The Drive & Control Company

Rexroth IndraDrive

Integrated Safety Technology According to IEC 61508

Functional Description Edition 04

R911327664

Title

Rexroth IndraDrive
Integrated Safety Technology
According to IEC 61508

Type of Documentation

Functional Description

Document Typecode

DOK-INDRV*-SI2-**VRS**-FK04-EN-P

Internal File Reference

RS-033bc8493754ba300a6846a000e3f0a3-6-en-US-6

Purpose of Documentation

This documentation is used to

- make oneself familiar with the subject of "Integrated Safety Technology",
- get to know the IndraDrive system with integrated safety technology according to IEC 61508 employ and commission application-related safety functions,
- recognize and fix errors, and
- replace the hardware and update the firmware.

Record of Revision

Edition	Release Date	Notes
DOK-INDRV*-SI2-**VRS**-FK01-EN-P to DOK-INDRV*-SI2-**VRS**-FK04-EN-P	2009 to 2015-11-30	See chapter "About this documentation", marginal note "Editions of this documentation"

Liability

The specified data is intended for product description purposes only and shall not be deemed to be a guaranteed characteristic unless expressly stipulated in the contract. All rights are reserved with respect to the content of this documentation and the availability of the product.

Editorial Department

Dept. DC-IA/EDY (SA, RB, RS, BB)

Note

This document has been printed on chlorine-free bleached paper.

Table of Contents

Page

Table of Contents

Page

Page

Table of Contents

Page

Table of Contents

Page

1 Introduction

1.1 About this documentation

Editions of this documentation

Edition	Release date	Notes
DOK-INDRV*-SI2-**VRS**-FK01-EN-P	2009-07-31	First edition for prototype release
DOK-INDRV*-SI2-**VRS**-FK01-EN-P	2009-09-17	Second edition for prototype release
DOK-INDRV*-SI2-**VRS**-FK02-EN-P	2009-10-02	Third edition for prototype release Added SIL1 for L2/"Safe Torque Off"
DOK-INDRV*-SI2-**VRS**-FK03-EN-P	2011-02-22	Corrections and additions ● Added in "Safely-monitored stopping process on basis of actual velocity": with active monitoring after P-0-3226 is over ● Conformity with Machinery Directive is declared for the optional safety technology modules "L2" and "S2" ● Addition in "Safe Direction (SDI)"
DOK-INDRV*-SI2-**VRS**-FK04-EN-P	2015-11-30	Corrections and additions

Tab. 1-1: Record of revisions

Means of representation in this documentation

To make the reading of this documentation easier for you, the table below contains the means of representation and notations of recurring terms.

What?	How?	For example...
Important facts which are to be highlighted in the body text	Boldface	With the safety function "Safe parking axis", the following monitoring functions are **deactivated**: ...
Parameter names, diagnostic message names, function designations	Quotation marks	The missing speed information can be replaced via the control bit "defined safety with parked axis" in "P-0-3210, Safety technology configuration".

Tab. 1-2: Conventions of notation

Notes and tips are highlighted in the text. A symbol tells you what kind of note or tip is used in the text:

☞ This box contains important information that should be taken into consideration.

💡 This symbol highlights useful tips and tricks.

Signal words in accordance with ANSI Z535.6-2006 draw the reader's attention to hazards (see "Explanation of signal words and the safety alert symbol").

Structure of documentation

Concerning integrated safety technology, the descriptions of the IndraDrive systems have the following structure:

- **Functional Description** for Rexroth IndraDrive, **Integrated Safety Technology According to IEC 61508** (this documentation)

- **Project Planning Manual of Rexroth IndraDrive control sections**

  Assists with electrical design and installation of the drive system
- **Parameter Description** for Rexroth IndraDrive

  Apart from the specific safety technology parameters, all other drive parameters are documented in the Parameter Description
- **Description of Diagnostic Messages** for Rexroth IndraDrive

  Apart from the specific diagnostic messages of safety technology, all other diagnostic drive messages are documented in the Description of Diagnostic Messages (also called "Troubleshooting Guide").

☞ For an overview of reference documentations, please refer to: "Reference documentations"

Trademark information

sercos the automation bus	sercos is registered trademark of sercos International e.V.
PROFI NET®	PROFINET® (Process Field Network) is the open Industrial Ethernet standard of Profibus & Profinet International (PI) for automation. ProfiNet® is registered trademark of PROFIBUS Nutzerorganisation e. V.
	HIPERFACE® is registered trademark of SICK-STEGMANN GmbH
	EnDat® is registered trademark of Dr. Johannes Heidenhain GmbH

Your Feedback

Your experience is important for our improvement processes of products and documentations.

If you discover mistakes in this documentation or suggest changes, you can send your feedback to the following e-mail address:

Dokusupport@boschrexroth.de

We need the following information to handle your feedback:

- The number indicated under "Internal File Reference".
- The page number.

1.2 Documentations

1.2.1 Drive Systems, System Components

Title Rexroth IndraDrive …	Kind of documentation	Document typecode[1)] DOK-INDRV*-…	Part number R911…
Drive Systems With HMV01/02 HMS01/02, HMD01, HCS02/03	Project Planning Manual	SYSTEM*****-PRxx-EN-P	309636
Mi Drive Systems	Project Planning Manual	KCU+KSM****-PRxx-EN-P	320924
Supply Units, Power Sections HMV, HMS, HMD, HCS02, HCS03	Project Planning Manual	HMV-S-D+HCS-PRxx-EN-P	318790
Drive Controllers Control Sections CSB01, CSH01, CDB01	Project Planning Manual	CSH********-PRxx-EN-P	295012

Title Rexroth IndraDrive …	Kind of documentation	Document typecode[1)] DOK-INDRV*-…	Part number R911…
Additional Components and Accessories	Project Planning Manual	ADDCOMP****-PRxx-EN-P	306140
C Drive Controllers HCS02.1, HCS03.1	Operating Instructions	FU**********-IBxx-EN-P	314905

1) In the document typecodes, "xx" is a wild card for the current edition of the documentation (example: PR01 is the first edition of a Project Planning Manual)

Tab. 1-3: Documentations – Overview

Title	Kind of documentation	Document typecode[1)]	Part number R911…
Automation Terminals Of The Rexroth Inline Product Range	Application Manual	DOK-CONTRL-ILSYSINS***-AWxx-EN-P	317021

1) In the document typecodes, "xx" is a wild card for the current edition of the documentation (example: AW01 is the first edition of an Application Manual)

Tab. 1-4: Documentations – Overview

1.2.2 Motors

Title Rexroth IndraDyn …	Kind of documentation	Document typecode[1)] DOK-MOTOR*-…	Part number R911…
A Asynchronous Motors MAD / MAF	Project Planning Manual	MAD/MAF****-PRxx-EN-P	295781
H Synchronous Kit Spindle Motors	Project Planning Manual	MBS-H******-PRxx-EN-P	297895
L Synchronous Linear Motors	Project Planning Manual	MLF********-PRxx-EN-P	293635
S MSK Synchronous Motors	Project Planning Manual	MSK********-PRxx-EN-P	296289
T Synchronous Torque Motors	Project Planning Manual	MBT********-PRxx-EN-P	298798

1) In the document typecodes, "xx" is a wild card for the current edition of the documentation (example: PR01 is the first edition of a Project Planning Manual)

Tab. 1-5: Documentations – Overview

1.2.3 Cables

Title	Kind of documentation	Document typecode[1)] DOK-…	Part number R911…
Rexroth Connection Cables IndraDrive and IndraDyn	Selection Data	CONNEC-CABLE*INDRV-CAxx-EN-P	322949

1) In the document typecodes, "xx" is a wild card for the current edition of the documentation (example: CA02 is the second edition of the documentation "Selection Data")

Tab. 1-6: Documentations – Overview

1.2.4 Firmware

Title Rexroth IndraDrive …	Kind of documentation	Document typecode[1)] DOK-INDRV*-…	Part number R911…
Firmware for Drive Controllers MPH-08, MPB-08, MPD-08, MPC-08	Functional Description	MP*-08VRS**-APxx-EN-P	332643
Firmware for Drive Controllers MPH-07, MPB-07, MPD-07, MPC-07	Functional Description	MP*-07VRS**-FKxx-EN-P	328670
Firmware for Drive Controllers MPH-06, MPB-06, MPD-06, MPC-06	Functional Description	MP*-06VRS**-FKxx-EN-P	326766
Firmware for Drive Controllers MPH-05, MPB-05, MPD-05	Functional Description	MP*-05VRS**-FKxx-EN-P	320182
Firmware for Drive Controllers MPH-04, MPB-04, MPD-04	Functional Description	MP*-04VRS**-FKxx-EN-P	315485
Firmware for Drive Controllers MPH-03, MPB-03, MPD-03	Functional Description	MP*-03VRS**-FKxx-EN-P	308329
Firmware for Drive Controllers MPH-02, MPB-02, MPD-02	Functional Description	MP*-02VRS**-FKxx-EN-P	299223
Drive Controllers MPx-02 to MPx-08	Parameter Description	GEN-**VRS**-PAxx-EN-P	297317
MPx-02 to MPx-08 and HMV	Troubleshooting Guide	GEN-**VRS**-WAxx-EN-P	297319
Integrated Safety Technology	Functional and Application Description	SI*-**VRS**-FKxx-EN-P	297838
Integrated Safety Technology According to IEC61508	Functional Description	SI2-**VRS**-FKxx-EN-P	327664
Rexroth IndraMotion MLD	Application Manual	MLD-**VRS**-AWxx-EN-P	306084
Rexroth IndraMotion MLD Library	Library Description	MLD-SYSLIB*-FKxx-EN-P	309224

1) In the document typecodes, "xx" is a wild card for the current edition of the documentation (example: FK02 is the second edition of a Functional Description)

Tab. 1-7: Documentations – Overview

Title	Kind of documentation	Document typecode[1)]	Part number R911…
Productivity Agent Extended Diagnostic Functions With Rexroth IndraDrive	Application Manual	DOK-INDRV*-MLD-PAGENT*-AWxx-EN-P	323947

1) In the document typecodes, "xx" is a wild card for the current edition of the documentation (example: AW01 is the first edition of an Application Manual)

Tab. 1-8: Documentations – Overview

2 Important directions for use

2.1 Appropriate use

2.1.1 Introduction

Rexroth products reflect the state-of-the-art in their development and their manufacture. They are tested prior to delivery to ensure operating safety and reliability.

⚠ **WARNING** **Personal injury and property damage caused by incorrect use of the products!**

The products have been designed for use in industrial environments and may only be used in the appropriate way. If they are not used in the appropriate way, situations resulting in property damage and personal injury can occur.

☞ Rexroth as manufacturer is not liable for any damages resulting from inappropriate use. In such cases, the guarantee and the right to payment of damages resulting from inappropriate use are forfeited. The user alone carries all responsibility of the risks.

Before using Rexroth products, the following pre-requisites must be met to ensure appropriate use of the products:

- Personnel that in any way, shape or form uses our products must first read and understand the relevant safety instructions and be familiar with their appropriate use.
- If the products take the form of hardware, then they must remain in their original state, in other words, no structural changes are permitted. It is not permitted to decompile software products or alter source codes.
- Damaged or faulty products may not be installed or put into operation.
- Make sure that the products have been installed in the manner described in the relevant documentation.

2.1.2 Areas of use and application

Drive controllers made by Rexroth are designed to control electrical motors and monitor their operation.

Control and monitoring of the Drive controllers may require additional sensors and actors.

☞ The drive controllers may only be used with the accessories and parts specified in this documentation. If a component has not been specifically named, then it may neither be mounted nor connected. The same applies to cables and lines.

Operation is only permitted in the specified configurations and combinations of components using the software and firmware as specified in the relevant Functional Descriptions.

Drive controllers have to be programmed before commissioning to ensure that the motor executes the specific functions of an application.

Drive controllers of the Rexroth IndraDrive line have been developed for use in single- and multi-axis drive and control tasks.

To ensure application-specific use of Drive controllers, device types of different drive power and different interfaces are available.

Typical applications include, for example:

- Handling and mounting systems,
- Packaging and food machines,
- Printing and paper processing machines and
- Machine tools.

Drive controllers may only be operated under the assembly and installation conditions described in this documentation, in the specified position of normal use and under the ambient conditions as described (temperature, degree of protection, humidity, EMC, etc.).

2.2 Inappropriate use

Using the Drive controllers outside of the operating conditions described in this documentation and outside of the technical data and specifications given is defined as "inappropriate use".

Drive controllers may not be used, if ...

- they are subject to operating conditions that do not meet the specified ambient conditions. This includes, for example, operation under water, under extreme temperature fluctuations or extremely high maximum temperatures.
- Furthermore, Drive controllers may not be used in applications which have not been expressly authorized by Rexroth. Please carefully follow the specifications outlined in the general Safety Instructions!

☞ Components of the Rexroth IndraDrive system are **products of category C3** (with limited availability) according to IEC 61800-3. To ensure that this category (limit values) is maintained, suitable line filters must be used in the drive system.

These components are not provided for use in a public low-voltage network supplying residential areas with power. If these components are used in such a public network, high-frequency interference is to be expected. This can require additional measures of radio interference suppression.

3 Safety instructions for electric drives and controls

3.1 Definitions of terms

Application Documentation

Application documentation comprises the entire documentation used to inform the user of the product about the use and safety-relevant features for configuring, integrating, installing, mounting, commissioning, operating, maintaining, repairing and decommissioning the product. The following terms are also used for this kind of documentation: Operating Instructions, Commissioning Manual, Instruction Manual, Project Planning Manual, Application Description, etc.

Component

A component is a combination of elements with a specified function, which are part of a piece of equipment, device or system. Components of the electric drive and control system are, for example, supply units, drive controllers, mains choke, mains filter, motors, cables, etc.

