of both channels is the same.

Result

The mean time to dangerous failure with the Emergency-stop safety function is around 208 years. The maximum to be taken into account by the standard is 100 years, which corresponds to a level based on EN ISO 13849-1 table 5 of MTTF_d = "high".

3.3 Determining the diagnostic coverage (DC)

The safety integrity can be increased by the internal testing of the subsystems. The diagnostic coverage is a measure of fault detection efficiency. The DC can be determined for parts of the safety-related system or for the entire system.

If a safety-related control system consists of several parts, an average value DC_{avg} is used for determining the achieved performance level. In complex systems a failure mode and effects analysis (FMEA) is necessary.

For simple systems, the standard supplies a simplified approach for determining the DC (see EN ISO 13849-1, Annex E).

Example

For our example, this means in real terms that we take the appropriate DC for the input, logic and output unit from the standard Table E.1.

The input unit is assigned the measure "Cross monitoring of inputs without dynamic test", i.e. a value between 0 and 99 %. We will select 99 % since a fault exclusion according to EN ISO 13849-2 is possible for the Emergency-stop device.

We select the measure Direct monitoring (monitoring of electromechanical devices by mechanically linked contact elements)", which corresponds to a DC of 99 %. The DC of the logic unit is taken from the manufacturer's specification of 99 %.

The average DC_{avg} is calculated from the following equation:

$$DC_{avg} = \frac{\frac{DC_{Input}}{MTTF_{d, Input}} + \frac{DC_{Logic}}{MTTF_{d, Logic}} + \frac{DC_{Output}}{MTTF_{d, Output}}}{\frac{1}{MTTF_{d, Input}} + \frac{1}{MTTF_{d, Logic}} + \frac{1}{MTTF_{d, Output}}} = 0.99$$

Result

The calculated average DC of the Emergency-stop device is 0.99 and this corresponds to the denotation DC_{avg} = "high" according to EN ISO 13849-1 Table 6.

The way to a safe machine

Steps to the Performance Level PL in accordance with EN ISO 13849-1

Faults and fault exclusion

A fault is characterized by the inability of an item of equipment to perform a required function. There are many types of faults which can theoretically occur. In practice you can however exclude some faults (see EN ISO 13849-2).

We have excluded the following faults in our example:

- Detaching of the auxiliary contact modules from the contactors
- Connection faults within the contactor circuit in the switching cabinet.
- Mechanical defect of the Emergency-stop actuator.

Reason: Protected mounting in the switching cabinet, well-tried technology and overdimensioning.

Take into account the following fault criteria:

- If other components fail as a result of a fault, the first fault and all resulting faults must be considered as a single fault.
- Faults with the same cause are considered as a single fault.
- The simultaneous occurrence of two separate faults is not taken into account.

3.4 Scoring process and quantification of measures against CCF

Evaluating the avoidance of common cause failures provides a qualitative assessment of resistance to external influences (e.g. ambient conditions, such as temperature/vibration/humidity).

Measures against CCF must be implemented with multi-channel systems.

Table F.1 from the EN ISO 13849-1 standard, Annex F lists suitable measures for machinery and contains appropriate values based on an engineering assessment, representing the contribution of each measure to the reduction of common cause failures.

Example

The evaluation of our example is shown in the figure below.

Use the table with the points scoring system provided to assess the measures taken to avoid common cause failures on your safety-related control system.

Only enter whole numbers as scores. If a measure is only fulfilled in part, the corresponding points number is zero. The minimum requirement is 65 points.

No.	Measures for preventing common cause failures	Score ¹⁾	
		is reached	Maximum possible
1	Separation/segregation		
	Physical isolation of signal paths:	15	15
	• Separation of wiring/conduits		
	• Sufficient creepage and clearance distances on printed circuits		
2	Diversity		
	Different technologies/design/physical principles 0	0	20
3	Design/Application/Experience		
3.1	Overvoltage protection, protection against overcurrent, overpressure, etc.	15	15
3.2	Use of well-tried components.	5	5
4	Assessment/analysis		
	Completion of a failure mode and effects analysis (FMEA)	5	5
5	Competence/Training		
	Implementation of training for designers/fitters	5	5
6	Environment		
6.1	Protection against contamination, EMC testing according to relevant standards	25	25
6.2	Insensitivity to all relevant environmental influences (temperature, shock, vibration, humidity) according to the relevant standards	10	10
	Total	80	100

1) Only enter whole numbers as scores.



Result

The minimum requirement for avoiding common cause failures (CCFs) is fulfilled with a score of 80.

3.5 Relationship between the categories, DC_{avg} , $MTTF_d$ and PL

The following chart shows the different combinations for estimating the category with DC_{avg} and the $MTTF_d$ of each channel to determine the achieved PL.

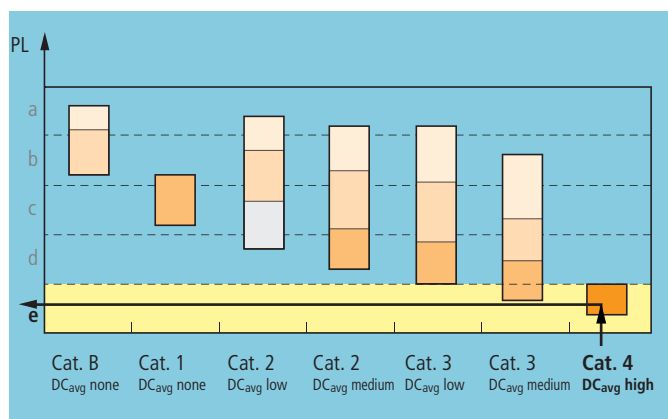


Figure 86: Calculation of the PL using $MTTF_d$, DC_{avg} and the category

PL = Performance Level

- MTTF_d each channel = low
- MTTF_d each channel = medium
- MTTF_d each channel = high

Result

With the structure of category 4, our Emergency-stop device achieves an $MTTF_d$ "high" and a high DC and a performance level of PL e (see yellow area).

Step 4: Verification of the achieved risk reductiong

The verification compares the achieved PL (step 3.5) with the required PL_r (step 1).

If the comparison shows $PL \geq PL_r$, the risk reduction is sufficient.

If the comparison shows a lesser value ($PL < PL_r$), the iterative design process must be repeated.

Result

The achieved PL corresponds to the required PL_r:

$$PL_r = PL_e = PL$$

This determines the required risk reduction.

Step 5: Validation of the safety functions

Unlike the verification, the validation is a final confirmation that the requirements for the necessary risk reduction are fulfilled by using the selected safety functions.

Draw up a validation plan as to which analyses and tests you wish, to determine compliance of the solution with the requirements. Check in each case:

- Are all safety-related output signals generated in a correct and logical fashion by the input signals?
- Does the behaviour in the event of a fault comply with the defined categories?
- Depending on the complexity of the control system and the sequences involved, a theoretical test of the circuit diagrams is sufficient. Otherwise carry out a practical test with fault simulation.
- Are the control system and the devices dimensioned sufficiently for all operating modes and ambient conditions?

The way to a safe machine

12.6 Steps to SIL safety integrity level according to IEC 62061

IEC 62061 covers the functional safety of safety-related electrical, electronic and programmable electronic control systems.

→ The German version EN 62061 (2005) is not listed additionally in this manual.

In the overall framework of EN ISO 12100 it serves as an alternative to EN ISO 13849-1 for the specification of the required safety performance of safety-related electrical control systems for the reduction of risks.

IEC 62061 is a sector specific standard beneath IEC 61508 and covers the entire life cycle of the machine (from the concept phase to dismantling) and describes the safety performance by means of the so-called safety integrity level (SIL).

The IEC 62061 does not specify any requirements for the performance of nonelectric (e.g. hydraulic, pneumatic, electromechanical) safety-related control elements for machines and refers to EN ISO 13849-1.

The safety integrity requirements of a safety-related electrical control system (SRECS) are determined from the risk analysis.

The basic principle for risk reduction is achieved by means of an iterative process like EN ISO 13849-1.

The following iterative process from IEC 62061 describes the necessary procedures to sufficiently reduce the probability of systematic and random faults that can lead to a dangerous failure of the safety function.

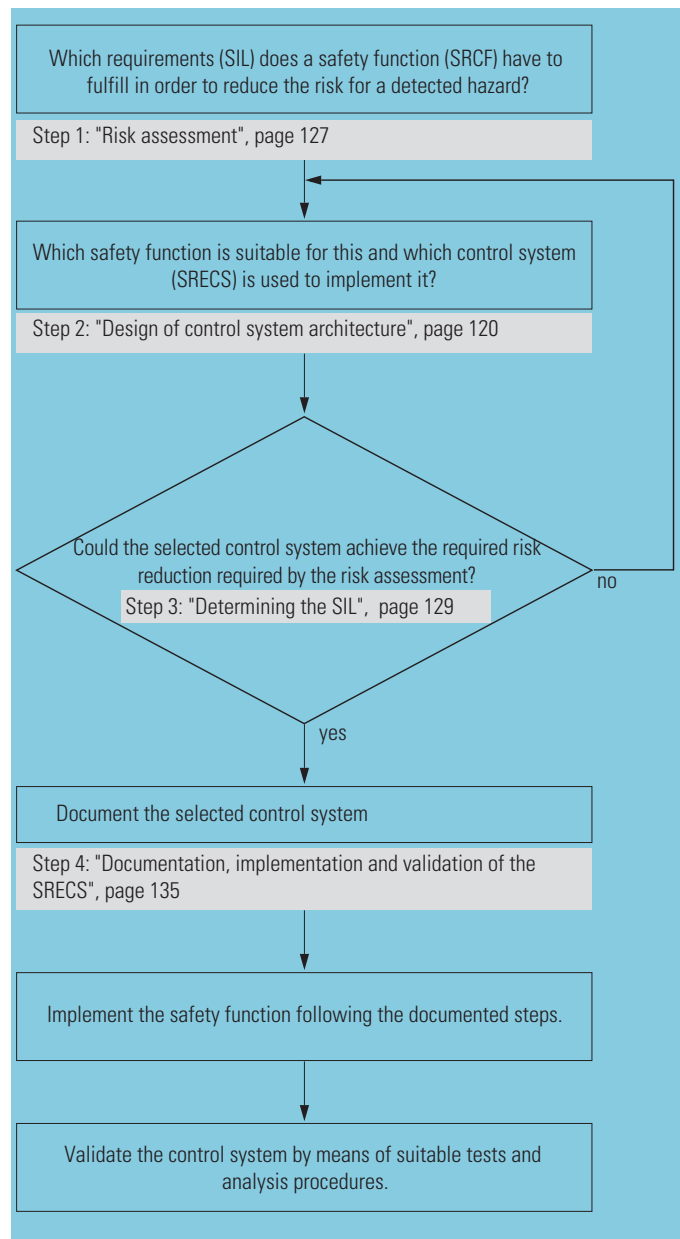


Figure 87: Design process of safety-related control systems



Step 1: Risk assessment

The need for safety-related control functions (SRCF) in accordance with IEC 62061 and their specifications are derived from the risk analysis according to EN ISO 12100.

The risk evaluation should be carried in the same way as the EN ISO 13849-1 by the assessment of individual risk parameters. IEC 62061 also considers the probability of the occurrence of a hazardous situation.

The analysis of the necessary risk reduction leads to a failure limit value for the probability of a dangerous failure per hour (PFH_d) of each SRCF.

Risk parameters to IEC 62061:

- Severity of injury S
- Probability of the occurrence of damage as a function of:
 - Frequency and time of exposure of persons to the hazard.
 - Probability of occurrence of a hazardous event Pr.
 - Possibilities to limit or avoid the harm Av.

Example

An additional precautionary measure in the form of an emergency-stop function on a machine is required for a hazardous area.

First determine the severity of injury Se. A significantly irreversible or even fatal injury is assigned the value 4, a major irreversible injury the value 3, a reversible injury 2 and a minor injury the value 1.

For the example we will select the highest severity and assign the value Se = 4.

The probability of harm CI is calculated as the sum of the individual parameters F, Pr and Av. The frequency and time of exposure to the hazard is in a range between >1 hour and ≤ 1 day and is assigned the value F = 5. We shall estimate the probability of the occurrence of the hazardous event as seldom and assign it the value Pr = 2. We shall estimate the avoidance or limitation of the injury on entry as impossible and assign the value Av = 5. This produces the following result:

$$K = F + W + P = 5 + 2 + 5 = 12$$

Enter the calculated values in the standard table to IEC 62061 (Annex A – Figure A.3).

The table shows the required safety integrity level for the safety function provided for risk reduction.

Result

For our Emergency-stop function we require a safety integrity level of SIL 3.

Frequency and time [Fr]		Probability of occurrence of a hazardous event [Pr]		Avoidance [Av]	
5	≤ 1 hour	5	frequently	—	—
5	> 1 h ... ≤ 1 day	4	probably	—	—
4	> 1 day ... ≤ 2 weeks	3	possible	5	impossible
3	> 2 weeks ... ≤ 1 year	2	rarely	3	possible
2	> 1 year	1	insignificant	1	probable

Effects	Severity Se	Class CI				
		3 - 4	5 - 7	8 - 10	11 - 13	14 - 15
Death, loss of an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, loss of fingers	3			SIL 1	SIL 2	SIL 3
Reversible, medical treatment	2				SIL 1	SIL 2
Reversible, first aid	1					SIL 1

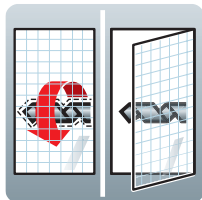
The way to a safe machine

Steps to SIL safety integrity level according to IEC 62061

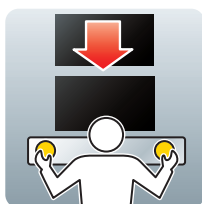
Step 2: Design of the safety function

Now design a safety-related control function (SRCF) meeting the requirements of risk reduction with the integrity level SIL determined.