Control system

A control system comprises several interconnected control components placed on the market as a single functional unit.

Device

A device is a finished product with a defined function, intended for users and placed on the market as an individual piece of merchandise.

Electrical equipment

Electrical equipment encompasses all devices used to generate, convert, transmit, distribute or apply electrical energy, such as electric motors, transformers, switching devices, cables, lines, power-consuming devices, circuit board assemblies, plug-in units, control cabinets, etc.

Electric drive system

An electric drive system comprises all components from mains supply to motor shaft; this includes, for example, electric motor(s), motor encoder(s), supply units and drive controllers, as well as auxiliary and additional components, such as mains filter, mains choke and the corresponding lines and cables.

Installation

An installation consists of several devices or systems interconnected for a defined purpose and on a defined site which, however, are not intended to be placed on the market as a single functional unit.

Machine

A machine is the entirety of interconnected parts or units at least one of which is movable. Thus, a machine consists of the appropriate machine drive elements, as well as control and power circuits, which have been assembled for a specific application. A machine is, for example, intended for processing, treatment, movement or packaging of a material. The term "machine" also covers a combination of machines which are arranged and controlled in such a way that they function as a unified whole.

Manufacturer

The manufacturer is an individual or legal entity bearing responsibility for the design and manufacture of a product which is placed on the market in the individual's or legal entity's name. The manufacturer can use finished products, finished parts or finished elements, or contract out work to subcontractors. However, the manufacturer must always have overall control and possess the required authority to take responsibility for the product.

Product

Examples of a product: Device, component, part, system, software, firmware, among other things.

Project planning manual

A Project Planning Manual is part of the application documentation used to support the sizing and planning of systems, machines or installations.

Qualified persons

In terms of this application documentation, qualified persons are those persons who are familiar with the installation, mounting, commissioning and operation of the components of the electric drive and control system, as well as with the hazards this implies, and who possess the qualifications their work requires. To comply with these qualifications, it is necessary, among other things,

- to be trained, instructed or authorized to switch electric circuits and devices safely on and off, to ground them and to mark them.
- to be trained or instructed to maintain and use adequate safety equipment.
- to attend a course of instruction in first aid.

User A user is a person installing, commissioning or using a product which has been placed on the market.

3.2 General information

3.2.1 Using the Safety instructions and passing them on to others

Do not attempt to install and operate the components of the electric drive and control system without first reading all documentation provided with the product. Read and understand these safety instructions and all user documentation prior to working with these components. If you do not have the user documentation for the components, contact your responsible Rexroth sales partner. Ask for these documents to be sent immediately to the person or persons responsible for the safe operation of the components.

If the component is resold, rented and/or passed on to others in any other form, these safety instructions must be delivered with the component in the official language of the user's country.

Improper use of these components, failure to follow the safety instructions in this document or tampering with the product, including disabling of safety devices, could result in property damage, injury, electric shock or even death.

3.2.2 Requirements for safe use

Read the following instructions before initial commissioning of the components of the electric drive and control system in order to eliminate the risk of injury and/or property damage. You must follow these safety instructions.

- Rexroth is not liable for damages resulting from failure to observe the safety instructions.
- Read the operating, maintenance and safety instructions in your language before commissioning. If you find that you cannot completely understand the application documentation in the available language, please ask your supplier to clarify.
- Proper and correct transport, storage, mounting and installation, as well as care in operation and maintenance, are prerequisites for optimal and safe operation of the component.
- Only qualified persons may work with components of the electric drive and control system or within its proximity.
- Only use accessories and spare parts approved by Rexroth.
- Follow the safety regulations and requirements of the country in which the components of the electric drive and control system are operated.
- Only use the components of the electric drive and control system in the manner that is defined as appropriate. See chapter "Appropriate Use".
- The ambient and operating conditions given in the available application documentation must be observed.

- Applications for functional safety are only allowed if clearly and explicitly specified in the application documentation "Integrated Safety Technology". If this is not the case, they are excluded. Functional safety is a safety concept in which measures of risk reduction for personal safety depend on electrical, electronic or programmable control systems.
- The information given in the application documentation with regard to the use of the delivered components contains only examples of applications and suggestions.

  The machine and installation manufacturers must

  - make sure that the delivered components are suited for their individual application and check the information given in this application documentation with regard to the use of the components,
  - make sure that their individual application complies with the applicable safety regulations and standards and carry out the required measures, modifications and complements.
- Commissioning of the delivered components is only allowed once it is sure that the machine or installation in which the components are installed complies with the national regulations, safety specifications and standards of the application.
- Operation is only allowed if the national EMC regulations for the application are met.
- The instructions for installation in accordance with EMC requirements can be found in the section on EMC in the respective application documentation.

  The machine or installation manufacturer is responsible for compliance with the limit values as prescribed in the national regulations.
- The technical data, connection and installation conditions of the components are specified in the respective application documentations and must be followed at all times.

National regulations which the user has to comply with

- European countries: In accordance with European EN standards
- United States of America (USA):
  - National Electrical Code (NEC)
  - National Electrical Manufacturers Association (NEMA), as well as local engineering regulations
  - Regulations of the National Fire Protection Association (NFPA)
- Canada: Canadian Standards Association (CSA)
- Other countries:
  - International Organization for Standardization (ISO)
  - International Electrotechnical Commission (IEC)

3.2.3 Hazards by improper use

- High electrical voltage and high working current! Danger to life or serious injury by electric shock!
- High electrical voltage by incorrect connection! Danger to life or injury by electric shock!
- Dangerous movements! Danger to life, serious injury or property damage by unintended motor movements!

- Health hazard for persons with heart pacemakers, metal implants and hearing aids in proximity to electric drive systems!
- Risk of burns by hot housing surfaces!
- Risk of injury by improper handling! Injury by crushing, shearing, cutting, hitting!
- Risk of injury by improper handling of batteries!
- Risk of injury by improper handling of pressurized lines!

3.3 Instructions with regard to specific dangers

3.3.1 Protection against contact with electrical parts and housings

☞ This section concerns components of the electric drive and control system with voltages of **more than 50 volts**.

Contact with parts conducting voltages above 50 volts can cause personal danger and electric shock. When operating components of the electric drive and control system, it is unavoidable that some parts of these components conduct dangerous voltage.

High electrical voltage! Danger to life, risk of injury by electric shock or serious injury!

- Only qualified persons are allowed to operate, maintain and/or repair the components of the electric drive and control system.
- Follow the general installation and safety regulations when working on power installations.
- Before switching on, the equipment grounding conductor must have been permanently connected to all electric components in accordance with the connection diagram.
- Even for brief measurements or tests, operation is only allowed if the equipment grounding conductor has been permanently connected to the points of the components provided for this purpose.
- Before accessing electrical parts with voltage potentials higher than 50 V, you must disconnect electric components from the mains or from the power supply unit. Secure the electric component from reconnection.
- With electric components, observe the following aspects:

  Always wait **30 minutes** after switching off power to allow live capacitors to discharge before accessing an electric component. Measure the electrical voltage of live parts before beginning to work to make sure that the equipment is safe to touch.
- Install the covers and guards provided for this purpose before switching on.
- Never touch any electrical connection points of the components while power is turned on.
- Do not remove or plug in connectors when the component has been powered.
- Under specific conditions, electric drive systems can be operated at mains protected by residual-current-operated circuit-breakers sensitive to universal current (RCDs/RCMs).

- Secure built-in devices from penetrating foreign objects and water, as well as from direct contact, by providing an external housing, for example a control cabinet.

High housing voltage and high leakage current! Danger to life, risk of injury by electric shock!

- Before switching on and before commissioning, ground or connect the components of the electric drive and control system to the equipment grounding conductor at the grounding points.
- Connect the equipment grounding conductor of the components of the electric drive and control system permanently to the main power supply at all times. The leakage current is greater than 3.5 mA.
- Establish an equipment grounding connection with a minimum cross section according to the table below. With an outer conductor cross section smaller than 10 mm^2 (8 AWG), the alternative connection of two equipment grounding conductors is allowed, each having the same cross section as the outer conductors.

Cross section outer conductor	Minimum cross section equipment grounding conductor Leakage current ≥ 3.5 mA	
	1 equipment grounding conductor	2 equipment grounding conductors
1.5 mm^2 (16 AWG)	10 mm^2 (8 AWG)	2 × 1.5 mm^2 (16 AWG)
2.5 mm^2 (14 AWG)		2 × 2.5 mm^2 (14 AWG)
4 mm^2 (12 AWG)		2 × 4 mm^2 (12 AWG)
6 mm^2 (10 AWG)		2 × 6 mm^2 (10 AWG)
10 mm^2 (8 AWG)		-
16 mm^2 (6 AWG)	16 mm^2 (6 AWG)	-
25 mm^2 (4 AWG)		-
35 mm^2 (2 AWG)		-
50 mm^2 (1/0 AWG)	25 mm^2 (4 AWG)	-
70 mm^2 (2/0 AWG)	35 mm^2 (2 AWG)	-
...	...	...

Tab. 3-1: Minimum cross section of the equipment grounding connection

3.3.2 Protective extra-low voltage as protection against electric shock

Protective extra-low voltage is used to allow connecting devices with basic insulation to extra-low voltage circuits.

On components of an electric drive and control system provided by Rexroth, all connections and terminals with voltages up to 50 volts are PELV ("Protective Extra-Low Voltage") systems. It is allowed to connect devices equipped with basic insulation (such as programming devices, PCs, notebooks, display units) to these connections.

Danger to life, risk of injury by electric shock! High electrical voltage by incorrect connection!

If extra-low voltage circuits of devices containing voltages and circuits of more than 50 volts (e.g., the mains connection) are connected to Rexroth products, the connected extra-low voltage circuits must comply with the requirements for PELV ("Protective Extra-Low Voltage").

3.3.3 Protection against dangerous movements

Dangerous movements can be caused by faulty control of connected motors. Some common examples are:

- Improper or wrong wiring or cable connection
- Operator errors
- Wrong input of parameters before commissioning
- Malfunction of sensors and encoders
- Defective components
- Software or firmware errors

These errors can occur immediately after equipment is switched on or even after an unspecified time of trouble-free operation.

The monitoring functions in the components of the electric drive and control system will normally be sufficient to avoid malfunction in the connected drives. Regarding personal safety, especially the danger of injury and/or property damage, this alone cannot be relied upon to ensure complete safety. Until the integrated monitoring functions become effective, it must be assumed in any case that faulty drive movements will occur. The extent of faulty drive movements depends upon the type of control and the state of operation.

Dangerous movements! Danger to life, risk of injury, serious injury or property damage!

A **risk assessment** must be prepared for the installation or machine, with its specific conditions, in which the components of the electric drive and control system are installed.

As a result of the risk assessment, the user must provide for monitoring functions and higher-level measures on the installation side for personal safety. The safety regulations applicable to the installation or machine must be taken into consideration. Unintended machine movements or other malfunctions are possible if safety devices are disabled, bypassed or not activated.

To avoid accidents, injury and/or property damage:

- Keep free and clear of the machine’s range of motion and moving machine parts. Prevent personnel from accidentally entering the machine’s range of motion by using, for example:
  – Safety fences
  – Safety guards
  – Protective coverings
  – Light barriers
- Make sure the safety fences and protective coverings are strong enough to resist maximum possible kinetic energy.
- Mount emergency stopping switches in the immediate reach of the operator. Before commissioning, verify that the emergency stopping equip-

ment works. Do not operate the machine if the emergency stopping switch is not working.

- Prevent unintended start-up. Isolate the drive power connection by means of OFF switches/OFF buttons or use a safe starting lockout.
- Make sure that the drives are brought to safe standstill before accessing or entering the danger zone.
- Additionally secure vertical axes against falling or dropping after switching off the motor power by, for example,
  - mechanically securing the vertical axes,
  - adding an external braking/arrester/clamping mechanism or
  - ensuring sufficient counterbalancing of the vertical axes.
- The standard equipment **motor holding brake** or an external holding brake controlled by the drive controller is **not sufficient to guarantee personal safety**!
- Disconnect electrical power to the components of the electric drive and control system using the master switch and secure them from reconnection ("lock out") for:
  - Maintenance and repair work
  - Cleaning of equipment
  - Long periods of discontinued equipment use
- Prevent the operation of high-frequency, remote control and radio equipment near components of the electric drive and control system and their supply leads. If the use of these devices cannot be avoided, check the machine or installation, at initial commissioning of the electric drive and control system, for possible malfunctions when operating such high-frequency, remote control and radio equipment in its possible positions of normal use. It might possibly be necessary to perform a special electromagnetic compatibility (EMC) test.

3.3.4 Protection against electromagnetic and magnetic fields during operation and mounting

Electromagnetic and magnetic fields!

Hazards for persons with active medical implants or passive metallic implants, as well as for pregnant women.

- Persons with active medical implants (e.g. heart pacemakers), passive metallic implants (e.g. hip implants) and pregnant women might possibly risk hazards by electromagnetic or magnetic fields in the immediate vicinity of components of the electric drive and control system and the associated current-carrying conductors.

  Entering the following areas can cause danger to these persons:
  - Areas in which components of the electric drive and control system and the associated current-carrying conductors are mounted, commissioned and operated.
  - Areas in which parts of motors with permanent magnets are stored, repaired or mounted.
- Before entering these areas, the above-mentioned persons should seek advice from their physician.
- Observe the occupational safety and health regulations applicable at the site of operation, for installations equipped with components of the elec-

tric drive and control system and the associated current-carrying conductors.

3.3.5 Protection against contact with hot parts

Hot surfaces of components of the electric drive and control system. Risk of burns!

- Do not touch hot surfaces of, for example, braking resistors, heat sinks, supply units and drive controllers, motors, windings and laminated cores!
- According to the operating conditions, temperatures of the surfaces can be **higher than 60 °C** (140 °F) during or after operation.
- Before touching motors after having switched them off, let them cool down for a sufficient period of time. Cooling down can require **up to 140 minutes**! The time required for cooling down is approximately five times the thermal time constant specified in the technical data.
- After switching chokes, supply units and drive controllers off, wait **15 minutes** to allow them to cool down before touching them.
- Wear safety gloves or do not work at hot surfaces.
- For certain applications, and in accordance with the respective safety regulations, the manufacturer of the machine or installation must take measures to avoid injuries caused by burns in the final application. These measures can be, for example: Warnings at the machine or installation, guards (shieldings or barriers) or safety instructions in the application documentation.

3.3.6 Protection during handling and mounting

Risk of injury by improper handling! Injury by crushing, shearing, cutting, hitting!

- Observe the relevant statutory regulations of accident prevention.
- Use suitable equipment for mounting and transport.
- Avoid jamming and crushing by appropriate measures.
- Always use suitable tools. Use special tools if specified.
- Use lifting equipment and tools in the correct manner.
- Use suitable protective equipment (hard hat, safety goggles, safety shoes, safety gloves, for example).
- Do not stand under hanging loads.
- Immediately clean up any spilled liquids from the floor due to the risk of falling!

3.3.7 Battery safety

Batteries consist of active chemicals in a solid housing. Therefore, improper handling can cause injury or property damage.

Risk of injury by improper handling!

- Do not attempt to reactivate low batteries by heating or other methods (risk of explosion and cauterization).
- Do not attempt to recharge the batteries as this may cause leakage or explosion.

- Do not throw batteries into open flames.
- Do not dismantle batteries.
- When replacing the battery/batteries, do not damage the electrical parts installed in the devices.
- Only use the battery types specified for the product.

☞ Environmental protection and disposal! The batteries contained in the product are considered dangerous goods during land, air, and sea transport (risk of explosion) in the sense of the legal regulations. Dispose of used batteries separately from other waste. Observe the national regulations of your country.

3.3.8 Protection against pressurized systems

According to the information given in the Project Planning Manuals, motors and components cooled with liquids and compressed air can be partially supplied with externally fed, pressurized media, such as compressed air, hydraulics oil, cooling liquids and cooling lubricants. Improper handling of the connected supply systems, supply lines or connections can cause injuries or property damage.

Risk of injury by improper handling of pressurized lines!

- Do not attempt to disconnect, open or cut pressurized lines (risk of explosion).
- Observe the respective manufacturer's operating instructions.
- Before dismounting lines, relieve pressure and empty medium.
- Use suitable protective equipment (safety goggles, safety shoes, safety gloves, for example).
- Immediately clean up any spilled liquids from the floor due to the risk of falling!

☞ Environmental protection and disposal! The agents (e.g., fluids) used to operate the product might not be environmentally friendly. Dispose of agents harmful to the environment separately from other waste. Observe the national regulations of your country.

3.4 Explanation of signal words and the Safety alert symbol

The Safety Instructions in the available application documentation contain specific signal words (DANGER, WARNING, CAUTION or NOTICE) and, where required, a safety alert symbol (in accordance with ANSI Z535.6-2011).

The signal word is meant to draw the reader's attention to the safety instruction and identifies the hazard severity.

The safety alert symbol (a triangle with an exclamation point), which precedes the signal words DANGER, WARNING and CAUTION, is used to alert the reader to personal injury hazards.

⚠ DANGER

In case of non-compliance with this safety instruction, death or serious injury **will** occur.

⚠ WARNING

In case of non-compliance with this safety instruction, death or serious injury **could** occur.

⚠ CAUTION

In case of non-compliance with this safety instruction, minor or moderate injury could occur.

NOTICE

In case of non-compliance with this safety instruction, property damage could occur.

4 System overview

4.1 Introduction

4.1.1 Motivation and objectives

Overview

The operational safety of machines and installations depends largely upon the extent of dangerous movements generated by the machine.

In **normal operation** (also called productive operation or automatic operation), protective equipment prevents humans from accessing danger zones and keeps parts / materials from being thrown outward.

In the **special mode** (also called manual mode or setting-up mode), it is often necessary for persons to access danger zones when the entire installation has not been de-energized. In such situations machine operators must be protected by mechanisms internal to the drive and the control unit.

The integrated Rexroth safety technology provides the user the requirements, on the control unit and drive side, for realizing functions of personal and machine protection with a minimum of planning and installation work required. Compared to conventional safety technology, the integrated safety technology considerably increases the functionality and availability of your machine. Integrated safety technology is characterized by the following features:

- Complies with valid standards
- Simplified system structure (e.g., use of PROFIBUS for communication and safety)
- Increased system performance
- Reduced system costs
- Easy understanding of complex subjects
- Improved diagnostics
- Simplified certification
- Easy commissioning
- Independent of control units

Safe Braking and Holding System

Machine setup, trouble shooting or process optimization: During operation of machines and installations, it is necessary for persons to work in the processing area of machines. With gravity-loaded axes in the area of access, particular precaution is required. Whereas horizontal axes are not subject to gravitational force, vertical or inclined axes can move down accidentally and thereby cause danger, even when they have been de-energized. This can occur, for example, by soiling, mechanical wear or when holding brakes get oiled-up and thereby lose their nominal holding torques.

With the safe braking and holding system in the drive, Rexroth as drive manufacturer provides an integrated system solution which has been certified according to EN ISO 13849-1, Category 3 PL d and EN 61800-5-2, SIL 2. The safety functions already available in the drive are usefully complemented for the use of gravity-loaded axes.

Comparison with conventional safety technology

A drive and control system with integrated safety technology differs from systems with conventional safety technology by the fact that the safety functions are directly integrated in the intelligent drives in the form hardware and software. This increases the functionality in all operation modes with a maximum of safety (short reaction times).

The following components of conventional safety technology are not included in drive and control systems with integrated safety technology:

- Motor zero-speed relay for monitoring safe standstill
- Speed monitor for monitoring safely-reduced velocities
- Power contactors between controllers and motors
- Limit switches or position cams for detection of range

> ☞ The integrated safety technology is **not** intended to replace conventional safety technology, such as EMERGENCY STOP monitoring devices and safety door monitors.

Using the integrated safety technology increases the available personnel and machine safety, because the total reaction time of the system in the case of an error event, for example, is considerably reduced with regard to comparable systems with conventional safety technology. The safety signals are transmitted with conventional wiring in diversitary (manifold) design. Master communication (SERCOS interface, PROFIBUS, CANopen, etc.) can be used for transmission of a channel.

4.1.2 Conceptual overview

An IndraDrive system consists of the components power section, control section (incl. firmware) and motor and possibly required additional components.

The integrated safety technology is implemented based on the interaction of the hardware and firmware components.

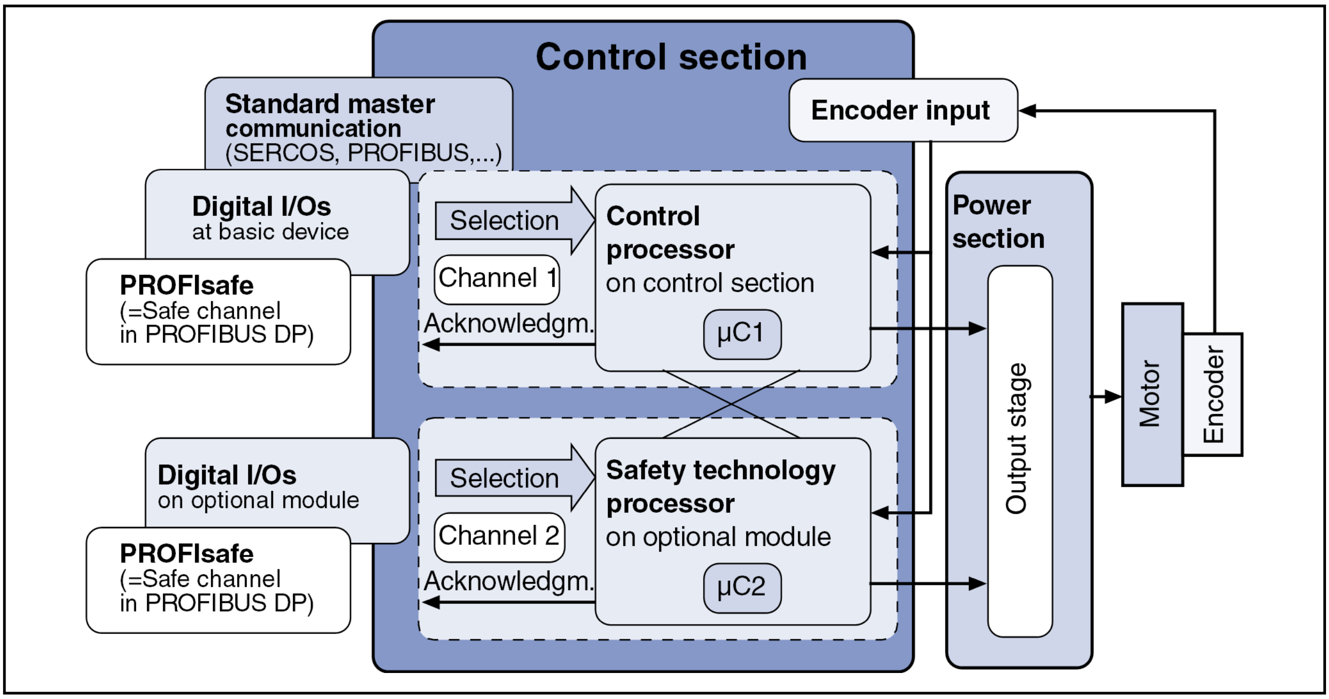

Control section
Standard master communication (SERCOS, PROFIBUS,...)
Encoder input
Digital I/Os at basic device
PROFIsafe (=Safe channel in PROFIBUS DP)
Selection
Channel 1
Acknowledgm.
Control processor on control section
µC1
Power section
Output stage
Motor
Encoder
Digital I/Os on optional module
PROFIsafe (=Safe channel in PROFIBUS DP)
Selection
Channel 2
Acknowledgm.
Safety technology processor on optional module
µC2

Figure name DF000308

Fig. 4-1: Schematic diagram of IndraDrive with integrated safety technology

The above diagram contains all 3 variants of control of integrated safety technology:

- Digital I/Os

- Digital I/Os and master communication
- PROFIsafe (PROFIBUS as master communication is the prerequisite for using PROFIsafe)

See also "Interfaces for selection and acknowledgment"

☞ Using only one encoder is sufficient.

☞ Under "Required motors and measuring systems", the allowed encoder types (measuring systems) are mentioned.

4.1.3 Risk analysis

Before he is allowed to place a machine on the market, the manufacturer of the machine has to carry out a risk analysis according to Machinery Directive 98/37/EEC or 2006/42/EC (after 2009-12-29) in order to determine the hazards associated with the use of the machine.

The risk analysis is a multilevel, iterative process. The procedure is described in detail in "EN ISO 14121 - Safety of machinery - Risk assessment" . This documentation can only give a very short overview on the subject of risk analysis; users of integrated safety technology are obligated to intensively study the respective standards and legal status.

The risk analysis carried out provides you the requirements for determining the category for safety-related control units according to the valid C-standard the safety-relevant parts of the machine control have to comply with.

☞ For more detailed information on the required Safety Integrity Levels (SIL) and Performance Levels (PL), please refer to the applied component- and machine-relevant standards in "Safety-relevant standards and regulations".

Procedure

To obtain the highest possible degree of safety, the machine manufacturer when choosing the solutions has to apply the following basic principles in the indicated order:

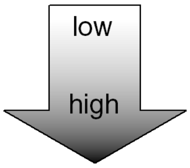
1. Eliminate or minimize the hazards by construction measures.
2. Take the required protective measures against hazards that cannot be eliminated.
3. Document the remaining risks and inform the user of these risks.

Simplification by use of integrated safety technology

When using integrated safety technology, the machine manufacturer will benefit from the following simplifications:

- The safety-related components of the IndraDrive range with the options "Safe Motion" or "Safe Torque Off" are suited for applications up to SIL 2 or SIL3 (only "Safe Torque Off") of IEC EN 62061. This means that functions realized with the optional safety technology modules of the IndraDrive range comply with SIL1, SIL2 or SIL3 (only "Safe Torque Off") of IEC EN 62061.
- The safety functions integrated in IndraDrive were certified by TÜV Rheinland®; this guarantees the user that the solution complies with the state-of-the-art / the conformity of the components according to Machinery Directive 98/37/EC or 2006/42/EC (after 2009-12-29) is ensured.

Safety Integrity Level (SIL): relation between the SILs of IEC 62061 and the Performance Level (PL) of EN ISO 13849-1

Performance Level (PL)	Average probability of dangerous failure [1/h] (PFH)	Safety Integrity Level (SIL)	Risk
a	$\geq 10^{-5}...<10^{-4}$	-	
b	$\geq 3*10^{-6}...<10^{-5}$	1	
c	$\geq 10^{-6}...<3*10^{-6}$	1	
d	$\geq 10^{-7}...<10^{-6}$	2	
e	$\geq 10^{-8}...<10^{-7}$	3	

Tab. 4-1: Safety Integrity Level: failure limit values for a safety function of a PDS(SR)

4.2 Product presentation

4.2.1 What is "Integrated Safety Technology"?

The control sections of the IndraDrive range can be equipped with one of the following optional modules:

- One optional module "Safe Torque Off" ("L2") or
- One optional module "Safe Motion" ("S2")

By the mentioned optional modules, IndraDrive is equipped with integrated safety technology which provides the user with an electronic starting lockout, as well as with universally programmable safe motion and standstill monitoring.

Definition

"Safe Motion" means application-related safety functions which are applicable for personal protection at machines according to EN ISO 13849-1 Category 3 PL d and IEC EN 62061 SIL 2.