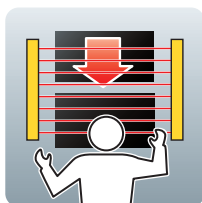
Examples of SRCF can be:



Monitoring movable guards such as a safety door, safety guard, protective cover



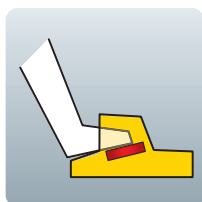
Enable safe operation with two-hand control



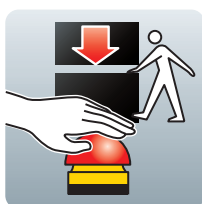
Monitor open hazardous area: e.g. with light matrix, light barriers/curtains, active optoelectronic sensors.



Enable safe setting mode with manually actuated enabling device



Enable safe setting mode with foot operated enabling device



Emergency-Stop circuits

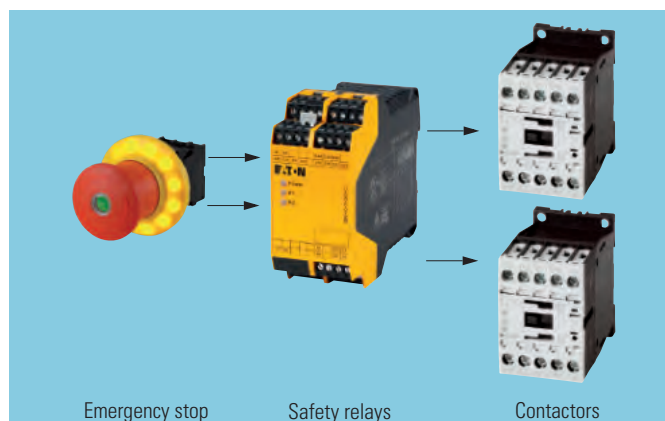
Observe the following criteria when developing and selecting the safety function:

- Features and characteristics of the machine, environment and persons operating this machine.
- Features of the machine design.
- Type and number of guards.
- Position and dimension of the guard (distance from the hazardous area, size of the protective field).
- Type and number of logic units (safety relay, safety control).

Example

We will select "Stopping in an emergency" for our example with the circuit from section 1.5 "Two-channel with safety relay", page 20.

The safety-related electrical control system (SREC) is then specified for each SRCF safety function:



Result

We will use a combination of M22-PVT emergency-stop actuator, ESR5 safety relay and DIL... contactor.

The achieved safety integrity SIL must now be defined for the designed safety function.



Step 3: Determining the SIL

After the safety-related control function SRCF is designed, the achieved safety integrity level SIL of the safety function is determined in order to determine the required risk reduction on the basis of the risk analysis. The determination of the safety integrity is carried out taking the following criteria into account:

- Probability of dangerous random hardware failure per hour (PFH_d).
- Architectural constraints for safety integrity of the hardware.
- Requirements for systematic safety integrity.

The following additional considerations are necessary to determine these criteria.

3.1 Determining the subsystem architectures

The IEC 62061 standard provides a number of basic subsystem architectures for a simple approach to determining the probability of dangerous hardware failure.

The subsystem can consist of one or several subsystem elements. The IEC 62061 standard defines a subsystem element as the part of a subsystem, which comprises an individual or a group of components.

The standard provides 4 different subsystem architectures (A,B,C,D) that offer different hardware fault tolerances (HFT) and the diagnostic functions provided. Appropriate calculation equations for each of these architectures are specified in the IEC 62061 standard.

- Basic subsystem architecture A:
Zero fault tolerance, without diagnostic function

Each failure of a subsystem element causes a failure of the SRCF. This results in a hardware fault tolerance $HFT = 0$. A diagnostic function is not provided.

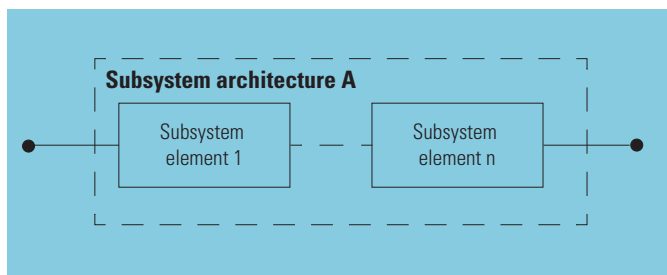


Figure 88: Logical representation of the subsystem A: Zero fault tolerance without diagnostic function

- Basic subsystem architecture B:
Single fault tolerance, without diagnostic function

A single fault of a subsystem element does not cause the loss of safety function. A hazardous fault in more than one element can cause the loss of the safety function ($HFT = 1$). The calculation also considers the susceptibility to common cause failures (β).

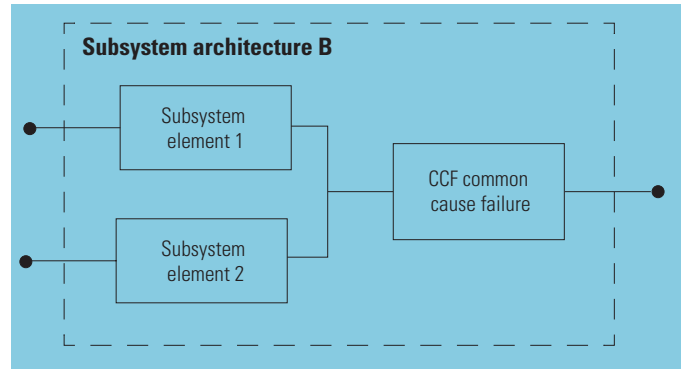


Figure 89: Logical representation of the subsystem B: Single fault tolerance without diagnostic function

- Basic subsystem architecture C:
Zero fault tolerance, with diagnostic function

Each hazardous fault of a subsystem element that is undetected causes the loss of the safety function. The DC diagnostic coverage is therefore also included.

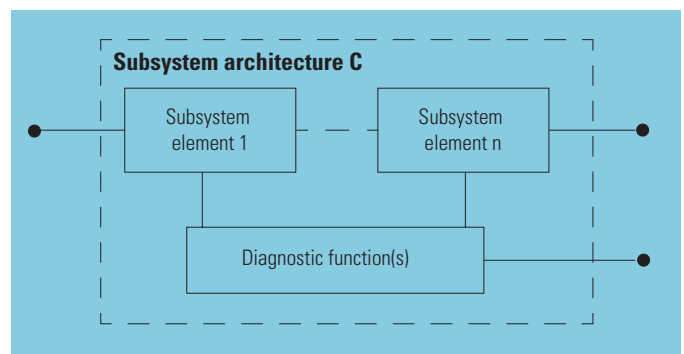


Figure 90: Logical representation of the subsystem C: Zero fault tolerance with diagnostic function

- Basic subsystem architecture D:
Single fault tolerance, with diagnostic function
- A single fault of a subsystem element does not cause the loss of the entire safety function. Two equations are provided for the calculation, with the dependence on the diagnostic coverage DC, the susceptibility to common cause failures, the diagnostic interval T_2 and the lifetime T_1 .

The way to a safe machine

Steps to SIL safety integrity level according to IEC 62061

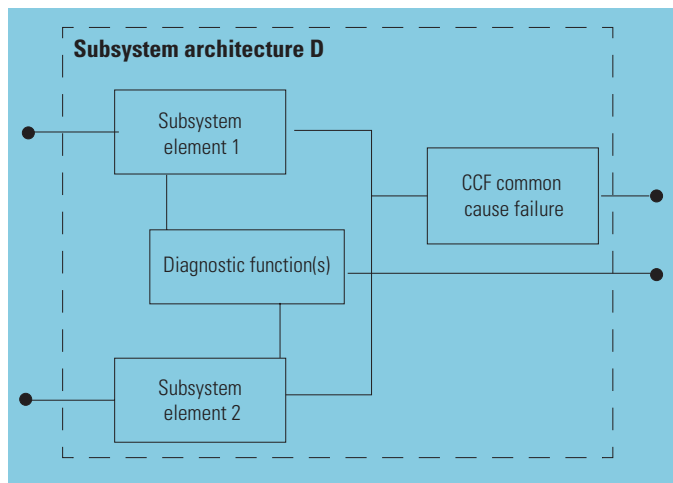


Figure 91: Logical representation of the subsystem D:
Single fault tolerance with diagnostic function

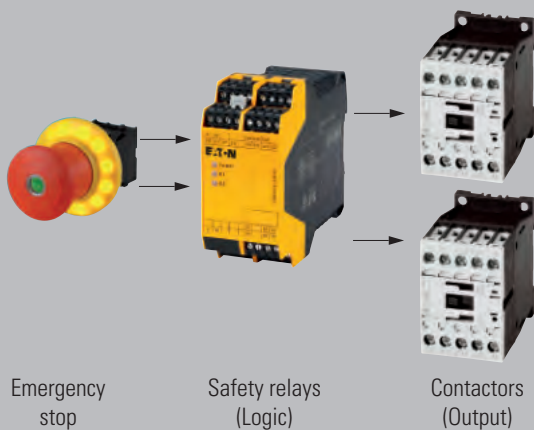
Für die Berechnung wird zwischen Teilsystem-Elementen gleicher (homogene Structure) und unterschiedlicher Konstruktion unterschieden.

Equations are provided for subsystem elements of the same (homogeneous structure) and different design. Now divide up the designed SRCF safety function, e.g. input – logic – output into function blocks, and then allocate these to subsystems.

Example

We shall divide our example into the following subsystems:

Subsystem TS1 Subsystem TS2 Subsystem TS3



Result

Each subsystem in our example complies with an architecture D with a homogeneous structure, with the assumption that both contactors are switched at the same frequency (start/stop function is ignored). There is a hardware fault tolerance of HFT = 1 for the subsystems.

3.2 Determining safety characteristics of the subsystems

The required characteristics must be determined for each subsystem to calculate the probability of a dangerous failure per hour PFH_d for subsystem architecture D.

The **subsystems** are described by the following characteristics:

SIL CL	SIL claim limit
PFH _d	Probability of a dangerous failure per hour
T1	Lifetime

The individual **subsystem elements** are described by the following characteristics:

λ_d	Dangerous failure rate
β	Characteristic value for the common cause failure
DC	Diagnostic coverage
T2	Diagnostic test interval
SFF	Safe Failure Fraction

The individual characteristics must not be determined if the PFH_d value is specified directly by the manufacturer.

Example

In our example, this applies to the subsystem SS2 – safety relay. The manufacturer's specifications can be considered for the intended use of the certified ERS4 safety relay. These are specified as:

SIL CL 3
PFH_d = 7.2×10^{-9}

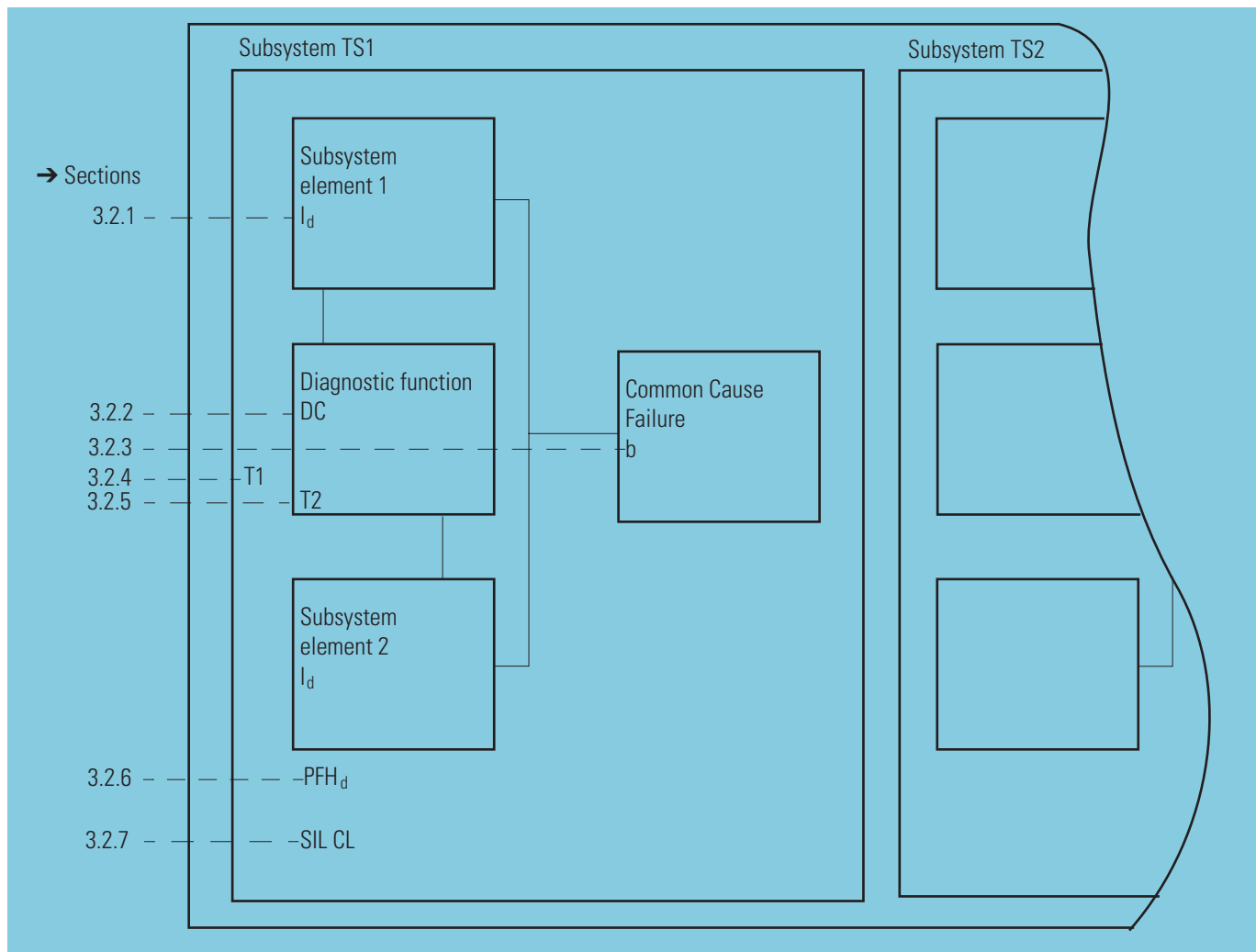


Figure 92: Stepwise determination of safety characteristic values for each subsystem

- 3.2.1 "Determining the dangerous failure rate (I_d) of the individual subsystem elements", page 132
- 3.2.2 "Determining the diagnostic coverage (DC)", page 132
- 3.2.3 "Determining common cause failures CCF (b)", page 132
- 3.2.4 "Determining the interval for the proof test or the lifetime T1 per hour", page 133
- 3.2.5 "Determination of the diagnostic test interval T2", page 133
- 3.2.6 "Determining the probability of dangerous failure of the subsystems PFH_d ", page 133
- 3.2.7 "Determining the SIL claim limit", page 134

The way to a safe machine

Steps to SIL safety integrity level according to IEC 62061

3.2.1 Determining the dangerous failure rate (λ_d) of the individual subsystem elements

The subsystem elements in the subsystems SS1 and SS3 are formed from electromechanical components. The dangerous failure rate λ_d of each subsystem element with electromechanical components is calculated with the following equations:

$$\lambda = \frac{0.1 \times C}{B10}$$

λ = Total failure rate per hour.