"Safe Torque Off" means application-related safety functions which are applicable for personal protection at machines according to EN ISO 13849-1 Category 3 PL e and IEC EN 62061 SIL 3.

Selecting the function

The safety functions can be alternatively selected via

- 24 V inputs at the drive controller or
- 24 V inputs at the drive controller and master communication (one channel each) or
- The safe channel in PROFIBUS (PROFIsafe)

Certification

The safety technology was certified by TÜV Rheinland®; the NRTL listing by TÜV Rheinland of North America is in preparation.

Requirements that can be realized

The integrated safety technology is independent of the type of master communication, the higher-level control unit and the supply modules. It is available as an optional module for the standard drive system. The following requirements can be implemented in the machine or in the installation:

- Measures in accordance with EN ISO 12100-2, if accessing the danger zone is required, for example, for equipping, teaching or material withdrawal.
- Requirements for safety-related parts of control units according to EN ISO 13849-1 Category 3 PL d and IEC EN 62061 SIL 2 (when using "Safe Motion") or EN ISO 13849-1 Category 3 PL d/PL e and IEC EN 62061 SIL 2/SIL 3 (when using "Safe Torque Off"), as required

in EN 1010-1 (printing and paper converting machines), EN 12415 (turning machines) and EN 12417 (machining centres).

- Control functions in the case of error according to EN 60204-1 (see "Using Diversity" in EN 60204-1).

4.2.2 Integrated safety technology as IndraDrive platform solution

The different characteristics (e.g. PROFIsafe) require different hardware:

Control section type	Description	Characteristics of integrated safety technology		
		Safe Torque Off (optional module "L2")	Safe Motion (optional module "S2")	
			Digital I/Os	PROFIsafe
CSH01.1C	ADVANCED	X	X	X
CSH01.3C	ADVANCED	X	X	X
CSB01.1C	BASIC UNIVERSAL (single-axis)	X	-	-
CDB01.1C	BASIC UNIVERSAL (double-axis)	X	X	X
CSB01.1N-FC	BASIC OPENLOOP	-	-	-
CSB01.1N-AN	BASIC ANALOG	X	-	-
CSB01.1N-SE	BASIC SERCOS	X	-	-
CSB01.1N-PB	BASIC PROFIBUS	X	-	-

Tab. 4-2: Overview of hardware requirements for integrated safety technology

☞ To employ the integrated safety technology "Safe Motion" or "Safe Torque Off" according to IEC EN 61508 or EN ISO 13849-1, at least the firmware version MP*07VRS or higher has to be used in the drive.

In addition to the optional module "S2", using PROFIsafe requires the master communication module "PROFIBUS" (PB) together with the respective firmware version (as of MP*07VRS)!

4.2.3 Characteristics and classification of safety technology

Functionality levels

The available integrated safety functions can be divided into 2 levels:

- Level 1: Purely hardware-based safety technology, "Safe torque off" is part of it (optional safety technology module "L2" required)
- Level 2: Extensive integrated safety technology including all other safety functions, such as "Safely-limited speed", "Safely-monitored position",... (optional safety technology module "S2" required)

Characteristics regarding the interfaces

Apart from the classification of the safety functions, we distinguish the types of control (e.g. digital I/Os or PROFIBUS). The following characteristics are supported:

- Digital I/Os
- PROFIsafe

4.3 Safety-relevant standards and regulations

4.3.1 General information

☞ Standard documents and sheets are subject to copyright protection and Bosch Rexroth cannot pass them on. If required, contact the authorized sales agencies; in Germany directly contact Beuth Verlag GmbH (http://www.beuth.de).

Below the user will find a short overview of the relevant standards for the use of safety-related control units.

This documentation does not claim completeness; besides, only the safety-relevant standards and regulations for functional safety are taken into consideration.

4.3.2 Standards relevant to components

Product group	Standard	Title
Electric drives	IEC EN 61800-5-2	Adjustable speed electrical power drive systems, Part 5-2: Safety requirements - Functional
Complex controls	IEC 61508-1 to IEC 61508-7	Functional safety of electrical/electronic/programmable electronic safety-related systems

Tab. 4-3: Standards relevant to components

4.3.3 Standards relevant to machinery

Standard	Title
EN ISO 12100-1 and EN ISO 12100-2	Safety of machinery - Basic concepts, general principles for design
EN ISO 14121	Safety of machinery - Risk assessment
IEC EN 60204-1	Safety of machinery - Electrical equipment of machines
IEC EN 62061	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN ISO 13849-1 EN ISO 13849-2	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design Part 2: Validation
EN ISO 13850	Safety of machinery - Emergency stop - Principles for design
DIN EN 1037	Safety of machinery - Prevention of unexpected start-up
EN ISO 13855	Safety of machinery - The positioning of protective equipment in respect of approach speed of parts of the human body
DIN EN 1088	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
EN ISO 11161	Safety of machinery - Integrated manufacturing systems - Basic requirements
EN ISO 10218-1 EN ISO 10218-2	Robots and robotic devices - Safety requirements for industrial robots Part 1: Robots Part 2: Robot system and integration
DIN EN 1010-1	Safety of machinery - Safety requirements for the design and construction of printing and paper converting machines, Part 1: Common requirements
DIN EN 848-3	Safety of woodworking machines - One side moulding machines with rotating tools, Part 3: Numerically controlled (NC) boring and routing machines
DIN EN 415-1 to DIN EN 415-8	Safety of packaging machines

Standard	Title
DIN EN 201 DIN EN 201/A2	Plastics and rubber machines - Injection moulding machines - Safety requirements
DIN EN 12415	Safety of machine tools - Small numerically controlled turning machines and turning centres
DIN EN 12417	Machine tools - Safety - Machining centres
DIN EN 13218	Machine tools - Safety - Stationary grinding machines

Tab. 4-4: Standards relevant to machinery

4.3.4 Overview of the required safety categories in C-standards

The overview below shows the required safety categories for safety-related parts of control units in C-standards.

	EN 12417 Machining centres	EN ISO 23125 Automatic lathes	EN 1010 Printing and paper converting machines	EN ISO 10218-1 Robot	EN ISO 11161 Integrated manufacturing systems	DIN EN 848-3 Woodworking machines
Enabling control	Category 3	Category 3	-	Category 3	Determined by risk analysis within the scope of the standards EN ISO 13849 / EN ISO 14121	Category 3
Speed reduction, incl. protection against unexpected start-up (n=0)	Category 3	Category 3	Category 3	Category 3		Category 3
	Category B and enabling control device					Category B and enabling control device
Locking of protective equipment	Category 3	Category 3	Category 3	Category 3		Category 3 (electronic)
						Category 1 (with contacts)
Limitation of end positions	-	-		Category 3		-
Emergency stop	Category 1 (with contacts)	Category 1 (with contacts)		According to EN 60204-1		Category 1 (with contacts)
	Category 3 (electronic)	Category 3 (electronic)	Category 3			Category 3 (electronic)

Tab. 4-5: Requirements for safety-related control units in C-standards

4.3.5 Standards and regulations for PROFIBUS / PROFIsafe

Subject	Standard	Title
PROFIBUS	IEC 61158	Digital data communication for measurement and control - Fieldbus for use in industrial control systems
PROFIsafe	PNO Order No: 3.092	Profile for Safety Technology, Version 1.30
PROFIsafe	PNO Order No: 3.232	Requirements for Installation, Immunity and electrical Safety, Version 1.0

Tab. 4-6: Standards and regulations for PROFIBUS / PROFIsafe

4.3.6 EC directives

Description	Title
Directive 2006/42/EC	Machinery Directive
Directive 2006/95/EC	Low-Voltage Directive
Directive 2004/108/EC	EMC Directive

Tab. 4-7: EC Directives

4.4 Overview of Functions and Characteristics

4.4.1 Characteristics of Integrated Safety Technology

Introduction

Presently there are 3 different characteristics of integrated safety technology which differ as regards complexity and functionality.

- Safe Torque Off [pure hardware solution (optional safety technology module "L2")]
- Safe Motion [hardware solution (optional safety technology module "S2") and firmware solution]
- PROFIsafe [hardware solution (optional safety technology module "S2" and PROFIBUS master communication) and firmware solution]

The paragraphs below briefly explain the differences of the characteristics of integrated safety technology to allow you distinguishing them.

☞ For detailed information on the characteristics of integrated safety technology and the functions they provide, see chapter "Integrated Safety Functions".

Drive System With Optional Safety Technology Module "Safe Torque Off"

On the optional safety technology module "Safe Torque Off" ("L2"), there are 24 V inputs available for dual-channel selection and a floating changeover contact for dual-channel feedback (all 3 connections can be accessed).

By means of the optional safety technology module "Safe Torque Off", the drive can be protected against accidental restart and thereby be kept in a safe state.

Drive System With Optional Safety Technology Module "Safe Motion"

On the optional safety technology module "Safe Motion" ("S2"), there are the 24 V inputs of channel 2 available for selecting the application-related safety functions. The inputs of channel 1 can be connected either via the master communication or via the standard inputs of the drive controller. In addition, 24 V outputs for acknowledgment of safety are available on the optional module.

By means of the optional safety technology module "Safe Motion", it is possible to realize application-related safety functions of safe standstill and safe motion in the drive.

Drive System With Integrated Safety Technology "PROFIsafe"

For a drive system with integrated safety technology "PROFIsafe", the optional safety technology module "Safe Motion" ("S2") and PROFIBUS as master communication have to be available in the drive. Of the optional module inputs it is only the home switch that is used for this characteristic, as the safety function selection and the acknowledgment take place via the safe PROFIsafe protocol of the master communication.

By means of PROFIsafe, it is possible to realize application-related safety functions of safe standstill and safe motion in the drive via PROFIBUS.

4.4.2 Supported Safety Technology Functions

Introduction

The safety technology functions can be divided into the following categories:

- Normal operation and special mode
- "Safe standstill"
- "Safe motion"
- Auxiliary functions
- "Safe feedback"

Safe Standstill

The category "Safe standstill" includes the individual functions:

- Safe torque off
- Safe stop 1
- Safe stop 2
- Safe stop 1 (Emergency stop)
- Safe braking and holding system

☞ The functions "Safe stop 1", "Safe stop 2" and "Safe stop 1 (Emergency stop)" include the Safely-monitored stopping process (category of auxiliary functions).

Safe Motion

The category "Safe motion" includes the individual functions:

- Safe maximum speed
- Safely-limited speed
- Safe direction
- Safely-monitored deceleration
- Safely-limited increment
- Safely-monitored position
- Safely-limited position

☞ The special mode "Safe motion" includes the safely-monitored stopping process (category of auxiliary functions).

Safe Feedback

The category "Safe feedback" includes the individual functions:

- Safe diagnostic outputs
- Safe inputs/outputs
- Safe door locking

Auxiliary Functions

- Safely-monitored stopping process
- Safe homing procedure (is required for "Safely-monitored position" and "Safely-limited position")
- Safe parking axis
- "Safe brake check" (is required for "Safe braking and holding system")

Overviews

Safety technology function category	Safety technology function
Safe standstill	Safe torque off

Tab. 4-8: Safety Technology Function With Optional Module "Safe Torque Off" ("L2")

Safety technology function category	Safety technology function
Normal operation and special mode	Safe maximum speed
Normal operation and special mode	Safe direction
Normal operation and special mode	Safely-limited position
Safe standstill	Safe stop 1 (Emergency stop)
Safe standstill	Safe stop 1
Safe standstill	Safe stop 2
Safe standstill	Safe braking and holding system
Safe motion	Safely-limited speed
Safe motion	Safe direction
Safe motion	Safely-limited increment
Safe motion	Safely-monitored position
Safe feedback	Safe diagnostic outputs
Safe feedback	Safe door locking
Safe feedback	Safe inputs/outputs (1)
Auxiliary functions	Safely-monitored stopping process
Auxiliary functions	Safe homing procedure
Auxiliary functions	Safe parking axis
Auxiliary functions	Safe brake check

(1) Only available via master communication "PROFIBUS" (PROFIsafe)

Tab. 4-9: Overview of Available Safety Technology Functions With Optional Module "Safe Motion"

4.4.3 Performance

Time Response and Reaction Times

The performance of integrated safety technology for control via the digital I/Os of the optional safety technology module ("S2") is as follows:

- Internal safety functions processed in 2 ms clock
- System control runs in 1 ms clock
- Error reaction takes place in 1 ms clock

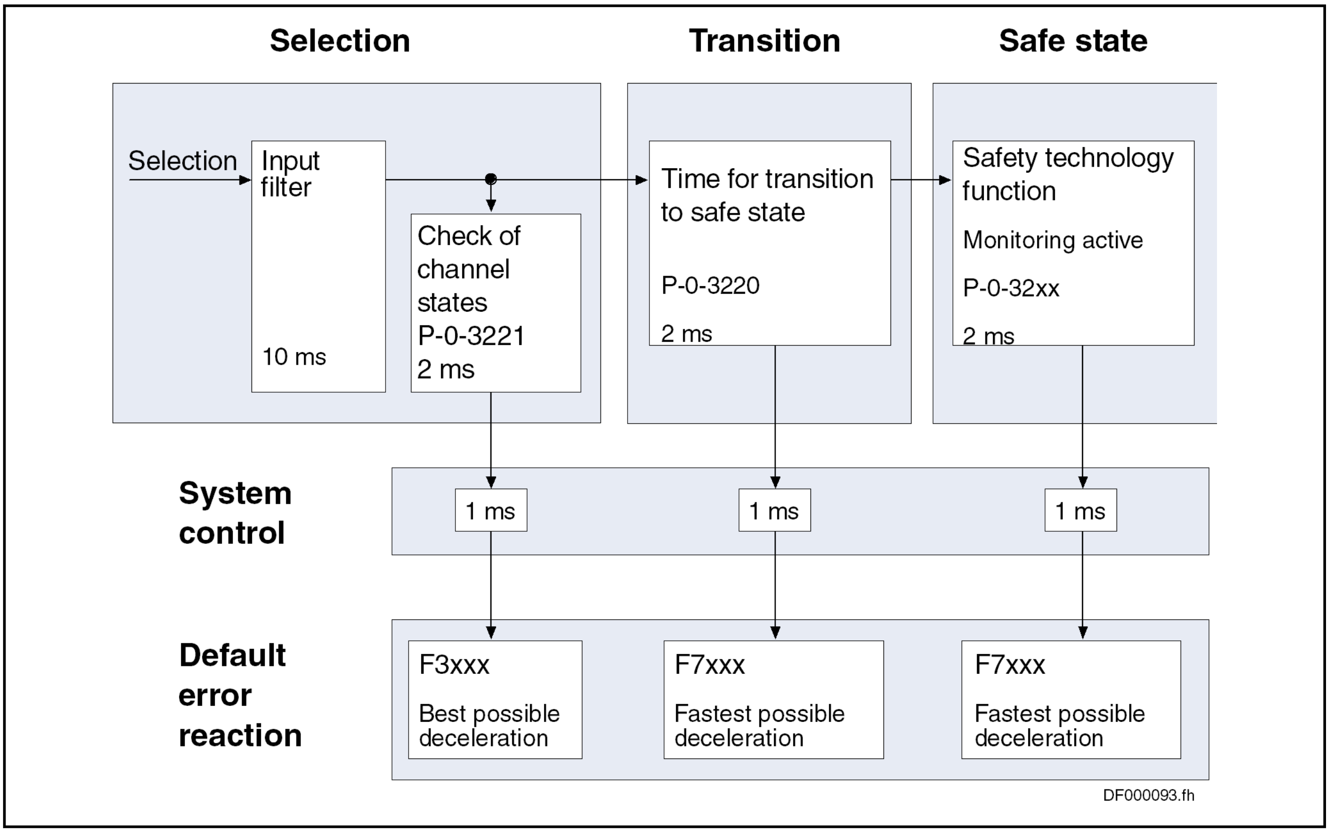


Figure name DF000093

Fig. 4-2: Reaction Times I/O (Optional Module "S2")

4.5 Safety characteristics of the safety system

4.5.1 Introduction

For using the optional safety technology modules "Safe Motion" or "Safe Torque Off", the "IndraDrive" system has been certified according to IEC 61508, IEC EN 61800-5-2, IEC EN 62061 and ISO EN 13849-1.

The risk assessment and risk reduction of a machine require assessing the safety functions of the individual components. The interaction of the components has to be taken into account, too. Therefor, it is necessary to determine the total PFH value for the machine or the machine part (e.g., a safety zone). The total PFH value allows assessing whether the required "Safety Integrity Levels" (SIL) or "Performance Levels" (PL) have been complied with. For the optional safety technology modules "Safe Motion" and "Safe Torque Off", the chapters below show how the PFH value can be determined for a drive system and how additional external components have to be integrated.

4.5.2 Safe Torque Off

Drives equipped with the optional safety technology module "Safe Torque Off" comply with the following "Safety Integrity Levels" (SIL) or "Performance Levels" (PL):

- SIL1, SIL2 or SIL3 according to IEC EN 62061
- Category 1, PL c and category 3 PL d/PL e according to EN ISO 13849-1

Depending on the "Safety Integrity Level" or "Performance Level" to be attained, there are the following safety characteristics:

Description	SIL1 / PL c	SIL2 / PL d	SIL3 / PL e
PFH[1)]	$50*10^{-9}$ 1/h (0.5% SIL1)	$<10*10^{-9}$ 1/h (1% SIL2)	$<2*10^{-9}$ 1/h (2% SIL3)
Mission Time	175,200 h (20 years)	175,200 h (20 years)	175,200 h (20 years)
"Proof Test" interval	175,200 h (20 years)	175,200 h (20 years)	175,200 h (20 years)
$MTTF_{d/channel}$[1)]	100 years [corresponds to the total value of the $MTTF_d$ for the safety function, as it is category 1 (single-channel system)]	>200 years	>200 years
DC_{avg}	-	>90%	>95%
Test interval	-	<168 h	<24 h[2)]

[1)] The specified safety characteristics refer to an average ambient temperature of 40°C (see also "Ambient and operating conditions" in the Project Planning Manual).

[2)] When guards are used, the test interval can be extended if a successful test was carried out directly before the safety area is enabled (see "Safe Torque Off (STO)")

☞ The safety characteristics are independent of the motor type and encoder type used.

For the selection configuration, it is possible to choose freely whether the optional safety technology module "Safe Torque Off" is selected via an "N/C-N/O" or "N/C-N/C" combination. This does not have any influence on the PFH value which is used.

For SIL1 / PL c, it is not required to carry out the dynamization of the safety function selection.

SIL3 / PL e can be attained under the following conditions:

- The selection, test and evaluation of the safety function is carried out via a safety master which also attains SIL3 / PL e.
- The time interval of forced dynamization (test interval) must be ≤ 24 hours. (When guards are used, the test interval can be extended if a successful test was carried out directly before the safety area is enabled).

☞ **"Mission Time" and "Proof Test" interval**

- The "Mission Time" of all components used has to be observed and complied with. After the "Mission Time" of a component has elapsed, the component has to be discarded or replaced. It is not allowed to continue operating the component!
- After the component was discarded ("Mission Time" has elapsed), it has to be ensured that the component cannot be reused (e.g., by disabling it).
- If a component (with valid "Mission Time") is decommissioned, the "Mission Time" has to be recorded and continued when the component is commissioned again.
- There is no specified "Proof Test" for the IndraDrive system. Therefore, the "Mission Time" cannot be reset by a "Proof Test".

4.5.3 Safe Motion

Drives equipped with the optional safety technology module "Safe Motion" comply with the following "Safety Integrity Levels" (SIL):

- SIL2 according to IEC EN 62061 and IEC 61800-5-2
- Category 3, PL d according to EN ISO 13849-1

Independent of the safety functions of the axis used, there are the following safety characteristics:

Description	SIL2 / PL d
PFH[1]	<5*10^{-9} 1/h (0.5% of SIL2)
Mission Time	175,200 h (20 years)
"Proof Test" interval	175,200 h (20 years)
MTTF$_{d/channel}$[1]	> 90 years
DC$_{avg}$	> 95%

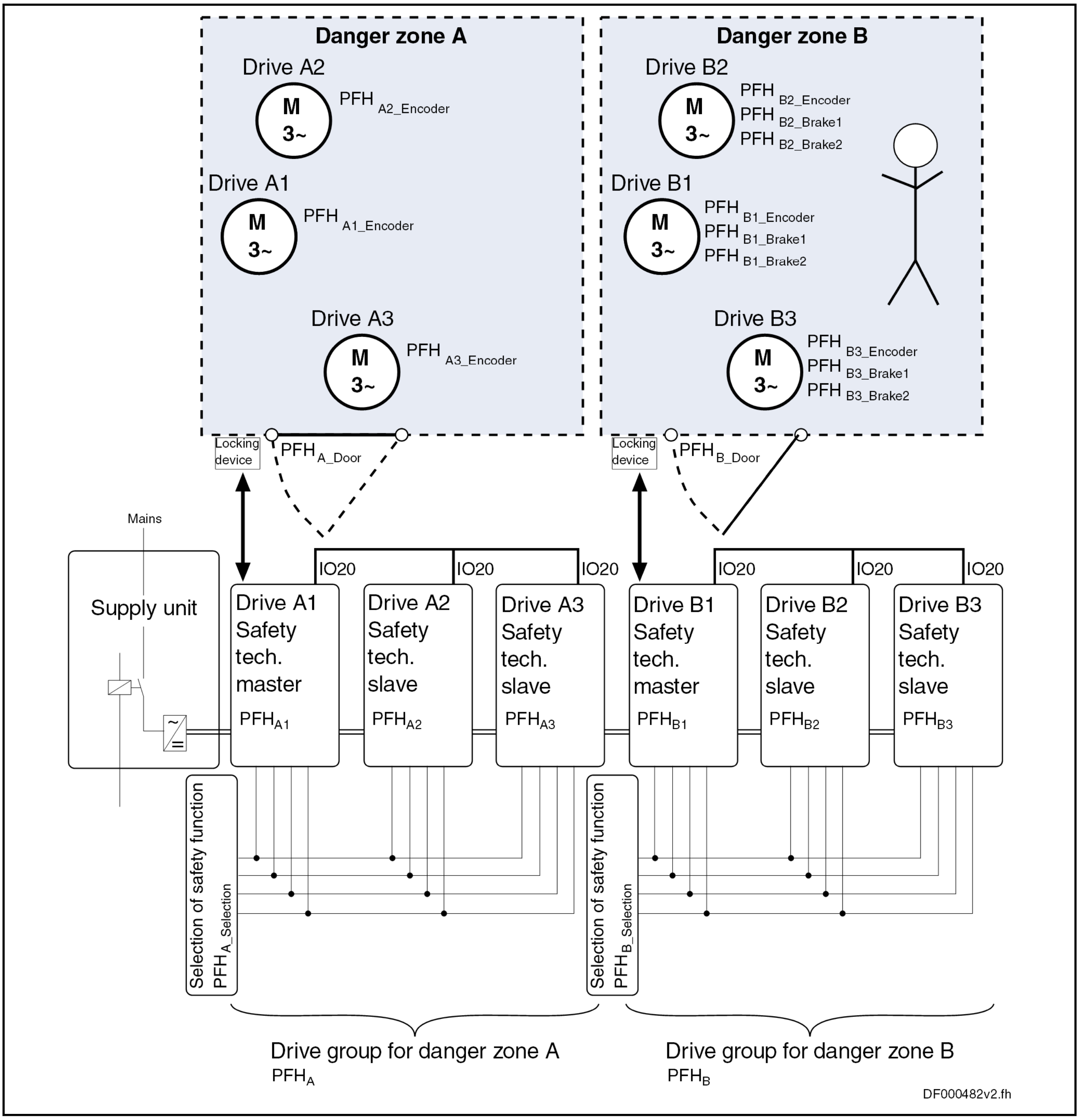
[1] The specified safety characteristics refer to an average ambient temperature of 40°C (see also "Ambient and operating conditions" in the Project Planning Manual).

☞ **"Mission Time" and "Proof Test" interval**

- The "Mission Time" of all components used has to be observed and complied with. After the "Mission Time" of a component has elapsed, the component has to be discarded or replaced. It is not allowed to continue operating the component!
- After the component was discarded ("Mission Time" has elapsed), it has to be ensured that the component cannot be reused (e.g., by disabling it).
- If a component (with valid "Mission Time") is decommissioned, the "Mission Time" has to be recorded and continued when the component is commissioned again.
- There is no specified "Proof Test" for the IndraDrive system. Therefore, the "Mission Time" cannot be reset by a "Proof Test".

To determine the required total PFH value of an installation or a safety zone, the PFH values of the individual axes and of the required external components have to be used for calculation as follows. The figure below shows an exemplary machine application with two safety areas. The calculation is made using this application:

System overview


Danger zone A
Drive A2
M 3~
PFH A2_Encoder
Drive A1
PFH A1_Encoder
Drive A3
PFH A3_Encoder
Danger zone B
Drive B2
PFH B2_Encoder
PFH B2_Brake1
PFH B2_Brake2
Drive B1
PFH B1_Encoder
PFH B1_Brake1
PFH B1_Brake2
Drive B3
PFH B3_Encoder
PFH B3_Brake1
PFH B3_Brake2
Locking device
PFH A_Door
PFH B_Door
Mains
Supply unit
IO20
Drive A1 Safety tech. master PFHA1
Drive A2 Safety tech. slave PFHA2
Drive A3 Safety tech. slave PFHA3
Drive B1 Safety tech. master PFHB1
Drive B2 Safety tech. slave PFHB2
Drive B3 Safety tech. slave PFHB3
Selection of safety function PFH A_Selection
Selection of safety function PFH B_Selection
Drive group for danger zone A PFHA
Drive group for danger zone B PFHB
DF000482v2.fh

PFH$_A$	Total PFH value of safety zone A
PFH$_{Ax}$	PFH value of drive Ax
PFH$_{Ax\_Encoder}$	PFH value of the safety technology encoder of drive Ax
PFH$_{A\_Selection}$	PFH value of the selection of safety zone A
PFH$_{A\_Door}$	PFH value of the locking device of safety zone A
PFH$_B$	Total PFH value of safety zone B
PFH$_{Bx}$	PFH value of drive Bx
PFH$_{Bx\_Encoder}$	PFH value of the safety technology encoder of drive Bx
PFH$_{Bx\_Brakex}$	PFH value of the brake x of drive Bx
PFH$_{B\_Selection}$	PFH value of the selection of safety zone B

PFH_{B_Door} PFH value of the locking device of safety zone B

Fig. 4-3: Safe Motion: Determining the PFH for individual safety zones

PFH calculation of safety zone A (without safe braking and holding system)

To calculate the PFH value for safety zone A (see fig. 4-3 "Safe Motion: Determining the PFH for individual safety zones" on page 38), a valid PFH value has to be available for all components which have an influence on the safety function (if necessary, procure the PFH value from the component manufacturer).