C = Switching frequency of the application per hour.

$B10$ = Number of operations, up to 10 % of the electromechanical devices tested that have failed (manufacturers' specifications).

$$\lambda_d = \lambda \times \text{Rate of dangerous failures}$$

λ_d = Dangerous failure rate per hour.

→ The ratio of dangerous failures is stated in this manual in the chapters 1...6 as a ratio of λ_d/λ .

The parameter C represents the operating cycles specified for the application.

If the $B10$ value is not specified by the manufacturer, an overview of typical failure rates for electrical components can be found in standard EN ISO 13849-1, Annex C.1.

$B10$ values can be calculated by using the conversion factor of 0.5 specified there.

Example

Emergency-stop device SS1 and actuator SS3:

- Operating frequency C for two 8-hour shifts per day and an actuation frequency of 5 actuations per day: $C = 0.3125$ operations per h
- $B10$ value: 20000 for SS1 / 975,000 for SS3
- Ratio of dangerous failures: 20 % for SS1 / 75 % for SS3

Result

- For the subsystem element of the Emergency-stop device TS1: $\lambda_d = 3.125 \times 10^{-7}$
- For the subsystem element of the contactors TS3: $\lambda_d = 2.404 \times 10^{-8}$

3.2.2 Determining the diagnostic coverage (DC)

Each subsystem of our example must be equipped with the associated diagnostic functions required to meet the requirements of the architectural constraints and the probability of dangerous hardware failures. To estimate the DC, the rate of detected dangerous failures is divided by the rate of total dangerous failures.

Result

- For SS1: A DC of 99% is assumed for subsystem SS1 based on the estimation of single fault probabilities and the manufacturing specifications for the Emergency-stop actuator in accordance with IEC 60947-5-1.
- For SS2: If the DC of the manufacturer is specified and assuming intended use SS2 = 99 %.
- For SS3: A redundant disconnection stage with contactors is implemented. Provided that both contactors are mounted within a protected mounting area together with the logic unit and provided that the probability is estimated, we shall set the DC of the subsystem SS 3 at 99 %.

3.2.3 Determining common cause failures CCF (β)

With multi-channel subsystems, measures are required to avoid common cause failures.

Table F.1 in Annex F of the IEC 62061 standard provides estimation criteria for the design of the subsystem. The listed criteria are assessed with a scoring system. The overall score calculated from the table F.2 of factors of common cause failures (β).

Table 5: Factor of the rate of common cause failures

Score	CCF factor (β)
< 35	10 % (0.1)
35 - 65	5 % (0.05)
65 - 85	2 % (0.02)
85 - 100	1 % (0.01)

Result

With an overall score of 57 points the CCF factor is $\beta = 0.05$.



3.2.4 Determining the interval for the proof test or the lifetime T1 per hour

The proof test is a repeated test that enables faults to be detected in a safety-related electrical control system SRECS. A proof test confirms that the SRECS is in a condition that guarantees the specified safety integrity. The proof test sets the SRECSs and the subsystems to an "as new state" if required.

The standard refers at this point to EN ISO 13849-1 and recommends a lifetime of 20 years.

Result

We shall use a proof test interval of 20 years and calculate the appropriate lifetime of:

$$T1 = 20 \text{ years} \times 365 \text{ days} \times 24 \text{ hours} = 175200 \text{ h}$$

3.2.5 Determination of the diagnostic test interval T2

The diagnostic test interval T2 is stated in hours and is the period between two diagnostic tests carried out by the system. The diagnostic test interval of each subsystem with a hardware fault tolerance of more than zero (HFT = 1), must be selected so that the subsystem can meet the requirements for the probability of a random hardware fault.

Result

The diagnostic tests of the subsystems SS1 and SS3 in our example are carried out when the contacts are triggered. This produces a test rate from the hourly actuation of both subsystem elements.

With a daily use of two shifts, i.e. 16 hours and 5 actuations, the diagnostic test interval of T2 = 3.2 hours of both subsystem elements.

3.2.6 Determining the probability of dangerous failure of the subsystems PFH_d

The single fault probabilities of the subsystems must be calculated from the individual subsystem elements in order to determine the total failure rate.

The dangerous failure rate of each subsystem can then be converted to an hourly rate.

Example

The following characteristic values can be combined from the previous steps:

	Subsystem TS1	Subsystem TS2	Subsystem TS3
λ_d	3.125×10^{-7}	PFH _d value is specified directly by the manufacturer.	2.404×10^{-8}
DC	99 %		99 %
T2	3.2 h		3.2 h
T1	175200 h		175200 h
β	0.05		0.05

The subsystems SS1 and SS3 have both elements with the same design so that the equation for structures with the same design must be used here.

$$\lambda_{d,TS} = (1 - \beta)^2 \{ [\lambda_d^2 \times 2 \times DC] \times T_2/2 + [\lambda_d^2 \times (1 - DC)] \times T_1 \} + \beta \times \lambda_d$$

$$PFH_d = \lambda_{d,TS} \times 1 \text{ h}$$

Result

The probability of a dangerous failure per hour is as follows for:

- TS1: PFH_d = 1.58×10^{-8}
- TS2: PFH_d = 7.2×10^{-9} (manufacturer's specification)
- TS3: PFH_d = 1.2×10^{-9}

The SIL for each subsystem is determined with the calculated PFH_d values using following Table from the standard.

Table 6: Determining the SIL of each subsystem

Safety integrity level SIL	Probability of a dangerous failure per hour PFH _d
3	$\cong 10^{-8} \text{ to } < 10^{-7}$
2	$\cong 10^{-7} \text{ to } < 10^{-6}$
1	$\cong 10^{-6} \text{ to } < 10^{-5}$

Result

The subsystems SS1 and SS3 of our example can each be assigned an integrity level of SIL 3.

The way to a safe machine

Steps to SIL safety integrity level according to IEC 62061

3.2.7 Determining the SIL claim limit

The SIL CL denotes the maximum SIL that can be claimed for a subsystem of the safety function in relation to architectural constraints and systematic safety integrity.

To determine the SIL CL, the hardware fault tolerance HFT and the safe failure fraction SFF are required.

- Safe failure fraction SFF

The SFF is defined as the ratio of the sum of failure rates for safe and dangerous failures detected to the overall failure rate.

A failure mode and effects analysis (FMEA) must be carried out for each subsystem in order to estimate the SFF.

$$SFF = \frac{\lambda_s + \lambda_{dd}}{\lambda_s + \lambda_d}$$

λ_s : Failure rate of safe failures

λ_d : Failure rate of dangerous failures

λ_{dd} : Failure rate of dangerous but detected failures

Intermediate result for the example::

By estimating the probabilities of each failure type we shall set an SFF for both subsystems SS1 and SS3 of 90 %.

- Hardware fault tolerance HFT

The HFT was determined in step 3.1 as $HFT = 1$.

The following table can be used with the SFF and HFT values to determine the highest SIL value that the subsystems can claim.

Table 7: Source: IEC 62061, Table 5.

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % to < 90 %	SIL 1	SIL 2	SIL 3
90 % to < 99 %	SIL 2	SIL 3	SIL 3
$\geq 99 \%$	SIL 3	SIL 3	SIL 3

Result

Both subsystems TS1 and TS3 comply with the highest safety integrity level SIL 3.

The SIL claim limit $SIL\ CL = 3$ is determined from the comparison of the SIL results for SS1 and SS3 from step 3.2.6 (SIL3) and step 3.2.7 (SIL3).

Determined by the parameters SFF and HFT, it does not restrict the safety integrity of the subsystems. Each subsystem can be assigned SIL CL 3 for the safety integrity of the SRCE.

If the SIL values are different, the lowest value is the SIL CL of the subsystem.

3.3 Determining the SIL for the entire SRECS

To assess the entire safety function, the safety integrity of the hardware is determined by the parameters PFH_d and SIL CL of the individual subsystems.

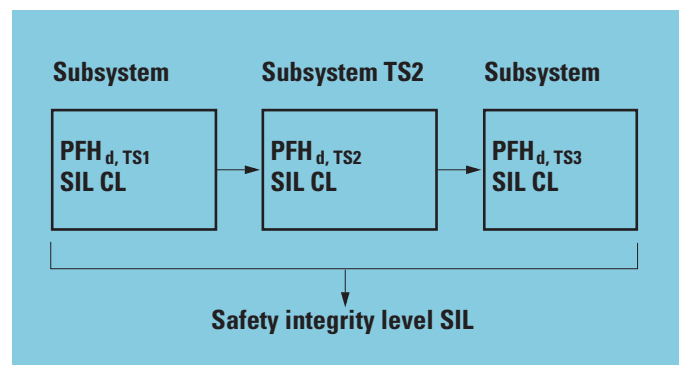


Figure 93: Determining the SIL

→ chapter 3.3.1 "Probability of dangerous failure of the entire safety function PFH_d ", page 135

→ chapter 3.3.2 "Examination of the architectural constraints for the entire system", page 135



3.3.1 Probability of dangerous failure of the entire safety function PFH_d

The probability of a dangerous hardware failure of the SRECS is the sum of the individual probabilities of all subsystems that are involved in the execution of the safety function.

$$PFH_d = PFH_{d, TS1} + PFH_{d, TS2} + PFH_{d, TS3} + \dots + PFH_{d, TSn}$$

Result

If the individual probabilities of the subsystems SS 1 to SS 3 of our example are added together, this produces the following total probability of dangerous failures:

$$PFH_d = 2.42 \times 10^{-8}$$

This value would correspond to a safety integrity level of SIL 3 in accordance with IEC 62061, Table 3. An integral evaluation of the safety integrity of the safety function must also include the architectural constraint.

3.3.2 Examination of the architectural constraints for the entire system

The SIL for the entire system achieved by the SRECS on the basis of architectural constraints must be less than or equal to the lowest SIL CL of a subsystem that is involved in the execution of the SRCF.

The design process must be repeated if the achieved SIL of the safety function is not the same as the SIL required by the risk estimation.

Result

The individual subsystems SS1/SS2/SS3 in our example each have SIL CL 3. The entire Emergency-stop system therefore achieves a safety integrity level of SIL 3.

(alternative example: An SIL CL 2 for SS 1 would lower the resulting SIL of the entire system to SIL 2.)



Faults and fault exclusion

Provided that the probability of their occurrence is low, specific faults can be excluded. Each individual fault exclusion must be substantiated sufficiently and documented.

It is also permissible to exclude faults in accordance with the EN ISO 13849-2 standard.

Step 4: Documentation, implementation and validation of the SRECS

The architecture of the SRECS with your assignment of subsystems, subsystem elements, safety functions and their interrelationships must be documented.

The implementation is the use of the SRECS in accordance with the documented SRECS design.

Ensure that the following requirements are observed:

- The appropriate parts of the SRECS safety requirements.
- The relevant requirements for wiring and cabling practice in accordance with IEC 60204-1
- The requirements for avoiding systematic hardware failures.
- The requirements for controlling systematic failures.

During the validation, the inspection and testing ensure that the design of each SRCF safety function meets the requirements of the specification.

The validation of the safety-related electrical control system according to a previously specified validation plan.

Each safety-related control function must be included and validated with suitable tests and analysis procedures. Adequate documentation must then be created, containing information on test and analysis procedures as well as the results and if necessary corrections and retests.

The documentation must be:

- Accurate and concise.
- Understood by those persons that have to work with it.
- Accessible.
- Easy to maintain.

The IEC 62061 standards provides further information on "validation and documentation".

13 Appendix

13.1 Glossary of terms

Access time (time for access to the danger zone) (ISO 14119)

The required time for access to the dangerous machine parts after the initiation of the stop command by the interlock, calculated on the basis of the speed of approach for which the value can be selected for each individual case, taking into account the parameters in DIN EN 999/ISO 13855 "Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body."

Active opto-electronic protective device (AOPD) (IEC 61496-2)

A device in which the sensor function is generated by opto-electronic sender and receiver units. The interruption of the light generated in the device by an opaque object within the defined protective field (with a light barrier: On the axis of the light beam) generates a stop signal.

AOPDs work either according to the single mode principle, in which the light beam crosses the protected area once, or according to a reflecting two-way principle by which the light beam crosses the protected area more than once.

Actuator (operating element) (IEC 60204-1)

The part of the operating system on which an external actuating force is applied.

The actuator may take the form of a handle, knob, push-button, roller, plunger etc. (IEV 441-15-22).

There are many actuating means which do not require an external actuating force but only an action.

See also machine actuator, IEC 60204-1, 3.36.

Actuator, operating element

Mechanical element of a safety position switch or a safety interlocking device which initiates the switching operation. Due to their design, the position switches and actuators are coded so that manipulation with simple tools (screwdriver, piece of wire) is not possible.

Adjustable guard (EN ISO 12100-1)

Fixed or movable guard which is adjustable as a whole or which incorporates adjustable part(s). The adjustment remains fixed during a particular operation.

Architectural constraint (IEC 62061)

Set of architectural requirements that limit the SIL that can be claimed for a subsystem.

Auxiliary circuit (IEC 60947-1/IEV 441-15-04)

All the conductive parts of a switching device or system which are intended to be included in a circuit other than the main circuit and the control circuits of the device.

Auxiliary contact (IEC 60947-1/IEV 441-15-10)

A contact which is included in an auxiliary circuit and is mechanically operated by the switching device.