In this example, it is assumed that the safe braking and holding system is not used at any of the axes of this safety zone.

$$PFH_A=PFH_{A\_Selection}+PFH_{A\_Door}+PFH_{A1}+PFH_{A2}+PFH_{A3}+PFH_{A1\_Encoder}+PFH_{A2\_Encoder}+PFH_{A3\_Encoder}$$

Tab. 4-10: Safe Motion: Formula to calculate PFH for safety zone A

The following conditions/restrictions apply to the general use of the formula for PFH calculation for safety zone A:

Variable	Value	Description
[1]$PFH_{A\_Selection}$	See manufacturer's specification	Enter the sum of the individual PFH values of the switches or safety devices involved in the selection. In this case, there is no distinction made as to which safety functions are selected in the drive.
DC_{Door}	99%	The diagnostic coverage attained by the monitoring functions in the drive.
[1]PFH_{A_Door}	See manufacturer's specification	Enter "0" for this variable, if the safety technology master (drive A1) does not directly control a safety door. All other receivers of acknowledgment do not need to be considered for the IndraDrive safety system, and have to be taken into account where appropriate in the machine design.
[1]PFH_{Ax}	$<5 *10^{-9}$ 1/h (0.5% of SIL2)	This value is independent of the parameterized safety functions and thresholds.
$DC_{Encoder}$	90%	The diagnostic coverage attained by the monitoring functions in the drive.
[1]$PFH_{Ax\_Encoder}$	See manufacturer's specification (when using Rexroth motors, see "Required motors and measuring systems")	Use the value of the encoder connected to X4 (resp. X4.1 or X4.2). This encoder is used for the safety technology functions.

[1] $PFH=(1-DC)/MTTF_D$

Tab. 4-11: Description of variables to calculate PFH for safety zone A

PFH calculation of safety zone B (with safe braking and holding system)

To calculate the PFH value for safety zone B (see fig. 4-3 "Safe Motion: Determining the PFH for individual safety zones" on page 38), a valid PFH value has to be available for all components which have an influence on the safety function (if necessary, procure the PFH value from the component manufacturer).

In this example, it is assumed that the safe braking and holding system is used at all axes of this safety zone.

$PFH_{Bx\_Brake}=[(\lambda_{Bx\_Brake1} + \lambda_{Bx\_Brake2}) / 400] + (\lambda_{Bx\_Brake1} \times \lambda_{Bx\_Brake2} \times 400)$

$PFH_{B}=PFH_{B\_Selection} + PFH_{B\_Door} +$

$PFH_{B1} + PFH_{B2} + PFH_{B3} +$

$PFH_{B1\_Encoder} + PFH_{B2\_Encoder} + PFH_{B3\_Encoder} +$

$PFH_{B1\_Brake} + PFH_{B2\_Brake} + PFH_{B3\_Brake}$

Tab. 4-12: Safe Motion: Formula to calculate PFH for safety zone B

The following conditions/restrictions apply to the general use of the formula for PFH calculation for safety zone B:

Variable	Value	Description
[1]$PFH_{B\_Selection}$	See manufacturer's specification	Enter the sum of the individual PFH values of the switches or safety devices involved in the selection. In this case, there is no distinction made as to which safety functions are selected in the drive.
DC_{Door}	99%	The diagnostic coverage attained by the monitoring functions in the drive.
[1]PFH_{B_Door}	See manufacturer's specification	Enter "0" for this variable, if the safety technology master (drive B1) does not directly control a safety door. All other receivers of acknowledgment do not need to be considered for the IndraDrive safety system, and have to be taken into account where appropriate in the machine design.
[1]PFH_{Bx}	$<5*10^{-9}$ 1/h (0.5% of SIL2)	This value is independent of the parameterized safety functions and thresholds.
$DC_{Encoder}$	90%	The diagnostic coverage attained by the monitoring functions in the drive.
[1]$PFH_{Bx\_Encoder}$	See manufacturer's specification	Use the value of the encoder connected to X4 (resp. X4.1 or X4.2). This encoder is used for the safety technology functions.
DC_{Brake}	99%	The diagnostic coverage attained by the monitoring functions in the drive.
$\lambda_{Bx\_Brakex}=1/MTTF$	See manufacturer's specification (when using Rexroth motors, see "Required motors and measuring systems")	Probability of **all failures** of the brake, **not only the number of dangerous failures** Only relevant when the safe braking and holding system is used; otherwise enter value "0". Enter the corresponding value of the brake connected to the drive system. Take series-connected devices, such as converters, etc. into account.

1) $PFH=(1-DC)/MTTF_{D}$

Tab. 4-13: Description of variables to calculate PFH for safety zone B

5 Functional principle of integrated safety technology

5.1 Basic functions

5.1.1 Overview

In the case of a standard drive, the axis / spindle / roll is moved according to the command values of the control unit. In this case, incorrect drive motion can be caused by operating errors, incorrect installation in the system, defects in parts or materials, failures in the system. Incorrect drive motion can endanger persons staying in the danger zone of the drive motion, even if the errors only occur for a short time and occasionally.

It is therefore necessary to take measures that limit the effects of errors on the drive motion to a minimum. The residual risk of danger to persons is then considerably reduced.

During operation, the safety functions are monitored by the drive system. For this purpose, three principles for detecting static error states, so-called "sleeping errors", were realized in the system:

- **Dual-channel data processing** with diversitary structure
- **Cross comparison** of the safety-relevant data
- **Dynamization** of static states

These measures ensure that a single error cannot cause the safety functions to be lost.

The installation or machine manufacturer has to determine in how far this is sufficient for an existing installation or machine by a risk analysis according to annex I of Directive 98/37/EWG.

☞ After 2009-12-29, the new Machinery Directive 2006/42/EC must be applied.

The schematic diagram below illustrates the basic functions and functional principles explained in this section:

Functional principle of integrated safety technology

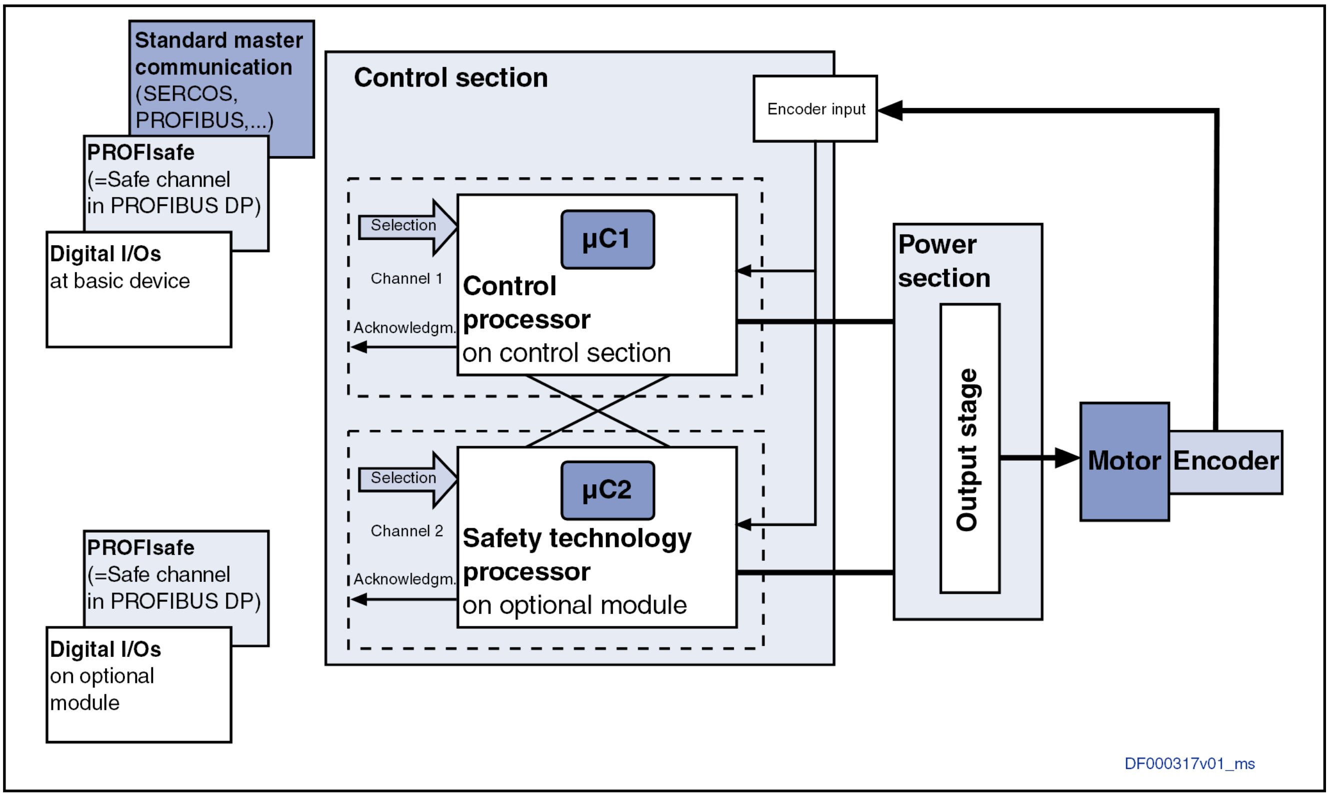

Standard master communication (SERCOS, PROFIBUS,...)
PROFIsafe (=Safe channel in PROFIBUS DP)
Digital I/Os at basic device
Control section
Encoder input
Selection
Channel 1
Acknowledgm.
µC1
Control processor on control section
Selection
Channel 2
Acknowledgm.
µC2
Safety technology processor on optional module
PROFIsafe (=Safe channel in PROFIBUS DP)
Digital I/Os on optional module
Power section
Output stage
Motor
Encoder
DF000317v01_ms

Fig. 5-1: Schematic diagram of IndraDrive with integrated safety technology

5.1.2 Dual-channel structure

All safety-relevant data are transmitted and processed by two independent channels.

- Channel 1: The drive µC (basic control unit) is the first monitoring channel.
- Channel 2: The additional safety technology µC on the optional safety technology module "S2" is the second channel.

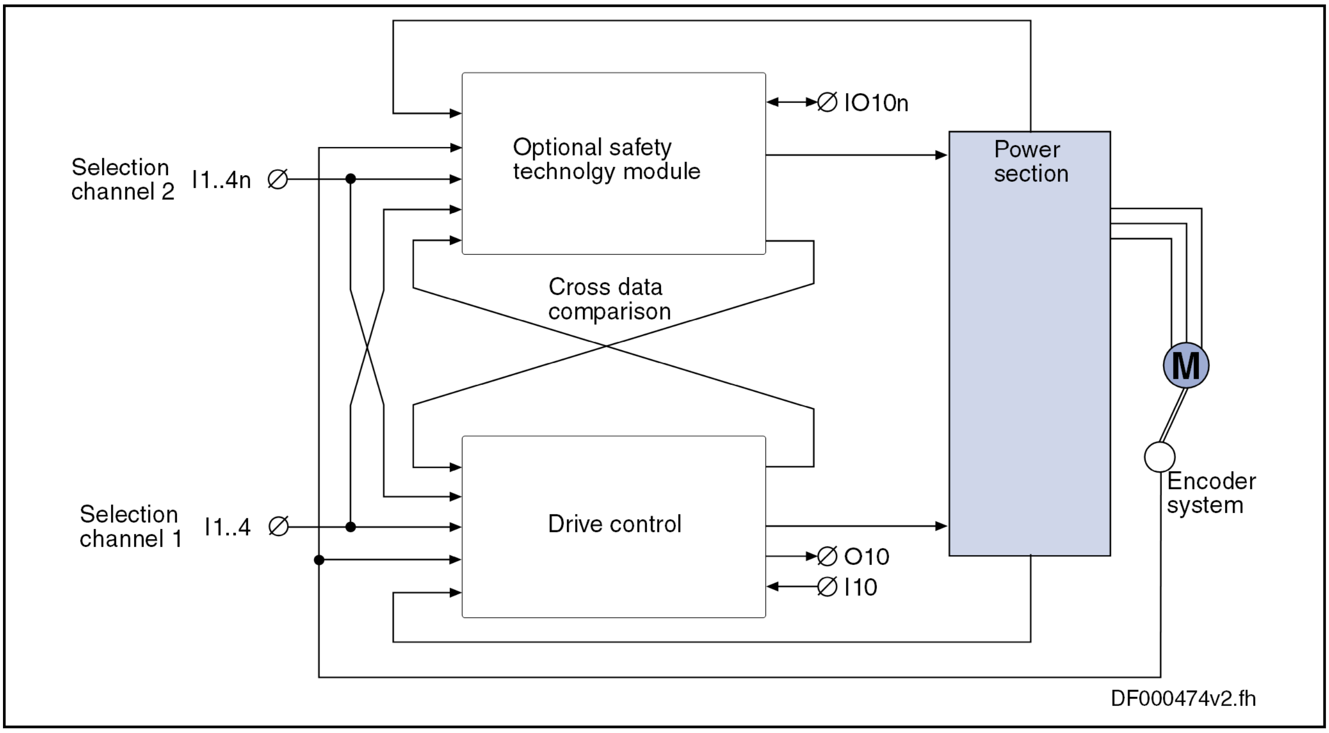


Fig. 5-2: Schematic diagram of the dual-channel structure by the example of I/O interface

5.1.3 Cross data comparison

Brief description

The respective monitoring functions for displaying the safety functions are processed independently in the basic drive (basic control unit) and on the optional safety technology module (safety control unit).

To make sure that the safety functions work with correct (identical) limit values, a cross data comparison is required. If a deviation of the monitored parameters is detected in one of the two channels, this causes the respective error reaction and the drive system goes to the safe state.

Functioning of cyclic cross data comparison

The cross data comparison is started with the "run up" of the drive. As soon as the operating mode ("phase 4") has been reached, the cross data comparison starts.

If the safety parameters of both channels are not identical during operation,

- "E3104 Safety parameters validation error" is generated in normal operation
- The error message "F3140 Safety parameters validation error" or "F7040 Validation error parameterized - effective threshold" is generated in special mode

☞ When one or several safety functions are activated, an additional cross data comparison is carried out by means of safety function selection.

Errors detected by cross data comparison

The following errors are detected by cross data comparison:

- Safety function only activated on one system

- Wrong safety function activated
- Different monitoring parameters used
- Safety function does not work (lifecounter)
- Accidental hardware errors
- Accidental software errors

5.1.4 Dynamization

Brief description

Dynamization is to detect static error states, so-called "sleeping errors", in the safety-relevant circuits. Dynamization takes place, in certain time intervals, automatically in the background without having an effect on the safety function.

Functional principle of dynamization

☞ In the case of safety function selection via PROFIsafe, dynamization does not take place because in this case it is impossible to parameterize selection signals via I/Os and selection via PROFIsafe is safe.

A safety function is selected via an N/C-N/O combination so that one channel of a safety function is always selected (the function is activated/deactivated by the switching).

Drive-internally the active channel (N/O) is cyclically checked.

Common dynamization of the inputs

A dynamization master automatically carries out dynamization for all selected inputs (via O30).

Synchronization of dynamization has to take place via I30.

☞ Due to hardware restrictions, a maximum of 25 drives (including the dynamization master) can be dynamized by a dynamization master!

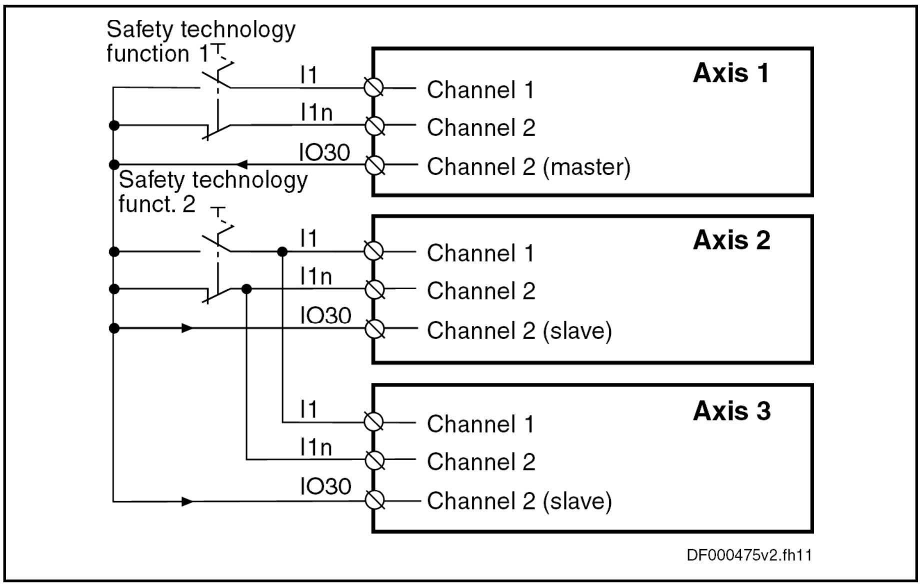


Fig. 5-3: Common dynamization of the inputs via I/O

Separate dynamization for inputs for channel 1 via master communication

When channel 1 is selected via the master communication, separate dynamization for channel 1 and 2 can be parameterized in the drive.

Dynamization of channel 1 and channel 2 takes place via the higher-level control unit. Synchronization of dynamization has to take place via I30 and substitute for I30 ("P-0-3212, Safety technology control word, channel 1").

Dynamization of interrupting circuits

Both the control section in standard design and the optional module "Safe Motion" have their own interrupting circuits.

Drive-internally, the activation of an interrupting circuit is cyclically checked.

5.2 State machine of integrated safety technology

5.2.1 Safety technology operating states

Overview

We distinguish the following safety technology operating states:

- Normal operation (corresponds to normal operation of the drive as a servo positioning axis, for example)
- Special mode "Safe standstill"
- Special mode "Safe motion"
- Safe stop 1 (Emergency stop)

The state diagram below illustrates how the different operating states can be selected with the three activation devices (mode selector, enabling control, SS1 (Emergency stop) switch).

Functional principle of integrated safety technology

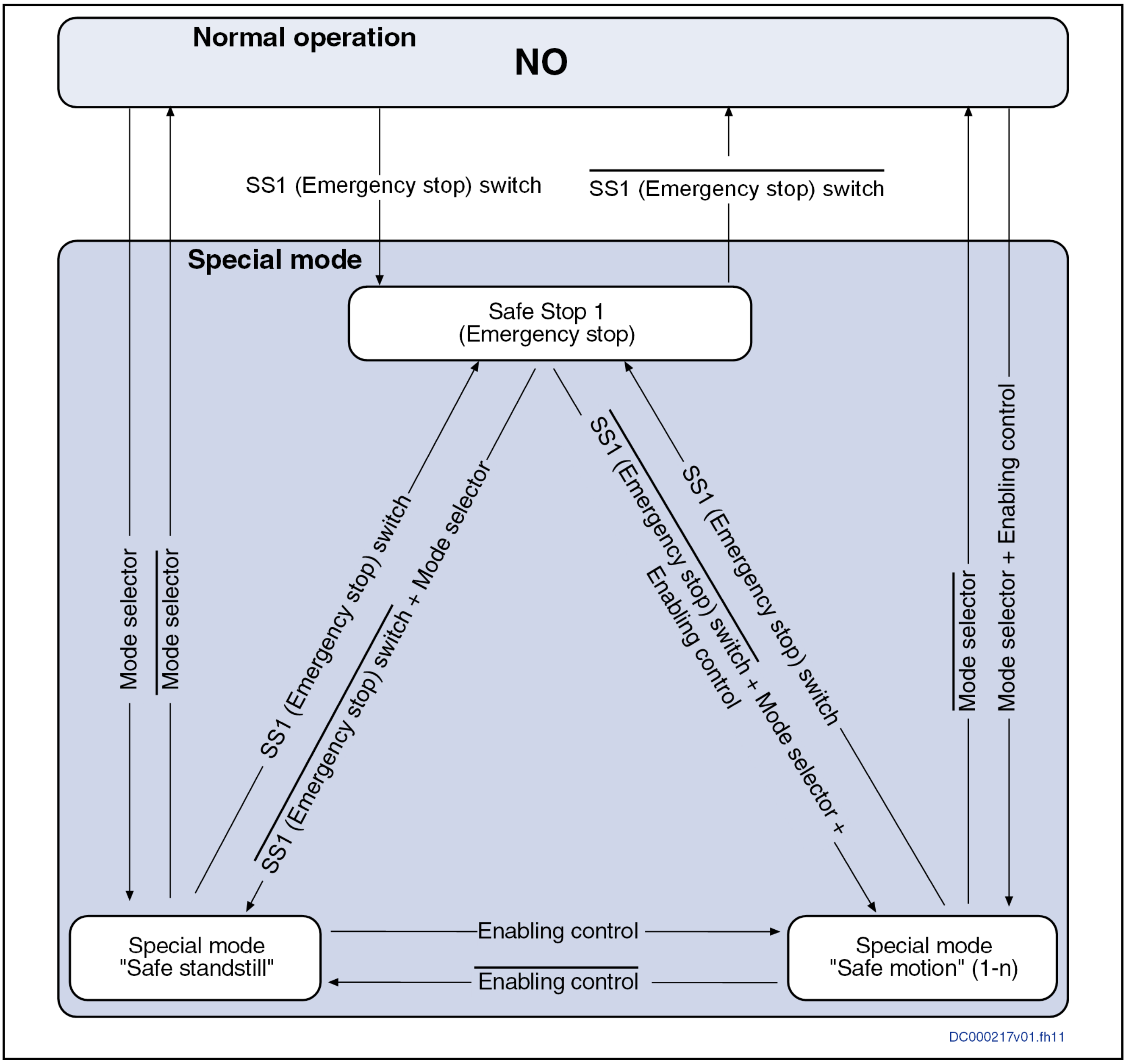

Normal operation
NO
SS1 (Emergency stop) switch
$\overline{\text{SS1 (Emergency stop) switch}}$
Special mode
Safe Stop 1 (Emergency stop)
Mode selector
$\overline{\text{Mode selector}}$
SS1 (Emergency stop) switch
$\overline{\text{SS1 (Emergency stop) switch}}$ + Mode selector
$\overline{\text{SS1 (Emergency stop) switch}}$ + Mode selector + Enabling control
SS1 (Emergency stop) switch
$\overline{\text{Mode selector}}$
Mode selector + Enabling control
Special mode "Safe standstill"
Enabling control
$\overline{\text{Enabling control}}$
Special mode "Safe motion" (1-n)
DC000217v01.fh11

Fig. 5-4: State diagram

Changing the safety technology operating states

Changing between the safety technology operating states takes place by means of the mode selector, the enabling control and the "SS1 (Emergency stop)" switch.

Selecting "Safe stop 1 (Emergency stop)"

"Safe stop 1 (Emergency stop)" can be selected using the "SS1 (Emergency stop)" switch. This selection is independent of the position of the mode selector and the enabling control.

Selecting the operating states using the mode selector

The safety technology operating states "normal operation" and "special mode" can be selected using the mode selector.

Changing states in special mode using enabling control

In the special mode, it is possible to switch between the following safety operating states using an enabling control:

- **Special mode "Safe standstill"**

The following safety functions can be configured in the special mode "Safe standstill" (note: selected via mode selector)

  - "Safe stop 1"
  - "Safe stop 2"

- **Special mode "Safe motion"**

  The following safety functions can be configured in the special mode "Safe motion" (note: selected via enabling control in special mode):

  - "Safely-limited speed"
  - "Safe direction"
  - "Safely-limited increment"
  - "Safely-monitored position"

Using the safety switches "S1" and "S2", four operating states can be selected in the special mode "Safe motion".

Overview of the safety technology functions in the individual operating states

The table below shows useful combinations of safety function selection in the respective safety technology operating states.

Functional principle of integrated safety technology

Safety functions		Control elements for selecting/deselecting safety functions					
		Mode selector	Enabling control	Safety switch 1	Safety switch 2	SS1 (Emergency stop) switch	Home switch
		Position	Position	Position	Position	Position	Available
Normal operation	Safe direction	NO	-	-	-	Off	-
	Safe maximum speed	NO	-	-	-	Off	-
	Safely-limited position	NO	-	-	-	Off	Yes
	Safe stop 1 (Emergency stop)	-	-	-	-	On	-
Special mode safe standstill	Safe stop 2 (SS2)	SM	Off	-	-	Off	-
	Safe stop 1 (SS1)	SM	Off	-	-	Off	-
Special mode safe motion	SLS1 + SDI1 + SLI1+ SMO1	SM	On	Off	□	Off	□
	SLS2 + SDI2 + SLI2 + SMO2	SM	On	On	□	Off	□
	SLS1 + SDI1 + SLI1 + SMP1 + SMO1	SM	On	Off	□	□	Yes
	SLS2 + SDI2 + SLI2 + SMP2 + SMO2	SM	On	On	□	□	Yes
	SLS3 + SDI3 + SLI3 + SMO3	SM	On	Off	On	□	□
	SLS4 + SDI4 + SLI4 + SMO4	SM	On	On	On	□	□
	Safe maximum speed	-	-	-	-	Off	-
	Safely-limited position	-	-	-	-	Off	Yes
	Safely-monitored stopping proc. for SS1 / SS2	SM	Off	-	-	Off	-
	Safely-monitored stopping proc. for Safe stop 1 (Emergency stop)	-	-	-	-	Ein	-
	Safely-monitored stopping proc. for SMM	SM	On	-	-	Off	

NO:	Normal operation
SM:	Special mode
SMM:	Special mode safe motion
SS1:	Safe stop 1 (no torque)
SS2:	Safe stop 2 (control loops are active)
SLS:	Safely-limited speed
SDI:	Safe direction
SLI:	Safely-limited increment
SMP:	Safely-monitored position
SMO:	Safely-monitored transient oscillation
— :	Input for control element is not queried
□ :	No input for control element available (max. 4 inputs)

Fig. 5-5: Combining the safety functions in the respective state when selected via I/Os

☞ The restriction to 4 inputs is abolished when PROFIsafe is used; i.e. more functions can be configured accordingly.

Notes on application

Observe the following points for handling the safety technology operating states:

- If the enabling control is activated in normal operation, the reduction of the command value input can take effect. Switching to the special mode internally activates the monitoring functions for Safe motion after the end of the transition times.
- Before the safety function "Safely-monitored position" is selected, the "Safe homing procedure" has to be carried out. The safe homing procedure requires an input on the optional safety technology module. Only one input will then be available, for example for switching two instead of four operating states in the special mode "Safe motion".
- When user-defined scalings for position, velocity, acceleration and torque or force are used, the following parameterizations are **not allowed**:
  - Scaling factors unequal 1
  - Rotational position resolution unequal 360*10^n (n=1, 2, 3…)

5.2.2 Transition to safe state

Brief description

When a safe state is selected, the command value system has to be accordingly adjusted for the drive. This adjustment takes place in the transition to the safe state. We distinguish the following kinds of transition:

- Transition from normal operation to special mode
- Transition from one special mode to another special mode

Transition can be controlled by the drive or the control unit.

Functional principle

The kind of transition to the special mode (controlled by drive or control unit) has to be parameterized in "P-0-3210, Safety technology configuration".

The transition process is started immediately after the safe operation mode has been selected.

According to parameter setting (controlled by drive or control unit) and selected safe state ("Safe standstill" or "Safe motion"), the transition can be terminated by different events:

- Tolerance time for transition is over (P-0-3220 or P-0-3225)
- Drive enable is reset
- Higher-level control unit gives feedback in "P-0-3212, Safety technology control word, channel 1" that it has adjusted the command value system of the drive

☞ During the transition to the safe state, "Safely-monitored stopping process" is always active (see "Safely-monitored stopping process").

Tolerance time for transition

The tolerance time is monitored during each transition to the special mode. For transition from normal operation / special mode to the safe state, there is one programmable time available for each kind of transition:

- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation

Drive-controlled transition

Drive-controlled transition to "Safe stop 2" takes place by activating the "Drive Halt" function. The drive is shut down with the acceleration and jerk parameterized for this purpose.