Auxiliary switch (IEC 60947-1/IEV 441-15-11)

Switch containing one or more control or auxiliary contacts and which is mechanically operated by a switching device. Auxiliary switches can be retrofitted in modular systems of contactors, circuit-breakers and motor-protective circuit-breakers, or they are a fixed component of a switching device, e.g. contactor relay. They are designated according to the functions

1. Making contact as an N/C contact, N/O contact, changeover contact or fleeting contact.
2. Function as normal, early, late, drive or trip indicator switches.

Beta (β)

Factor for common cause failure.

Failure that is the result of one or several events that cause simultaneously failures of two or several separate channels in a multi-channel subsystem (redundant architecture) and lead to the failure of an → SRECS.

C

Operating cycle per hour of an electromechanical component

Category

→ (Control) category

CCF common cause failure (IEC 62061)

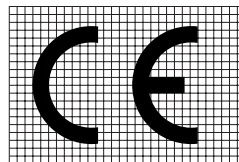
(Common Cause Failure (CCF))

Failures of different items, resulting from a single event, where these failures are not consequences of each other. Common cause failures should not be confused with common mode failures.

CE marking

(Communauté Européenne, European Community)

Marking that indicates the conformity of the marked product with the relevant European regulations and thus approval for the whole of Europe. The ruling directives are: The Machinery Directive (compulsory since 1995), the EMC Directive (from 1996) and the Low-voltage Directive (from 1997). The CE marking is not to be considered as a quality marking but as a "passport" for the free movement of goods within the European single market.



Contact, direct (IEC 60204-1)

Contact with live parts by persons or livestock (domestic animals) (IEV 826-03-05).

Contact, indirect (IEC 60204-1)

Contact with components of electrical devices by persons or domestic animals, which become live under fault conditions (IEV 826-03-06).



Contactor

Contactor which is suitable for the connection of loads in main circuits. Generally, the contactor is equipped with 3 main current paths and can be additionally equipped with further auxiliary contacts (N/O contact, N/C contact) to actuate auxiliary circuits. Contactors are classified according to their load switching capacity: Motor switching capacity AC-3 and AC-4, active load switching capacity AC-1 and conventional thermal current I_{th} .

Contactor relay (EN 60947-1/IEV 441-14-35)

Contactor for use as an auxiliary switch.

Control circuit (of a machine) (IEC 60204-1)

Circuit used for the operational control of the machine and for protection of the power circuits.

Control circuit device

Manually operated control devices for controlling, signalling, interlocking etc. of switching devices, e. g. pushbuttons, rotary switches.

Cross-circuit

Short-circuit between two channels with multi-channel circuits of safety switching devices.

Cross-circuit detection

Monitoring of the safety signals using a safety switching device by immediate or cyclical testing of the channels. In the event of a cross-circuit, the device switches to a safe state.

Current, prospective (IEC 60947-1/IEV 441-17-01)

Current which would flow in a circuit if poles of the switching device or the fuse would be replaced by conductors of negligible impedance.

Current/time characteristic curve

Graphical representation of the relationship between the overcurrent flowing through an overcurrent release or a fuse, and the time required until it trips. The curve is represented in a double-logarithmic matrix with the time on the vertical axis and the multiple of the current setting and the rated current on the horizontal axis (standard representation).

DC, diagnostic coverage (IEC 62061)

The fractional decrease in the probability of dangerous hardware failures due to automatic diagnostic tests [IEC 61508-4, 3.8.6 modified].

The diagnostic coverage (DC) can be calculated using the following equation:

$$DC = \lambda_{dd} / \lambda_{dtotal}$$

in which λ_{dd} is the rate of detected dangerous failures and λ_{dtotal} the rate of all dangerous hardware faults.

Device (IEC 60204-1)

A unit of an electrical system which is intended to carry but not utilize electric energy.

Diagnostic test interval (IEC 61508-4)

Time between online tests, to detect faults in a safety-related system with specified \rightarrow diagnostic coverage.

Emergency stop device

Arrangement of components to avert arising or to reduce existing hazards to persons, damage to machinery or to work in progress. The Emergency-Stop function must be designed such that machine operation and dangerous machine motion are halted in an appropriate manner without causing additional danger and without further action being required from any person. (emergency stop function EN ISO 13850)

Emergency stop device (EN ISO 13850)

Manually operated controlgear used for manually triggering an emergency stop function.

Emergency switching off (switch off in an emergency) (IEC 60204-1)

An operation in an emergency, designed to switch off the electrical energy supply to a complete installation or part of an installation as soon as there is a risk of electric shock or any other risk caused by electric current.

EMERGENCY-STOP (Stopping in an emergency) (IEC 60204-1)

An action in an emergency intended to stop a hazardous process or movement.

ESPE – electro-sensitive protective equipment (IEC 61496-1)

An assembly of devices and/or components working together for protective tripping or presence-sensing purposes and comprising as a minimum:

- A non-contact sensing device
- Controlling/monitoring devices
- Output switching devices

The safety-related control system associated with the ESPE, or the ESPE itself, may further include a secondary switching device, muting functions, stopping performance monitor, etc. (see Annex A).

Failure (EN ISO 13849-1)

Termination of the ability of an item to perform a required function.

After a failure, the item has a fault.

“Failure” is an event, as distinguished from “fault”, which is a state.

The concept as defined does not apply to items consisting of software only.

[IEC 60050-191:1990, 04-01]

Failures which only affect the availability of the process under control are outside of the scope of this part of ISO 13849.

Failure limit value

Intended PFHd to be achieved in order to meet the requirement(s) of safety integrity.

The failure limit value is specified as the probability of a dangerous failure per hour.

[IEC 61508-4, 3.5.13 modified]

Fault (EN ISO 13849-1)

State of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

A fault is often the result of a failure of the item itself, but may exist without prior failure.

Fault exclusion

Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault.

Fault exclusion can be based on

- the technical improbability of occurrence of some faults,
- generally accepted technical experience, independent of the considered application, and
- technical requirements related to the application and the specific hazard.

If faults are excluded, a detailed justification shall be given in the technical documentation.

Fault tolerance (Hardware fault tolerance (IEC 62061))

Ability of an SRECS, to continue the execution of a subsystem or subsystem element, a required function in the presence of faults or failures.

Feedback Circuit

The feedback circuit is used to monitor downstream, redundant contactors with mechanically linked contacts. N/C contacts of both contactors are connected in series to the feedback circuit of the safety circuit. If main or enable contact welds, reactivation a safety circuit is not possible. The safety circuit can only be switched on when the feedback loop is closed.

Fixed guard (EN ISO 12100-1)

Guard affixed in such a manner (e.g. by screws, nuts, welding) that it can only be opened or removed by the use of tools or destruction of the affixing means.

FMEA (IEC 60812)

Analysis techniques for system reliability – procedure for failure mode and effects analysis (**F**ailure **M**ode **E**ffect **A**nalysis)

Function test (IEC 60204-1)

Function tests can either be realized automatically using the control system or manually by monitoring or testing – when operational and at defined time intervals or in combination depending on the requirement.

Functional safety (IEC 62061)

Part of the safety of the machine and the machine control system that depends on the correct function of the SRECS, safety-relevant systems with different technologies and external devices to minimize risk.

Guard (EN ISO 12100-1)

Physical barrier, designed as part of the machine, to provide protection.

A guard may act:

- Alone; it is then only effective when it is “closed” for a movable guard or “securely held in place” for a fixed guard;
- In conjunction with an interlocking device with or without guard locking; in this case, protection is ensured whatever the position of the guard.

Depending on its design, a guard may be called e.g. casing, shield, cover, screen, door, enclosing guard.

See EN ISO 12100-2:2003; 5.3.2. and ISO 14120 for types of guards and their requirements.

Hazard (EN ISO 12100-1)

Potential source of harm.

The term “hazard” can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard, fire hazard).

Hazard envisaged in this definition:

- Either is permanently present during the intended use of the machine (e.g. motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature);
- Or may appear unexpectedly (e.g. explosion, crushing hazard as a consequence of an unintended / unexpected startup, ejection as a consequence of a breakage, fall as a consequence of acceleration / deceleration).

Hazardous area, danger zone (EN ISO 12100-1)

Any space within and/or around machinery in which a person can be exposed to a hazard.

Hazardous situation (EN ISO 12100-1)

Circumstance in which a person is exposed to at least one hazard. The exposure can immediately or over a period of time result in harm.

Industrial machine (IEC 60204-1)

A power-driven machine used to shape or form material by cutting, impact, pressure, electrical, thermal or optical techniques, lamination, or a combination of these processes or associated machines or equipment used in conjunction with these industrial machines to transfer raw material, work in progress, or tooling (including, fixtures); assemble/disassemble; spray or coat; inspect or test; or package. The associated electrical equipment including the logic controller(s) and associated software or logic together with the actuators and sensors are considered as part of the industrial machine.



Inherent stability

Property of a switching device that switches off at specified voltages at a current expected in the event of a short-circuit (the prospective short-circuit current) at any level (greater than 100 kA), without being affected in its function (conducting current, tripping in the event of an overload).

Inherent stability is normally obtained by damping components in the switching device which reduce a short-circuit current so that it can be switched off by the contact system. With circuit-breakers and motor-protective circuit-breakers for small rated operating currents, this is caused by the resistance in the bimetal trip and in the winding of the short-circuit release. Larger switching devices obtain this effect by the fast and wide opening of the contacts, leading quickly to an arc resistance which also limits the current. Inherent stability mainly applies to switching devices with small rated currents due to the increasing mass inertia of the contact system of large circuit-breakers.

Intended use of a machine (EN ISO 12100-1)

Use of a machine in accordance with the information provided in the instructions for use.

Interlock

The interlock of a locking device with retainer, mechanically prevents that the locking system returns to the locked position when the safety guard is open.

Interlocking device, interlock (EN ISO 12100-1)

Mechanical, electrical or other type of device, the purpose of which is to prevent the operation of hazardous machine functions under specified conditions (generally as long as a guard is not closed).

Interlocking guard (EN ISO 12100-1)

Guard associated with an interlocking device so that, together with the control system of the machine, the following functions are performed:

- The hazardous machine functions "covered" by the guard cannot operate until the guard is closed;
- If the guard is opened while hazardous machine functions are operating, a stop command is given;

When the guard is closed, the hazardous machine functions "covered" by the guard can operate. The closure of the guard does not by itself start the hazardous machine functions.

Interlocking guard with a start function (EN ISO 12100-1)

Special form of an interlocking guard which, once it has reached its closed position, gives a command to initiate the hazardous machine function(s) without the use of a separate start control.

EN ISO 12100-2:2003, 5.3.2.5, gives detailed provisions regarding the conditions of use.

Interlocking guard with guard locking (EN ISO 12100-1)

Guard associated with an interlocking device and a guard locking device so that, together with the control system of the machine, the following functions are performed:

- The hazardous machine functions "covered" by the guard cannot operate until the guard is closed and locked;
- The guard remains closed and locked until the risk due to the hazardous machine functions "covered" by the guard has disappeared;
- When the guard is closed and locked, the hazardous machine functions "covered" by the guard can operate. The closure and locking of the guard do not by themselves start the hazardous machine functions.

Isolating (VDE 0100 Part 200)

Disconnection of the entire system, a part of the system or a device from all conductors which are not grounded.

Isolating function (IEC 60947)

The function of switching devices whose switching contacts, when opened, achieve the required isolation for isolating circuits. The entire system or part of the system can thus be disconnected from the supply to ensure safety, e. g. during maintenance work.

Isolation and dissipation of energy (EN 1037)

Procedure which consists of the following four steps:

- a) Isolating (switch off, disconnection) the machine (or defined parts) from all supply sources.
- b) Locking (or securing in another way) of all isolating devices in the "isolated position" if required (e.g. with large machines or plants).
- c) Dissipating or retaining any stored energy which can cause a hazard.

Note: Energy as c) can be stored, for example, in:

- Mechanical parts which continue to move due to mass inertia;
- Mechanical parts which can move under gravity;
- Capacitors, accumulators;
- Pressurized media;
- Springs.

- d) Ensure by means of safe operation that the above measures as per a), b) and c) have the required effect.

Key-operated pushbutton (IEC 60947-5-1)

Pushbutton which can only be operated with the key inserted.

Lambda

Failure rate (per hour) of a channel in a subsystem.

Lifetime

Service life [h] of safety related components.

Light grid, light curtain, light barrier

An opto-electronic system consisting of a sender and receiver. An interruption of the emitted light beams generates a signal which can be processed further in a control system.

Limit switch

→ Position switch

Load rejection

1. Circuit measure to prevent dangerous overloads or reduce power/current peaks by disconnecting secondary loads. The load is disconnected by, for example, the trip electronics of a circuit-breaker in order to prevent an expected overcurrent trip. The load disconnection contact switches off the operating voltage of a contactor which isolates the load from the circuit.
2. Early disconnection and late connection of loads for reducing the contact load of isolating switches. The load connection is carried out by the assigned contactor control since disconnectors do not always provide the total load switching capacity.

Locking capability (IEC 60204-1)

Requirement for the functioning of a switching device as a main switch. The switching device must be lockable in the OFF position, e.g. by the attachment of at least one padlock.

Low-voltage switchgear

Switching devices for circuits up to 1000 V AC or 1500 V DC.

Machine (EN ISO 12100-1)

Assembly of linked parts or components, at least one of which moves, with the appropriate machine actuators, control and power circuits, joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material. The terms "machinery" and "machine" also cover an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

Annex A provides a general schematic representation of a machine.

Main circuit (IEC 60204-1)

A circuit for supplying power to the devices used for the production process and the control transformers.

Main switch

→ Power disconnecting device

Maintenance switch

Safety switch for the isolating of electrical drives during maintenance work.

Mechanically linked contact elements (IEC 17B/861/CD)

Combination of n N/O contact and m N/C contact elements which are connected mechanically so that they cannot be closed at the same time.

Modular system

Modular concept of switching devices which allows required functions to be added or retrofitted depending on the application, e.g. control switches, voltage releases, handles, enclosures.

Movable guard (EN ISO 12100-1)

Guard which can be opened without the use of tools.

MTBF (Mean Time Between Failure)

Mean time between two successive failures of a device.

MTTF/MTTF_d (IEC 62061) (Mean Time To Failure)

MTTF is normally expressed as an average value of expectation of the time to failure.

MTTR (Mean Time To Restoration)

Mean time to restoration (in hours).

Muting (IEC 61496-1)

A temporary automatic suspension of a safety function by safety-related parts of the control system.

Person, instructed (IEC 60204-1)

Individual adequately advised or supervised by a skilled person, to enable that individual to avoid hazards in the event of faulty behaviour, and who is trained, if required, as well as instructed on the required protection devices and measures.

PFH_d (IEC 62061)

Probability of dangerous failure per hour PFH_d.

PL, performance level (EN ISO 13849-1)

Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.

PLr, required performance level (EN ISO 13849-1)

PLr performance level (PI) applied in order to achieve the required risk reduction for each safety function.

Position switch (IEC 60947-5-1/IEV 441-14-49)

Auxiliary switch which is actuated by a moving part of the machine if this part has reached a specified position.

Position switches are divided into the following types according to their operation:

- Mechanical position switches
Actuation by means of direct contact or over-travelling of the drive head by a part of the machine. Safety position switches with separate actuators are used for the position monitoring of working machines.
- Proximity switches
Non-contact actuation by the entry of a part into the monitored area. These are inductive, capacitive and optical devices depending on their method of operation.

Position switch with safety function (IEV 441-14-50)

Position switch having positive opening operation.

Positive drive (IEC 60947-5-1)

Positive drive denotes a connection between actuator and contact element such that the force applied to the actuator is directly (without springs) transmitted to the contact element.

Positive opening (IEC 60947-1/IEV 441-16-11)

An opening operation which ensures that the main contacts of a mechanical switching device have attained the open position when the actuator is in the Off position.



Positive opening force (IEC 60947-5-1)

Actuating force or torque (of a rotary switch) which is required on the opening element obtain positive opening operation.

Positive opening travel (IEC 60947-5-1)

Minimum travel from the start of the operation of the operating element until final position of the positive opening operation of the contacts to be opened.

Power disconnecting device

A manually operated switch which is always required for the electrical equipment of machines. Its task is to disconnect the electrical equipment in order to exclude hazards occurring when cleaning, repairing, maintaining the machine concerned as well as for long periods. A power disconnecting device must:

1. Be an operating element that is externally accessible.
2. Have only one OFF and ON position with assigned limit stops. Mark the two switch positions with "0" and "I".
3. Be lockable in the OFF position.
4. Cover the connection terminals against accidental contact.

Have a minimum switching capacity for load disconnectors and motor switches for AC-23.

Proof test (IEC 62061)

Test that can detect faults and degradation in an SRECS and its subsystems so that, if necessary, the → SRECS and its subsystems can be restored to an "as new" condition or as close as practical to this condition.

A proof test confirms that the SRECS is in a condition that guarantees the specified safety integrity.

Protection type

The degree of protection of an electrical device or an enclosure provides information:

- Contact protection:
Protection of persons against contact of dangerous parts
- Protection against foreign bodies:
Protection of the operating device against the ingress of solid foreign bodies

Protection against water:

Protection of the operating device against the ingress of water. The degree of protection provided by an enclosure is indicated by the IP code (international protection) and two numbers. The first number indicates the degree of protection against contact and the ingress of foreign bodies, and the second number indicates the degree of protection against water.

Protective conductor (IEC 60204-1)

A conductor which is required for some measures of protection against electric shock, for electrically connecting any of the following parts:

- Frame.
- Extraneous conductive parts.
- Main ground terminal

Protective extra-low voltage with isolation (PELV) (IEC 364-4-41)

Low voltages up to 50 V AC and 120 V DC, which are safely isolated from other circuits and where active parts and bodies are earthed.

→ Protective extra-low voltage, safe isolation

Protective separation

Protective measure by which the operating equipment is potentially isolated from the mains supply (isolating transformer, motor generator) and not grounded.

Rated short-circuit protection, conditional (EN 60947-1/IEV 441-17-20)

The short-circuit current that a switching device, e.g. a circuit-breaker, protected by a short-circuit protective device, such as a motor-protective circuit-breaker, can carry for the duration of the tripping delay of the protective mechanism.

Redundancy (IEC 60204-1)

The application of more than one device or system, or part of a device or system with the objective of ensuring that in the event one failing to perform its function, another is available to perform that function.

Risk (EN ISO 12100-1)

Combination of the probability of occurrence of harm and the severity of that harm.

Risk evaluation (EN ISO 12100-1)

Judgement, on the basis of risk analysis, of whether the risk reduction objectives have been achieved.

Safe isolation

Reinforced or double isolation which prevents the voltage transfer from one circuit to another. The safe isolation is mainly applied between main and auxiliary circuits of switching devices as well as with safety and isolation transformers.

Safeguard (IEC 60204-1)

A → guard or safeguard is used in a safety function to protect persons from a present or impending hazard.

Safeguarding (IEC 60204-1)

Those safety measures consisting of specific technical means, called safeguards (guards, protective devices) in order to protect persons from hazards that cannot be reasonably removed or sufficiently restricted by the design.

Safeguarding, technical (EN ISO 12100-1)

Safety measures consisting of the use of specific technical means called safeguards (guards, safety devices) to protect persons from the hazards which cannot reasonably be removed or sufficiently limited by design.

Safety extra-low voltage (SELV) (IEC 364-4-41/VDE 0100 Part 410)

Protective measure by which circuits with voltages up to 50 V AC and 120 V DC, are operated ungrounded and safely isolated from circuits

with higher voltages. In the event of an insulation fault, safety extra-low voltage offers protection from high contact voltages by direct and indirect contact.

Safety measure (safety function) (IEC 60204-1)

A means that eliminates or reduces a hazard.

Safety position switches

Position switch which has a separate actuator which makes the actuator tamper proof via a mechanical coding. Safety position switches are used for position monitoring of protection coverings such as doors, flaps and shrouds.

Safety switches

Enclosed main switch very close to the drive or load, used for the release during maintenance and repair work. A safety switch is usually required if the relation between the main switch and load is not clear, or the main switch is not to be switched off. Each operator can ensure that no unauthorized person switches on the device by fitting a padlock.

Safety transformer

Isolating transformer with an output voltage ≤ 50 V. Safety transformers are used in systems with protected extra-low voltage (SELV) .

Safety-related part of a control system (EN ISO 13849-1) SRP/CS

Part of a control system that responds to safety-related input signals and generates safety-related output signals.

The combined safety-related parts of a control system start where the safety-related signals (including actuator and plunger of a position switch) are entered and terminate on the output of the power control element (including main contacts of a contactor).

If monitoring systems are used for diagnostics, they are also considered as SRP/CS.

Self maintaining

Property of a circuit in which a contactor remains in the “pick-up position” after an actuating pulse. When the actuation voltage is switched on by means of the ON actuator, this is normally bridged by an auxiliary contact of the contactor so that the voltage on the actuation coil is maintained.

Servicing level (operating level) (IEC 60204-1)

Level on which personnel normally stand when operating or maintaining electrical equipment.

SFF (IEC 62061)

Safe failure fraction.

Fraction of the overall failure rate of a subsystem that does not result in a dangerous failure.

Safe failure fraction (SFF) can be calculated using the following equation:

$$(\sum \lambda_s + \sum \lambda_{dd}) / (\sum \lambda_s + \sum \lambda_d)$$

λ_s	Rate of safe failure
$\sum \lambda_s + \sum \lambda_{dd}$	Total failure rate
λ_{dd}	is the rate of dangerous failure which is detected by the diagnostic functions.
λ_d	Rate of dangerous failure.

The diagnostic coverage (if any) of each subsystem in SRECS is taken into account in the calculation of the probability of random hardware failures. The safe failure fraction is taken into account when determining the architectural constraints on hardware safety integrity.

Short circuit (IEC 60947-1/IEV 151-03-41)

Conductive connection of two or more points in a circuit which normally have different voltages with a low resistance and impedance. The short-circuit is an operating state which causes a current exceeding the maximum current load capacity due to a fault or a faulty connection.

Short-circuit current (IEC 60204-1)

Overcurrent resulting from a short-circuit due to a fault or an incorrect connection in an electrical circuit (IEV 441-11-07).

SIL CL SIL claim limit (IEC 62061)

SIL claim limit (for a subsystem) SIL CL

Maximum SIL that can be claimed for a SRECS subsystem in relation to architectural constraints and systematic safety integrity.

SIL, Safety integrity level (EN ISO 13849-1)

Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the electrical, electronic and programmable electronic (E/E/PE) safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest safety integrity level.

Simultaneous (IEC 60204-1)

Connection actions; used to describe a situation in which two or more control circuit devices are in the actuated state at the same time (not necessarily synchronous).



Simultaneous operation (EN 574)

The simultaneous operation of both operating elements at the same time irrespective of the time difference between the start of one input signal and that of the other one.

Skilled individual (IEC 60204-1)

An individual with technical training, technical knowledge or sufficient experience as well as knowledge of valid standards, to enable that individual to judge and recognize possible dangers involved.

SRCF

Safety-related control function

Srecs

Safety-related electrical control system.

SRP/CS

→ Safety-related part of a control system – (EN ISO 13849-1)

Startup (machine startup) (EN 1037)

The transition from the stop position of a machine or part of the machine to motion.

Note: The definition includes other functions than movement functions, such as switching on a laser beam.

STOP – Category 0 (IEC 60204-1)

Stopping by immediate disconnection of the supply to the machine drives (e.g. uncontrolled stop).

STOP – Category 1 (IEC 60204-1)

Controlled stop where the supply to the machines is maintained to obtain the standstill status and the supply is only disconnected if the standstill status is achieved.

STOP – Category 2 (IEC 60204-1)

Controlled stop in which the supply to the machine drives is maintained.

Stop, controlled (IEC 60204-1)

The stopping of machine motion by setting the command signal to "0" once the stop signal has been recognized by the control system but retaining power to the machine actuators during the stopping process.

Stopping in case of emergency (EN ISO 13850)

Function intended to prevent hazards or minimize existing risks for people or of damage to machines or running processes, and which is triggered by a single action by one person.

Stopping time, time up to removal of the hazard (EN 1088)

Time from the release of the stop command by the interlocking device to the point when the risk caused by the hazardous machine function is no longer present.

Stopping, uncontrolled (IEC 60204-1)

The stopping of machine motion by removing power to the machine actuators, all brakes or other mechanical stopping devices being activated.

Switching device (IEC 60204-1)

Device for switching the current on or off in one or several circuits (IEV 441-14-01).

Synchronous actuation (EN 574)

A special case of simultaneous actuation where the time shift between the start of the input signal and the start of the other signal is less or equal to 0.5 s.

T2 (IEC 62061)

Diagnostic test interval

Tamper-proof

1. Term for the requirement of the employer's liability insurance association for protection against manipulation on position switches for the protection of personnel: "No hazardous movement of the tool (working machine) may be initiated by bypassing the protection device, e.g. by actuating the limit switch or by operation with simple tools such as screwdrivers, bolts, pieces of wire."
2. An Emergency-stop device is tamper-proof if an executed release operation cannot be cancelled without auxiliary means or prescribed procedures. The switching device locks in the release position. The accidental or controlled manipulation (inching) is excluded.

Two-hand control (EN 574)

A device that requires at least the simultaneous operation by both hands, to initiate and maintain the operation of a machine as long as a hazard is present, in order to achieve a protective measure solely for the operator.

Two-hand control, portable (EN 574)

A movable device which can be used in more than one specified position, in relation to the danger zone area of the machine which it controls.

Type A standards (EN ISO 12100-1)

These standards (safety basic standards) contain basic concepts, design principles general aspects which apply to all machines, devices and systems.

Type B standards (EN ISO 12100-1)

These standards (safety group standards) deal with a safety aspect or a kind of device required for more safety which can be used for a number of machines, devices and systems:

- Type B1 standards for certain safety aspects (e.g. safety distances, surface temperature noise);
- Type B2 standards for guards (e.g. two-hand controls, interlock devices, pressure-sensitive guards, mechanically separating guards).

Type C standards (EN ISO 12100-1)

These standards (machine safety standards) contain detailed safety requirements for a certain machine or groups of machines.

Type of coordination

State of a switchgear assembly (motor starter) during and after testing at rated conditional short-circuit current:

- Type "1" coordination:
 - No hazard to persons and systems.
 - No immediate operational readiness necessary.
 - Damage to the starter permissible.
- Type "2" coordination:
 - No hazard to persons and systems.
 - Starter is suitable for further operation.
 - No damage to the starter except slight welding of the switch contacts if these be separated easily without significant deformation.

→ Rated short-circuit current, conditional.

Undervoltage release (IEC 60947-1/IEV 441-16-42)

A release which permits a mechanical switching device to open or close, with or without time-delay, when the voltage across the terminals of the release falls below a predetermined value.

Undervoltage releases are used in emergency-stop devices, as a method of preventing restart after a voltage failure and in electrical interlocking devices.

Unexpected/unintended startup (EN ISO 12100-1)

Any unexpected startup that causes a hazard. This can be for example due to:

- A start command which is the result of a failure in, or an external influence on, the control system;
- A start command generated by inopportune action on a start control or other parts of the machine, such as a sensor or a power control element;
- Restoration of the power supply after an interruption;
- External / internal influences (e.g. gravity, wind, self-ignition in internal combustion engines) on parts of the machine.

Machine startup during normal sequence of an automatic cycle is not unintended, but can be considered to be unexpected from the point of view of the operator. Prevention of accidents in this case involves the use of safeguarding measures.

User information (EN ISO 12100-1)

Protective measures consisting of communication elements (such as texts, words, characters, signals, symbols, graphs), which are used individually or jointly to provide information to the user.

Voltage tolerance

Term for the operating reliability of a magnetic drive in terms of the limit values the applied actuating voltage.

A contactor has a satisfactory operating voltage tolerance if it is switched by the smallest permissible actuating voltage (pick-up voltage = seal-in voltage). A relatively low voltage is required for disconnection, so that no accidental switch conditions occur in the event of voltage failures. The drop-out voltage, however, may not be too low as with long control cables, is possible that the sealing current can flow even after opening the control contact, due the capacitance in the conductors, and the drop off is at least delayed.

Zero fault tolerance (IEC 62061)

Any undetected dangerous fault of the subsystem element leads to a dangerous failure of the SRCF.



Appendix

13.2 Overview of safety-related parameters

List of safety-related characteristics for Moeller SRP/CS

SRP/CS				Values according to EN ISO 13849-1			Values according to IEC 62061			
Eaton type				B10 _d [operations]	MTTF _d [years]	PL	B10 [operations]	PFH _d	SIL CL	
Input	Emergency switching off, turn-release M22-PVT..									
	N/O			2.000.000*			1.000.000			
	N/C			2.000.000*			1.000.000			
	Emergency switching off, pull release M22-PV..									
	N/O			2.000.000*			1.000.000			
	SMC-contact			2.000.000*			1.000.000			
	Emergency switching off, turn-release with MPI (switching position) M22-PVT..-MPI									
	N/O			900.000*			450.000			
	N/C			900.000*			450.000			
	Pushbutton, Mushroom actuators M22(S)-D..									
	NO			3.000.000*			1.500.000			
	N/C			3.000.000*			1.500.000			
	* For purposes of note 1 to table C.1. of DIN EN ISO 13849-1: 2008 + AC: 2009 „B10d is assumed to be twice B10“									
	Position switches									
	LS-11		1 N/C contact	1.000.000				500.000		
			1 N/O contact	20.000.000				4.000.000		
	LS-02		2 N/O contact	20.000.000				4.000.000		
Position switches with mechanical securing action										
LS-S02-24DFT-ZBZ/X			2.000.000				400.000			
Mushroom actuators (22 mm) installed in the two-hand control station										
M22-DP-Y + M22-AK11			2.000.000				1.000.000			
Operating mode selector switches										
T0-2-8241/E			2.000.000				400.000			
Logic	Safety control relay easySafety (additional information see MN05013001Z-EN)									
	ES4P-221-DMXD1	Transistor output	HFT 0		455	up to PL e		2.3 x 10 ⁻⁹	3	
	ES4P-221-DMXX1		HFT 1				4 x 10 ⁻¹⁰			
			Relay output	HFT 0				K1 + K2 x c ²		
				HFT 1				K1 + K2 x c ² + K3 x c ³		
	ES4P-221-DRXD1	Relay output	HFT 0		1 / (K1 + K2 x c) ¹⁾		K1 + K2 x c ²			
	ES4P-221-DRXX1		HFT 1			K1 + K2 x c ² + K3 x c ³				
	Safety relays ESR5**									
	ESR5-NO-41-24VAC-DC					PL c	230.000	4.05 x 10 ⁻¹⁰	1	
	ESR5-VE3-42					PL d	300.000	1.35 x 10 ⁻⁹	3	
	ESR5-NO-21-24VAC-DC					up to PL e	300.000	5.05 x 10 ⁻¹⁰		
	ESR5-NO-31-24VAC-DC						300.000	5.05 x 10 ⁻¹⁰		
	ESR5-NZ-21-24VAC-DC						300.000	1.21 x 10 ⁻⁹		
	ESR5-NO-31-AC-DC						300.000	1.26 x 10 ⁻¹⁰		
	ESR5-NO-31-230VAC					230.000	1.89 x 10 ⁻¹⁰			
	ESR5-NOS-31-230VAC					PL c	300.000	2.42 x 10 ⁻¹⁰	1	
	ESR5-NV3-30					PL e	400.000	1.80 x 10 ⁻⁹	3	
ESR5-NV3-300					300.000		3.60 x 10 ⁻¹⁰			
ESR5-NE-51-24VAC-DC					230.000		1.02 x 10 ⁻¹⁰			

** PFHd values are for one switching operation per hour



SRP/CS		Values according to EN ISO 13849-1			Values according to IEC 62061		
Eaton type		B10 _d [operations]	MTTF _d [years]	PL	B10 [operations]	PFH _d	SIL CL
Contactor monitoring devices							
CMD			125				
SmartWire-DT System		No data as preclusion of errors possible Gateway PROFIBUS DP (additional information see MN03402001Z-EN)					
Gateway PROFIBUS DP							
SWIRE-GW-DP							
Gateway easy-NET/CANopen							
easy223-SWIRE							
Power-Modul							
SWIRE-PF							
DILM-Modul							
SWIRE-DIL							
Contactor							
DILEEM/XTMC6A		869.480			652.110		
DILEM/XTMC9A							
DILM7/XTCE007B, DILM9/XTCE009B, DILM12/XTCE012B		1.782.229			1.336.672		
DILM17/XTCE018C, DILM25/XTEC025C, DILM32/XTEC032C		966.617			724.963		
DILM40/XTCE040D, DILM50/XTCE050D, DILM65/XTCE065D		1.341.161			1.005.871		
DILM115/XTCE115G, DILM150/XTCE150G		1.705.268			1.278.951		
Circuit-breakers with undervoltage releases							
NZM1		10.000			2.000		
NZM2							
NZM3		7.500			1.500		
Variable Speed Drives							
DC1			4.525	PL d		1.23 x 10 ⁻⁹	2
DA1							

- ¹⁾ K1 = 6.3 x 10⁻⁴, K2 = 1.2 x 10⁻³, c = operating frequency per hour
²⁾ K1 = 1.3 x 10⁻⁹, K2 = 1.3 x 10⁻⁸, c = operating frequency per hour
³⁾ K1 = 4.0 x 10⁻¹⁰, K2 = 2.6 x 10⁻¹¹, K3 = 2.7 x 10⁻¹⁰, c = operating frequency per hour

SRP/CS	Safety-related parts of control systems
MTTF _d	Mean Time To Failure dangerous
B10 _d	Number of operations until 10% of the components fail dangerously.
B10	Number of operations until 10% of the tested components fail.
PFH _d	Probability of dangerous failure per hour
SILCL	Safety Integrity Level Claim Limit
PL	Performance Level
HFT	Hardware fault tolerance

Appendix

13.3 Safety integrity for circuits in chapters 1 to 6

1 Stopping in an emergency (Emergency-stop disconnection)

1.1 „In the main circuit“, page 12	Cat	B	1	2	3	4
1.2 „In the control circuit for simple drives“, page 14	PL	a	b	c	d	e
1.3 „For interrupting several control circuits with safety relay“, page 16	SIL	1	2	3		
1.4 „For interrupting several control circuits with easySafety “, page 18						

1.5 „Two-channel with safety relay“, page 20	Cat	B	1	2	3	4
1.6 „Two-channel with easySafety “, page 22	PL	a	b	c	d	e
1.7 „With electronically controlled drives“, page 24	SIL	1	2	3		

1.8 „Two-channel configuration with variable frequency drive using STO“, page 26	Cat	B	1	2	3	4
1.9 „With SmartWire-DT“, page 28	PL	a	b	c	d	e
1.10 „With CMD contactor monitoring relay“, page 30	SIL	1	2	3		

1.11 „Single-channel with EMS electronic motor starter“, page 32	Cat	B	1	2	3	4
	PL	a	b	c	d	e
	SIL	1	2	3		

1.12 „Two-channel configuration with EMS electronic motor starter, safety shutdown“, page 34	Cat	B	1	2	3	4
	PL	a	b	c	d	e
	SIL	1	2	3		

2 Monitoring a movable guard

2.1 „Single-channel with safety relay“, page 36	Cat	B	1	2	3	4
2.2 „Single-channel with easySafety “, page 38	PL	a	b	c	d	e
	SIL	1	2	3		

2.3 „Several guards with safety relay“, page 40	Cat	B	1	2	3	4
	PL	a	b	c	d	e
	SIL	1	2	3		

2.4 „Several guards with easySafety “, page 42	Cat	B	1	2	3	4
	PL	a	b	c	d	e
	SIL	1	2	3		

2.5 „Two-channel with safety relay“, page 44	Cat	B	1	2	3	4
	PL	a	b	c	d	e
	SIL	1	2	3		

2.6 „Two-channel with safety relay and RS2“, page 46	Cat	B	1	2	3	4
	PL	a	b	c	d	e
	SIL	1	2	3		

2.7 „Two-channel configuration with safety relay and redundant RS2“, page 48	Cat	B	1	2	3	4
	PL	a	b	c	d	e
	SIL	1	2	3		



2.8 „Two-channel with **easySafety**“, page 50

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

2.9 „With guard locking – enable via timer“, page 52

2.10 „With guard locking – enable via zero speed monitoring“, page 54

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

3 Monitoring open hazardous area

3.1 „With light curtain and safety relay“, page 56

3.2 „With light curtain and **easySafety**“, page 58

Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

3.3 „With light curtain muting and **easySafety**“, page 60

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

4 Enabling safe operation

4.1 „With two hand control type III C“, page 62

4.2 „With two hand control type III C“, page 64

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

5 Enabling setting

5.1 „With operating mode selector switch“, page 66

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

6 Combining several safety functions

6.1 „Stopping in an emergency (Emergency-stop disconnection)“, page 68

Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

6.2 „Monitoring a movable guard“, page 70

Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

6.3 „Speed monitoring with **easySafety**“, page 72

Case A

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

Case B

Cat	B	1	2	3	4
PL	a	b	c	d	e
SIL	1	2	3		

“Hazardous” machines and safety components in accordance with Annex IV of the Machinery Directive 2006/42/EC

Categoryn von Maschinen, für die eines der Verfahren nach Artikel 12 Absätze 3 und 4 anzuwenden ist.

1. Categories of machinery to which one of the procedures referred to in Article 12 (3) and (4) must be applied. 1. Circular saws (single- or multi-blade) for working with wood and material with similar physical characteristics or for working with meat and material with similar physical characteristics, of the following types:
 - 1.1 Sawing machinery with fixed blade(s) during cutting, having a fixed bed or support with manual feed of the workpiece or with a demountable power feed;
 - 1.2 Sawing machinery with fixed blade(s) during cutting, having a fixed bed or support;
 - 1.3 Sawing machinery with fixed blade(s) during cutting, having a built-in mechanical feed device for the workpieces, with manual loading and/or unloading;
 - 1.4 Sawing machinery with movable blade(s) during cutting, having mechanical movement of the blade, with manual loading and/or unloading.
2. Hand-fed surface planing machinery for woodworking.
3. Thicknessers for one-side dressing having a built-in mechanical feed device, with manual loading and/or unloading for woodworking.
4. Band-saws with manual loading and/or unloading for working with wood and material with similar physical characteristics or for working with meat and material with similar physical characteristics, of the following types:
 - 4.1 Sawing machinery with fixed blade(s) during cutting, having a fixed or reciprocating-movement bed or support for the workpiece;
 - 4.2 Sawing machinery with blade(s) assembled on a carriage with reciprocating motion.
5. Combined machinery of the types referred to in points 1 to 4 and in point 7 for working with wood and material with similar physical characteristics.
6. Hand-fed tenoning machinery with several tool holders for woodworking.
7. Hand-fed vertical spindle moulding machinery for working with wood and material with similar physical characteristics.
8. Portable chainsaws for woodworking.
9. Presses, including press-brakes, for the cold working of metals, with manual loading and/or unloading, whose movable working parts may have a travel exceeding 6 mm and a speed exceeding 30 mm/s.
10. Injection or compression plastics-moulding machinery with manual loading or unloading.
11. Injection or compression rubber-moulding machinery with manual loading or unloading.
12. Machinery for underground working of the following types:
 - 12.1 Locomotives and brake-vans;
 - 12.2 Hydraulic-powered roof supports.
13. Manually loaded trucks for the collection of household refuse incorporating a compression mechanism.
14. Removable mechanical transmission devices including their guards.
15. Guards for removable mechanical transmission devices.
16. Vehicle servicing lifts.
17. Devices for the lifting of persons or of persons and goods involving a hazard of falling from a vertical height of more than three metres.
18. Portable cartridge-operated fixing and other impact machinery.
19. Protective devices designed to detect the presence of persons.
20. Power-operated interlocking movable guards designed to be used as safeguards in machinery referred to in points 9, 10 and 11.
21. Logic units to ensure safety functions.
22. Roll-over protective structures (ROPS).
23. Falling-object protective structures (FOPS)..



Indicative list of the safety components referred to in Article 2(c)

1. Guards for removable mechanical transmission devices.
2. Protective devices designed to detect the presence of persons.
3. Power-operated interlocking movable guards designed to be used as safeguards in machinery referred to in items 9, 10 and 11 of Annex IV.
4. Logic units to ensure safety functions.
5. Valves with additional means for failure detection intended for the control of dangerous movements on machinery.
6. Extraction systems for machinery emissions.
7. Guards and protective devices designed to protect persons against moving parts involved in the process on machinery.
8. Monitoring devices for loading and movement control in lifting machinery.
9. Restraint systems to keep persons on their seats.
10. Emergency stop devices.
11. Discharging systems to prevent the build-up of potentially dangerous electrostatic charges.
12. Energy limiters and relief devices referred to in sections 1.5.7, 3.4.7 and 4.1.2.6 of Annex I.
13. Systems and devices to reduce the emission of noise and vibrations.
14. Roll-over protective structures (ROPS).
15. Falling-object protective structures (FOPS).
16. Two-hand control devices.
17. Components for machinery designed for lifting and/or lowering persons between different landings and included the following list:
 - a) Devices for locking landing doors;
 - b) Devices to prevent the load-carrying unit from falling or unchecked upwards movement;
 - c) Overspeed limitation devices;
 - d) Energy-accumulating shock absorbers,
 - non-linear, or
 - with damping of the return movement;
 - e) Energy-dissipating shock absorbers;
 - f) Safety devices fitted to jacks of hydraulic power circuits where these are used as devices to prevent falls;
 - g) Electric safety devices in the form of safety switches containing electronic components..

Appendix

13.5 Requirements for existing machines

Interpretation paper of the German Federal Ministry of Labour and Social Affairs on the subject of „Substantial Modifications to Machinery“ [„Wesentliche Veränderung von Maschinen“] (Announcement of the German Federal Ministry of Labour and Social Affairs from April 9, 2015 concerning the German Product Safety Act / Ninth Ordinance to the Product Safety Act [9. ProdSV])

This interpretation paper is the version of the interpretation paper by the German Federal Ministry of Labour and Social Affairs (BMA) and the German states, revised as required for the new German Product Safety Act1 (ProdSG) and based on the latest insights from risk assessments, on the subject of “Substantial Modifications to Machinery,” Announcement of the BMA from September 7, 2000 - Illc3-39607-3 - Bundesarbeitsblatt (German Federal Labor Law Gazette) 11/2000, p. 35.

ProdSG governs the provision of products on the market. These products include machinery. Together with the Ninth Ordinance to the Product Safety Act (Maschinenverordnung - 9. ProdSV), ProdSG sets forth the requirements that machines must meet when they are provided on the market. 9. ProdSV and ProdSG incorporate the applicable European Directive, i.e., the Machinery Directive, into German law.

Any modification to a machine, regardless of whether the machine is used or new, that may prejudice the legal rights set forth in ProdSG, e.g., as a result of output increases, functional changes, changes in intended use, etc., must first be assessed in terms of its safety-relevant impact. This means that it is necessary to determine, on a case-by-case basis, whether the modification to the (used) machine has resulted in new hazards or whether an existing risk has been increased.

Three different scenarios can be assumed:

1. There is no new hazard or no increased risk so that the machine can still be considered as safe.
2. There is a new hazard or an increased risk, but the machine's safety measures that existed before the modification are sufficient for the machine to continue to be deemed safe.
3. There is a new hazard or an increased risk, and the existing safety measures are not sufficient to deal with it.

Additional safety measures are not required in the case of altered machines that fall under case 1 or 2. In contrast, altered machines that fall under case 3 must be evaluated with a risk assessment in order to determine whether there is a substantial modification.

The first step is to determine whether it is possible to make the machine safe again with the use of simple protective devices, i.e., so that the risk does not increase in comparison to the machine's original safe condition. If this is the case, the modification can generally be considered not to be substantial. Otherwise, a more extensive risk assessment must be conducted.

A “simple protective device” within this context can be, for instance, a fixed guard. Movable guards and safety devices that do not significantly affect the machine's existing safety controller are also considered simple protective devices. “Do not significantly affect” means that these protective devices are simply used to connect signals that the existing safety controller is already designed to process or that they only bring about the safe stopping of the machine function posing the hazard independently of the existing safety controller.

Replacing machine components with identical components or with components with the exact same function and safety level, as well as installing protective devices that result in an increase in the machine's safety level and that do not provide any additional functions, is not considered making substantial modifications.

Note:

Regardless of this, other legal regulations may require employers that provide their employees with machinery for use as work equipment to establish additional safety measures.

Generally, a risk assessment must be conducted in accordance with § 3 of the German Ordinance on Industrial Safety and Health 9 (Betriebssicherheitsverordnung 9) after any modifications are made to machines, including modifications that are not considered substantial. This assessment is part of the industrial occupational health and safety obligations of any user of a machine or system using this machine or system as work equipment. This risk assessment may render measures - especially technical measures - necessary in order to provide employees with safe work equipment.

It is necessary to determine whether the information on how to safely operate the machines, e.g., the operating instructions, needs to be modified as well.

Conclusion:

Modifications to a machine/assembly of machinery can have the following effects:

1. The machine continues to be safe after the modification even without additional safety measures.
→ These is no substantial modification.
2. After the modification, the machine is no longer safe without additional safety measures. The new hazard or increased risk can be eliminated, or at least sufficiently minimized, with simple protective devices.
→ These is no substantial modification.
3. After the modification, the machine is no longer safe without additional safety measures, and simple protective devices will not be enough to reduce the risk sufficiently.
→ There is a substantial modification.

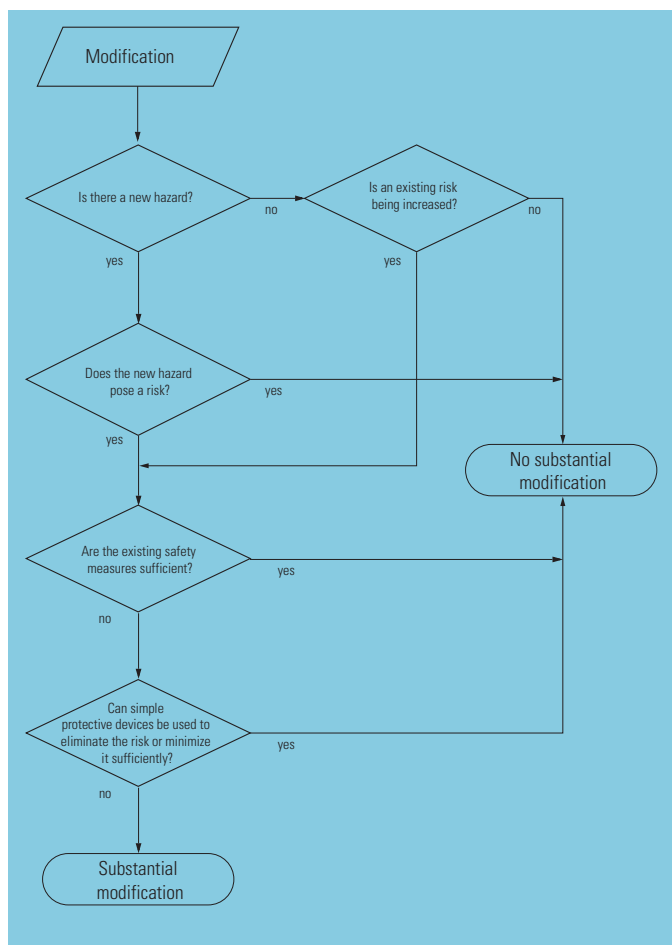


Figure 94: Steps for making a decision - substantial modifications to machinery

Application of the Machinery Directive (MD) for old or series machines

Old machines are considered as in the interpretation paper of the Federal Ministry of Labour and Social Affairs and the states on the "Significant modification of machines". In this case, the application of the MD depends on the scope of modifications of the machine.

The series produced machines are subject directly to the MD provisions.

The new Machinery Directive 2006/42/EC has been in force since 29.12.2009. A machine that was modified considerably as described above and was brought into circulation after 29.12.2009 must comply with the requirements of the new MD. The validity of the previous MD 98/37/EC elapsed on 28.12.2009.

Appendix

13.6 Reference sources for regulations, bibliography

Reference sources for regulations

Order addresses for the new regulations (without claim to be complete)

EU Directives

Bundesanzeiger Verlagsgesellschaft mbH

Amsterdamer Straße 192
50735 Köln
Germany
Telefon +49 (0) 221 97668-0
www.bundesanzeiger.de

Carl Heymanns Verlag KG

Luxemburger Straße 449
50939 Köln
Germany
Telephone +49 (0) 221 - 943730
www.heymanns.com

DIN EN standards

DIN Deutsches Institut für Normung e.V.

10772 Berlin
Germany
Telephone +49 (0) 30 - 2601-0
www.din.de

Beuth-Verlag GmbH

Burggrafenstraße 6
10787 Berlin
Germany
Telephone +49 (0) 30 - 26 01-0
www.beuth.de

European safety standards (EN) - Lists

VDMA

Lyoner Straße 18
60528 Frankfurt
Germany
Telephone +49 (0) 69 - 66 0-0
www.vdma.org

German Equipment Safety Act (GSG)

Carl Heymanns Verlag KG

Luxemburger Straße 449
50939 Köln
Germany
Telephone +49 (0) 221 - 943730
www.heymanns.com

Wirtschaftsverlag NW

Verlag für neue Wissenschaft GmbH
Bürgermeister-Schmidt-Str. 74 - 76
27568 Bremerhaven
Germany
Telefon +49 (0) 471 - 94 54 4-0
www.nw-verlag.de

List of "machines" in accordance with the Equipment Safety Act (GSG)

W. Kohlhammer GmbH

Heißbrühlstraße 69
70565 Stuttgart
Germany
Telefon +49 (0) 711 - 7 86 3 - 0
www.kohlhammer.de



Bibliography

- Main catalogue
HPL 0200-2010 Eaton Industries GmbH, Bonn
- Wiring manual
FB0200-004DE, Eaton Industries GmbH, Bonn
- Effect of the Cable Capacitance of Long Control Cables on the Actuation of Contactors.
Dipl.-Ing. Dirk Meyer,
Moeller, Bonn
- EN ISO 12100-1
Safety of machinery – ...
- EN ISO 12100-2
Safety of machinery – ...
- EN ISO 13850
Safety of machinery – Emergency-stop equipment – Principles for design
- EN 574
Safety of machinery – Two-hand controls, ...
- EN ISO 13849-1
Safety of machinery – Safety-related parts of control systems
- IEC 62061
Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems
- EN 1037
Safety of machinery – Prevention of unexpected startup
- EN ISO 14121
Safety of machines – risk assessment
- ISO 14119
Safety of machinery – Interlocking devices associated with guards
- IEC 60 204-1
Safety of machinery – Electrical equipment of machines
- IEC 60947-1
Low-voltage switchgear and controlgear
- DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)
- German Equipment Safety Act /9th (GSG)
- Interpretation paper of the Federal Ministry of Labour and Social Affairs and the states on the issue of "Significant Modifications to Machines Decl. of FML dated 7 September 2000 – IIIc 3-39607-3 – (BArbBl. 11/2000 p. 35
- BGIA Report (02/2008)
Functional safety of machine controls
German statutory accident insurance system (DGUV)
- Safety of machinery – Explanation of the application of standards IEC 62061 and EN ISO 13849-1
ZVEI – Central association of the electrical and electronic industry

A

Architectural constraints, for the entire system	135
Arranging devices effectively	96
Automatic start AST	76
Automatic stopping	113
Auxiliary release mechanism, manual	110
Avoiding danger, estimation	120

B

Basic standards	92
Bibliography	155

C

Cable length	94
Categories, summary	121
CCF	124
CE marking	99
Characteristic values, safety technical	130
Clearances	116
CMD contactor monitoring device	28
Common cause failure CCF	124, 132
Control actuators	116
Control system architecture, design	120
Controlled start CST	76
Covers	114
Create a factory standard	98
Current supply	92

D

Damage assessment	119
Danger, frequency and time	119
Dangerous failures	133
Dangerous failures PFHd	135
Dead man's switch	66
Declaration of conformity	98
Define diagnostic coverage (DC)	123
Define diagnostic test interval	133
Define MTTFd	123
Define performance level (PL)	122
Define short-circuit protective device	93
Define SIL	129
Design	103
Designing a control circuit correctly	92
Devices for isolation	112
Diagnostic coverage (DC)	132
Display	116
Dissipation of stored energy	113
Diversity	96
Documentation, SRECS	
Implementation, SRECS	135
Draft	106

Draft standards	100
-----------------------	-----

E

Electro-sensitive protective equipment (ESPE)	56, 58, 60
EMC Directive	101
Emergency stop	116
Function sequence	111
Emergency-stop	
Actuators	112
Operation	111
Emergency-stop disconnection	
Contactor monitoring device CMD	28
For disconnecting simple drives	14
For interrupting several circuits with easySafety	18
For interrupting several circuits with safety relays	16
Main circuit	12
Single-channel with EMS electronic motor starter	32
Two-channel configuration with EMS electronic motor starter	34
Two-channel configuration with variable frequency drive using STO	26
Two-channel with easySafety	22, 68
Two-channel with safety relay	20
With electronically controlled drives	24
With SmartWire-DT	28
Energy isolation and dissipation	116
EU Directive	100
European safety concept	100
European standards	100
External monitor EM (safety function block)	78

F

Failure rate, dangerous	132
Fault exclusion	124, 135
Feedback Circuit	78, 96
Functional aspects	108
Fuse	93

G

Glossary of terms	136
Group standards	101
Guard	
Device, two-channel	46
Guard door	
Monitoring, single-channel	36
Guard ring	114



H		Two-channel with easySafety	50
Hardware fault tolerance HFT	134	Two-channel with safety relay	44
Hazard analysis	105	Two-channel with safety relay and RS2	46
Hazard removal	103	Two-channel with safety relay and redundant RS2	48
		Multiple control cables	94
		Muting sensors	61
<hr/>			
I		N	
IEC	9	No current principle	14
Implementation	106		
Inherently safe design	103		
Inside distance	114	O	
Integrate a safety concept	98	Old machines	153
Interlocking features	108	Open hazardous area	
ISO	9	Light curtain and easySafety	58
Isolating and dissipating energy	112	Light curtain and safety relay	56
Isolation, partial	84	Light curtain muting	60
Iterative process	10, 118	Operating guidelines	5
		Operating mode switch OS (safety function block)	66
		Operating mode switches	66
		Overspeed monitoring OM (safety function blocks)	73
<hr/>			
J		P	
Jog Mode	66	Partial isolation	84
		PELV	90
		Performance Level	10
		Performance Level (PI)	
		Stepwise determination in accordance to EN ISO 13849-1 108	
		Performance tests	96
		Photoelectric circuit	88
		Power disconnecting device	
		Main switches	82
		Power supply disconnection	
		Emergency-stop function	12
		Precautionary measures	104
		Prepare operating instructions	98
		Prepare technical documentation	98
		Preventing misuse	97
		Preventing restarts	
		With contactors	74
		With easySafety	76
		With feedback circuit	78
		Preventing unexpected startup	80
		Product standards	101
		Proof Test	133
		Protection against direct and indirect contact	90
		Protective measures, additional	103
		Protective separation	88
		Proven circuit design	96
<hr/>			
K			
Key-switches	66, 80, 113		
<hr/>			
L			
Lifetime	123		
Light curtain	56, 58		
Light curtain muting	60		
Limit speed	73		
Limits of a machine	105		
Locking device, spring interlock	110		
Low-voltage Directive	101		
<hr/>			
M			
Machine specific standards	116		
Machinery Safety Directive	8, 101, 150		
Main switch, for Emergency-stop	12		
Main switches	113		
Maintenance -> Repair and maintenance			
Manual start MST	76		
Mechanical position switches	109		
Mirror contact	19, 31		
Movable guard	70		
Enable via timer element	52		
Enable via zero speed monitoring	54		
Several guards with easySafety	42		
Several guards with safety relay	40		
Single-channel with easySafety	38		
Single-channel with safety relay	36		

R

Redundancy	96
Reference sources, standards	154
Repair and maintenance	
Disconnecting devices	84
Power disconnecting device with main switch	82
Switch-on prevention by safety switch	86
Residual risks	103
Risk	
analysis	8
assessment	127
Estimation	105
estimation	119
Estimation and evaluation, overview	104
Evaluation	103, 105
Graph to EN ISO 13849-1	119
parameter	127
Reduction	8, 103
Reduction, verification	125

S

Safe failure (SFF)	134
Safe isolation PELV	90
Safe operation, with two-hand control (easySafety)	64
Safe operation, with two-hand control (ESR5)	62
Safety extra-low voltage	90
Safety features	116
Safety features, technical	103
Safety function block	
Zero speed monitoring ZM	104
Safety function blocks	
EM, external monitor	78
OM, overspeed monitoring	73
OS, operating mode switch	66
Safety function relays	
TS, Safety timing relay	52
Safety function, draft	128
Safety group standards	117
Safety Instructions	5
Safety Integrity Level (SIL)	
Steps to determine according to IEC 62061	126
Safety integrity level (SIL)	10, 107
Safety interlock	52
Safety position switches	108
Safety technical characteristic values	130
Safety technical data	
Moeller devices	146
Safety timing relay TS (safety function block)	52
Securing device	98
Self maintaining	14
Series machines	153
Setting startup behaviour, Mode parameter	76
Setting, with operating mode selector switch	66
Severity of injury	119

Signals	116
SIL	10
SIL claim limit	134
Single fault tolerance without diagnostic function	129
Single-channel	
Guard door monitoring with easySafety	38
Guard door monitoring with ESR5	36
Single-channel design	
Emergency-stop with ESR5	16
Speed monitoring	72
Spring-powered interlock	110
SRECS	188
SRP/CS	8
Standards	
EN 1037	112
EN 1088	108
EN 574	114
EN ISO 12100	103
EN ISO 13849 (brief overview)	106
EN ISO 13849-1,	
stepwise determination of performance level (PL)	118
EN ISO 13850	111
EN ISO 14121	104
For the design of safety-related parts of control systems	102
IEC 62061 (brief overview)	107
Machine-related product standards in overview	116
Reference sources	154
Safety standards in overview	102
Steps to SIL safety integrity level according to IEC 62061	126
Startup, unexpected	80
Stop category	111
Stopping in an emergency -> Emergency-stop disconnection	
Substantial modification of machines, interpretation paper Federal	
Ministry of Labour	152
Subsystem architectures definition	129
Surface temperatures	116

T

Three-stage method	103
Three-wire control (pulse contact)	94
Time-current characteristic (6 A fuse)	93
Transformers	92
Travel diagram, for a position switch	110
Two-channel	
Emergency-stop function with easySafety	22, 68
Guard door with ESR5	44
Movable guard with easySafety	70
Two-hand	116
Two-hand control	114
Two-hand control device	62, 64
Two-wire control (continuous contact)	94
Type of actuation, of mechanical position switches	109



V	
Validation	10
Safety functions	125
SRECS	135

W	
Welded contactor	31
Weld-free design	92

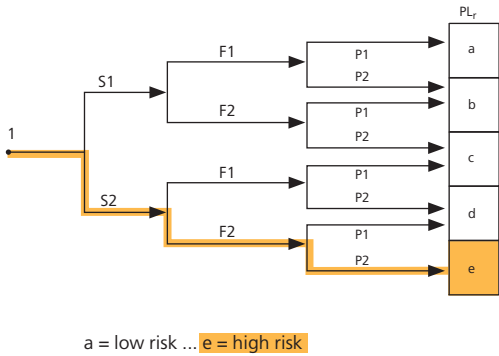
Z	
Zero fault tolerance	129
Zero speed monitoring ZM (safety function block)	54

All protective measures which are used to eliminate the dangers or reduce the risk as a result of these protective measures are to be undertaken in a predefined sequence in compliance with the EN ISO 12100-1:



- 1st step:** Avoidance of dangers: risk elimination and reduction through constructive measures during the planning and development phase of the machine
- 2nd step:** Protect against dangers: reduction of the risks by the introduction of necessary protective measures
- 3rd step:** Indicate remaining sources of danger: risk reduction through information/warnings concerning the residual risks

A) Determination of required performance level PL_r



- Risk parameters:
- S severity of injury
 - S1 slight (normally reversible injury)
 - S2 serious (normally irreversible injury or death)
 - F frequency and/or exposure to hazard
 - F1 seldom-to-less-often and/or exposure time is short
 - F2 frequent-to-continuous and/or exposure time is long
 - P possibility of avoiding hazard or limiting harm
 - P1 possible under specific conditions
 - P2 scarcely possible

B) Design of the control system architecture and determination of the achieved performance level

The safety integrity level SIL is determined by estimating the following parameters:

- Category depending on the specified control system architecture and its properties
- Mean time to dangerous failure $MTTF_d$

- Diagnostic coverage DC
- Common cause failure CCF

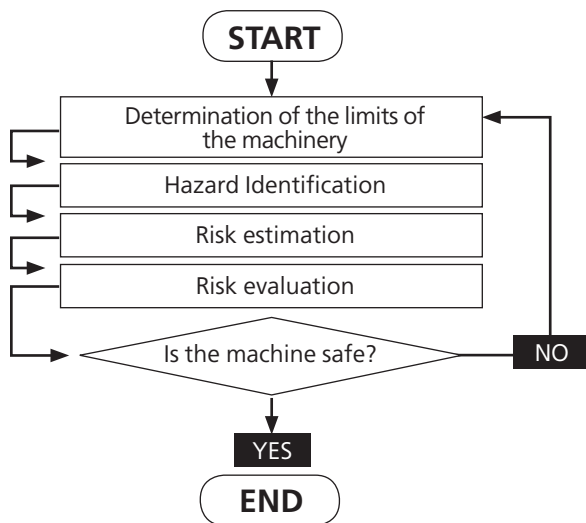
The achieved performance level is taken from a table and must be greater than or equal to the required performance level: $PL \geq PL_r$

Validation

The validation ensures by means of inspection and testing that the design of each safety function meets the appropriate requirements of the specification.

IEC 62061 (2005)

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



The EN ISO 12100-1 standard recommends the following iterative process for analysing and preventing hazards at a machine:

1. Define the physical and time limits of the machine
2. Identify the hazards and hazardous situations
3. Estimate the risk of each identified hazard
4. Evaluate the risk and decide on the necessity for risk reduction

A) Determination of the required SIL performance

Frequency and duration, Fr		+	Probability of hzd. event, Pr		+	Avoidance, AV		=	Class CL	
≤ 1 hour	5		very high	5						
> 1h – ≤ day	5		likely	4						
> 1 day – ≤ 2 weeks	4		possible	3		impossible	5		11-13	
> 2 weeks – ≤ 1 year	3		rarely	2		possible	3			
> 1 year	2		negligible	1		likely	1			

The result in the example is SIL 3:

Consequences	Severity	Class CL				
	5	3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, losing fingers	3		OM	SIL1	SIL2	SIL3
Reversible, medical attention	2			OM	SIL1	SIL2
Reversible, first aid	1				OM	SIL1

B) Design of the control system architecture and determination of the achieved performance level

The safety integrity level SIL is based on the following values that must be determined for each subsystem:

- SIL claim limit (SILCL)
- Probability of a dangerous failure per hour (PFH_d)
- Lifetime T1

The subsystems can be created from different components (subsystem elements). To determine the PFH_d value the following characteristics must be determined for each of these elements:

- Rate of dangerous failure λ_d
- Safe failure fraction SFF

PL and SIL are interrelated:

Performance Level PL	Average probability of dangerous failure per hour [1/h]	SIL
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

Safety parameters

The following safety parameters are used in this document in accordance with IEC 13849-1:

Abbreviation		Explanation
Structure	(Control) category	Classification of safety-related parts of a control system according to their hardware fault tolerance, the availability of diagnostic functions and their reliability; classification from category B (basic category) to category 4 (dual-channel structure with diagnostics)
MTTF _d	Mean Time to Dangerous Failure	Mean time to the occurrence of a dangerous failure
B10 _d		Number of cycles until 10% of a number of tested and worn components (e.g. electromechanical components) have failed
n _{op}		Mean number of annual operations
CCF	Common Cause Failure	Failures of different items, resulting from a single event, where these failures have a common cause.
DC _{avg}	Average Diagnostic Coverage	Average diagnostic coverage of the parts of a safety-related control function; Reduction of the probability of dangerous failures as a result of the execution of automatic diagnostic tests.
PL	Performance Level	Discrete level used to specify the ability of safety-related parts of a control system to perform a safety function under foreseeable conditions; Classification from PL a (highest failure probability) ... PL e (lowest failure probability)
T10 _d		Operating time, time of use of the safety-related control function

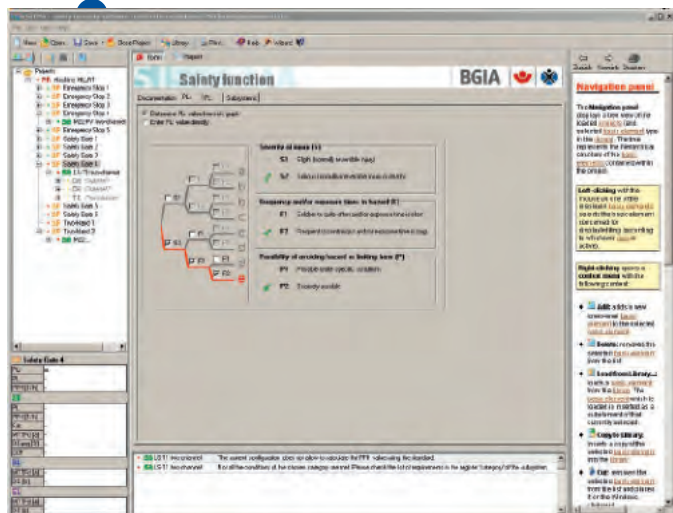
The following safety parameters are used in this document in accordance with IEC 62061:

Abbreviation		Explanation
Structure	Subsystem architecture	Classification of the subsystems of a safety-related control function to a subsystem architecture in accordance with IEC62061 depending on the hardware fault tolerance and the diagnostic function
PFH _d	Probability of a Dangerous Failure per Hour	Probability of a dangerous failure per hour
B10		Number of cycles until 10% of a number of tested and worn components (e.g. electromechanical components) have failed
λ _d /λ		Ratio between the dangerous failure rate and the total failure rate; proportion of dangerous failures
C		Mean number of hourly cycles
β	Beta factor	Common cause failure factor
DC	Diagnostic Coverage	Diagnostic coverage of the parts of a safety-related control function; Reduction of the probability of dangerous failures as a result of the execution of automatic diagnostic tests
SIL	Safety Integrity Level	Discrete level for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related function of an electrical control system of the machine; SIL1 (lowest level)... SIL 3 (highest level)

Safety of controls on machines – simple calculation with Eaton libraries

for Sistema

for VDMA 66413



The as per 2006/42/EC Machinery Safety Directive harmonized standards EN IS 13849-1, EN ISO 13849-2 and EN 62061 require evaluations and calculations relating to the likelihood of a dangerous failure and systematic aspects of a machine's safety functions.

- The evaluations and calculations must be conducted by the machine manufacturer (as the distributor) and be verifiably documented.
- The device manufacturers supply the relevant data (parameters) of the safety devices used in the machine from the point of view of product liability.
- Safety calculations can be performed with the aid of calculation tools (software programs).

Applying the aforementioned standards requires that relevant data is exchanged between the machinery manufacturers, device manufacturers and calculation tools involved.

Device Manufacturers create a parameters library in the form of a „Universal Database“ and make it generally available. Only the device manufacturer may also be the creator of a parameters library.

Calculation tools provide an import mechanism for the parameters libraries in the database format. The parameters are prepared for presentation and selection in the tool.

Machinery manufacturers use the parameters library (file) made available by the device manufacturer to import the parameters (device data) into the calculation tool and for updating.

This makes the universal database according to VDMA 66413 the common basis by which information is exchanged.

Following is a summary of the most important criteria:

- Definition of required information
- Clear description of device data, manufacturer-independent
- Appropriate for machine building, industry-independent
- Independent of physical interfaces, calculation tools, transfer protocols, database formats

The manufacturer-independent calculation tool SISTEMA from the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) provides assistance in the evaluation of safety-related control components in the context of EN ISO 13849-1 and simplifies risk assessment analysis.

Selection of the design structure of the protective devices and the assignment to an architecture compliant to the EN ISO 13849-1 is implemented in a Windows user interface. On this basis, the software calculates the reliability values as well as the attained Performance Level (PL). A direct comparison with the required Performance Level (PLr) is thus possible.

The software records the relevant parameters for evaluation such as MTTFd, B10d, DCavg and CCF. It directly indicates the influence of variable parameters on the overall result.

The calculation tool can be downloaded directly from the IFA website.

Eaton provides the libraries for integration into the SISTEMA software free-of-charge under: Input, Logic or Output. The individual libraries can be downloaded at www.eaton.eu/safety. Please note that the libraries are updated on an ongoing basis and new products are continuously added.

Eaton is dedicated to ensuring that reliable, efficient and safe power is available when it's needed most. With unparalleled knowledge of electrical power management across industries, experts at Eaton deliver customized, integrated solutions to solve our customers' most critical challenges.

Our focus is on delivering the right solution for the application. But, decision makers demand more than just innovative products. They turn to Eaton for an unwavering commitment to personal support that makes customer success a top priority. For more information, **visit www.eaton.eu/electrical**.

To contact an Eaton salesperson or local distributor/agent, please visit www.eaton.eu/electrical/customersupport

WWW.TM2A.PT info@tm2a.pt

WWW.TM2A.PT

WWW.TM2A.PT info@tm2a.pt

WWW.TM2A.PT



TM2A Soluções e Componentes Industriais
Rua Cidade de Viena 2, Parque Ind. Arneiro
2660-456 São Julião do Tojal
PORTUGAL

T: +351 219737330
www.tm2a.pt

F: +351 219737339
info@tm2a.pt