For transition to "Safe stop 1" or "Safe stop 1 (Emergency stop)", the drive is shut down according to the best possible deceleration (P-0-0119, bit 0...3) that was parameterized. Subsequently, drive enable is removed.

☞ Transition to the special mode "Safe motion" is always controlled by the NC, independent of the setting in parameter "P-0-3210, Safety technology configuration".

The selected special mode becomes active when the actual velocity of the drive, after the stopping process has been completed, is lower than "P-0-3233, Velocity threshold for safe standstill".

If the actual velocity is not lower than "P-0-3233, Velocity threshold for safe standstill" or the parameterized tolerance time for transition (P-0-3220 or P-0-3225) is over, the error "F7050 Time for stopping process exceeded" is generated.

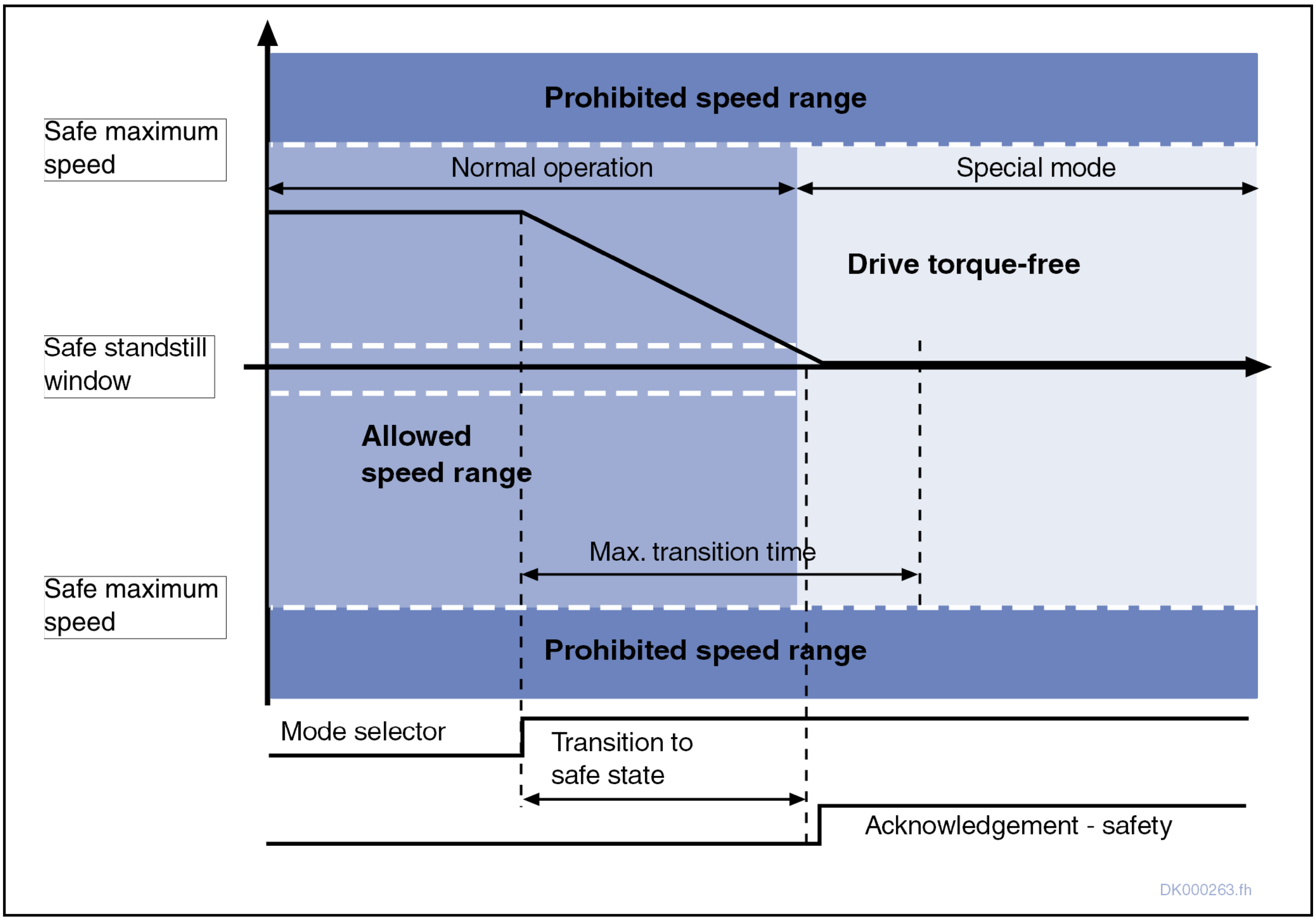


Fig. 5-6: Drive-controlled transition to "Safe stop 1" from normal operation

NC-controlled transition

For NC-controlled transition, the higher-level control unit has to bring the drive to the new command value system.

The selected special mode is only activated after the tolerance time for transition (P-0-3220 or P-0-3225) is over.

When the special mode "Safe standstill" has been selected, a check is run to find out whether the actual velocity of the drive is smaller than "P-0-3233, Velocity threshold for safe standstill"; if this is not the case, the error "F7050 Time for stopping process exceeded" is generated.

When the special mode "Safe motion" has been selected, direct switching to the special mode "Safe motion" takes place after the parameterized transition time is over and the monitoring functions valid in this mode become active. The corresponding error is generated in case the monitors trigger.

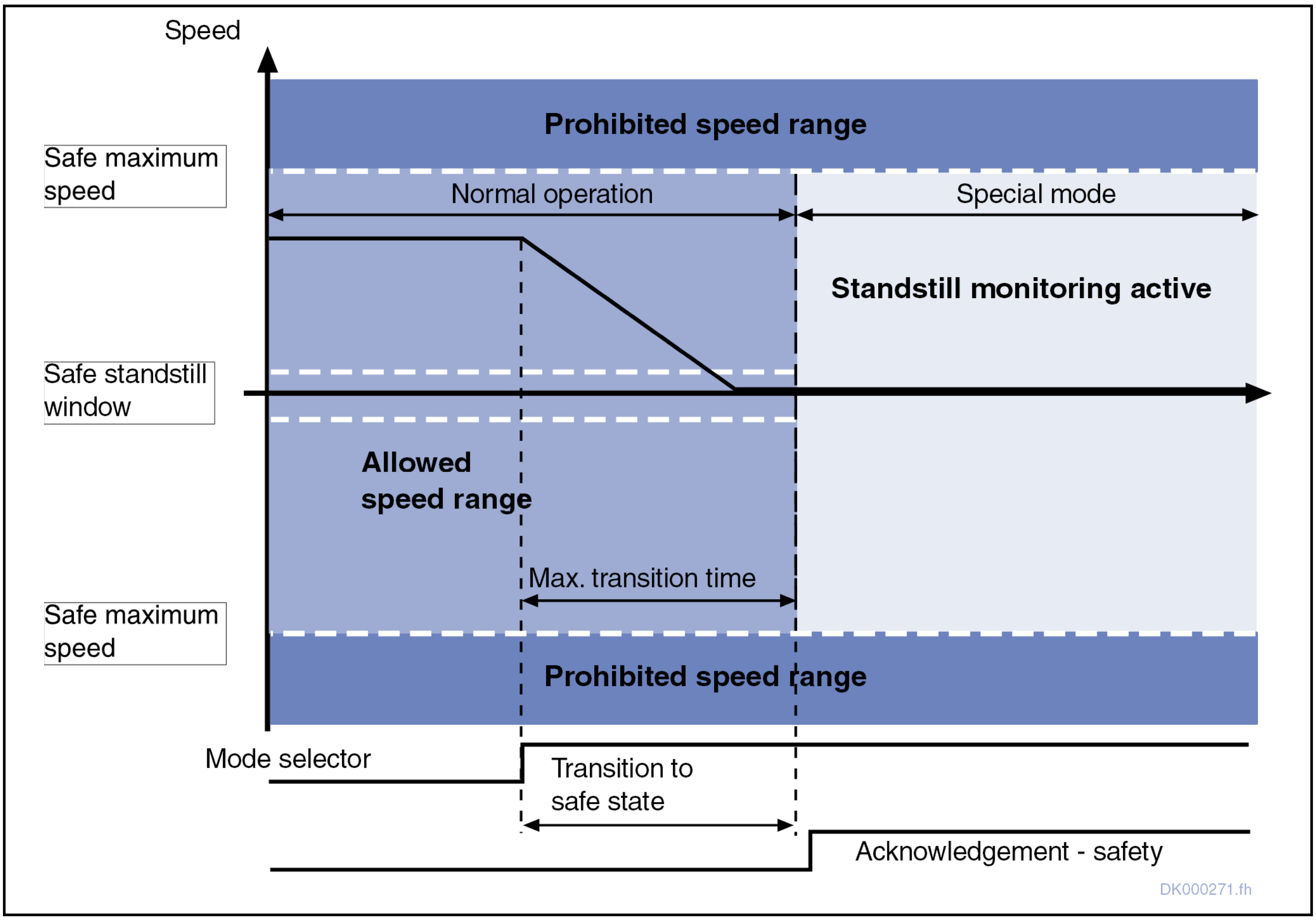


Fig. 5-7: NC-controlled transition to "Safe stop 2" from normal operation

To avoid unnecessary waiting times, the selected safety technology operating status is activated in the case of all transitions, as soon as

- drive enable has not been set and
- the actual velocity of the drive is lower than "P-0-3233, Velocity threshold for safe standstill" (only with special mode "Safe standstill" selected).

Functional principle of integrated safety technology

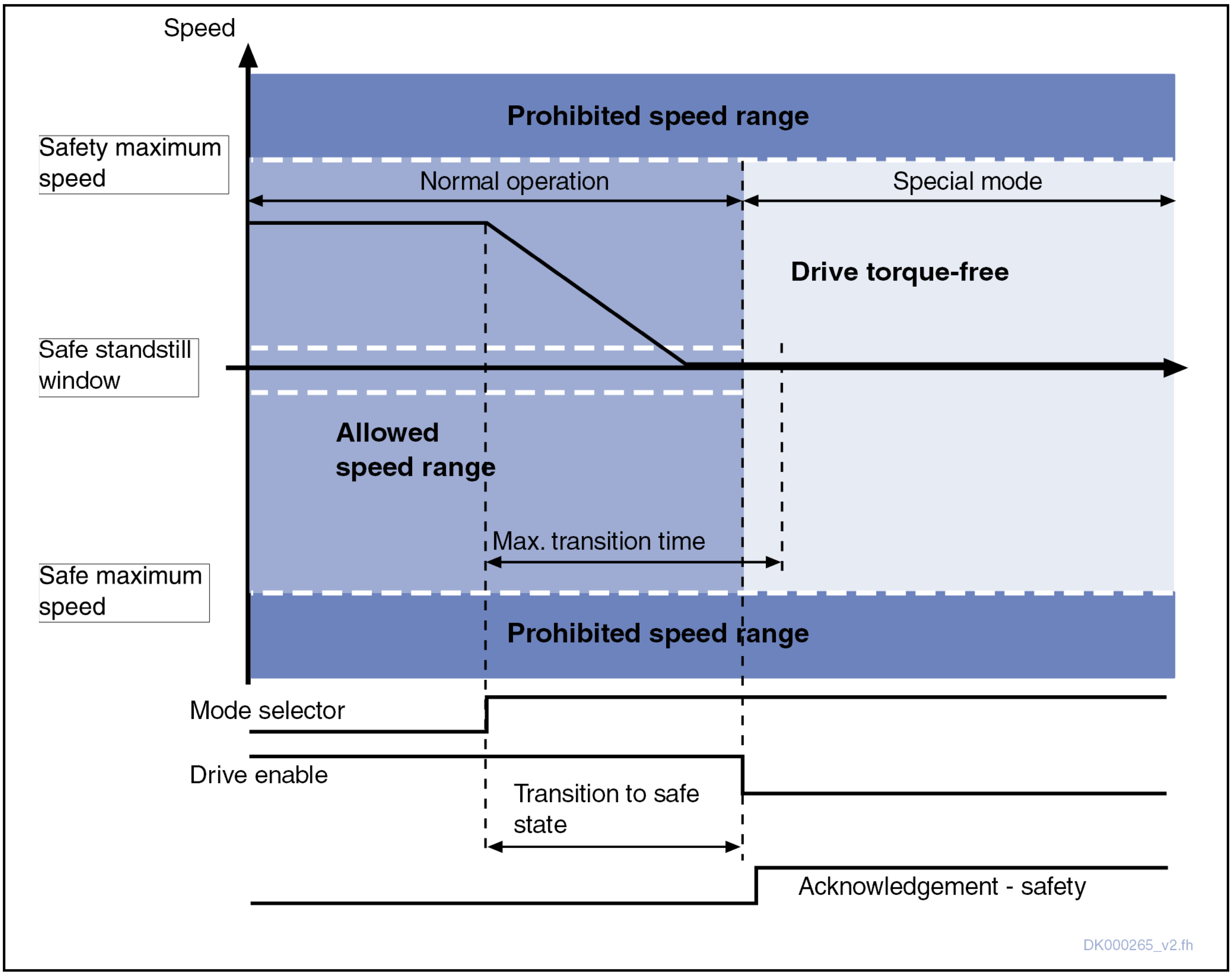


Fig. 5-8: NC-controlled transition to "Safe stop 1" from normal operation, with drive enable removed

Via bit 11 (NC-Ready) in "P-0-3212, Safety technology control word, channel 1", the control unit can signal to the drive that the adjustment of the command value system has been completed. By this signal the control unit can reduce the transition time. The bit has to be reset when the selected safety technology operating status is active or after some constant time which depends on the application.

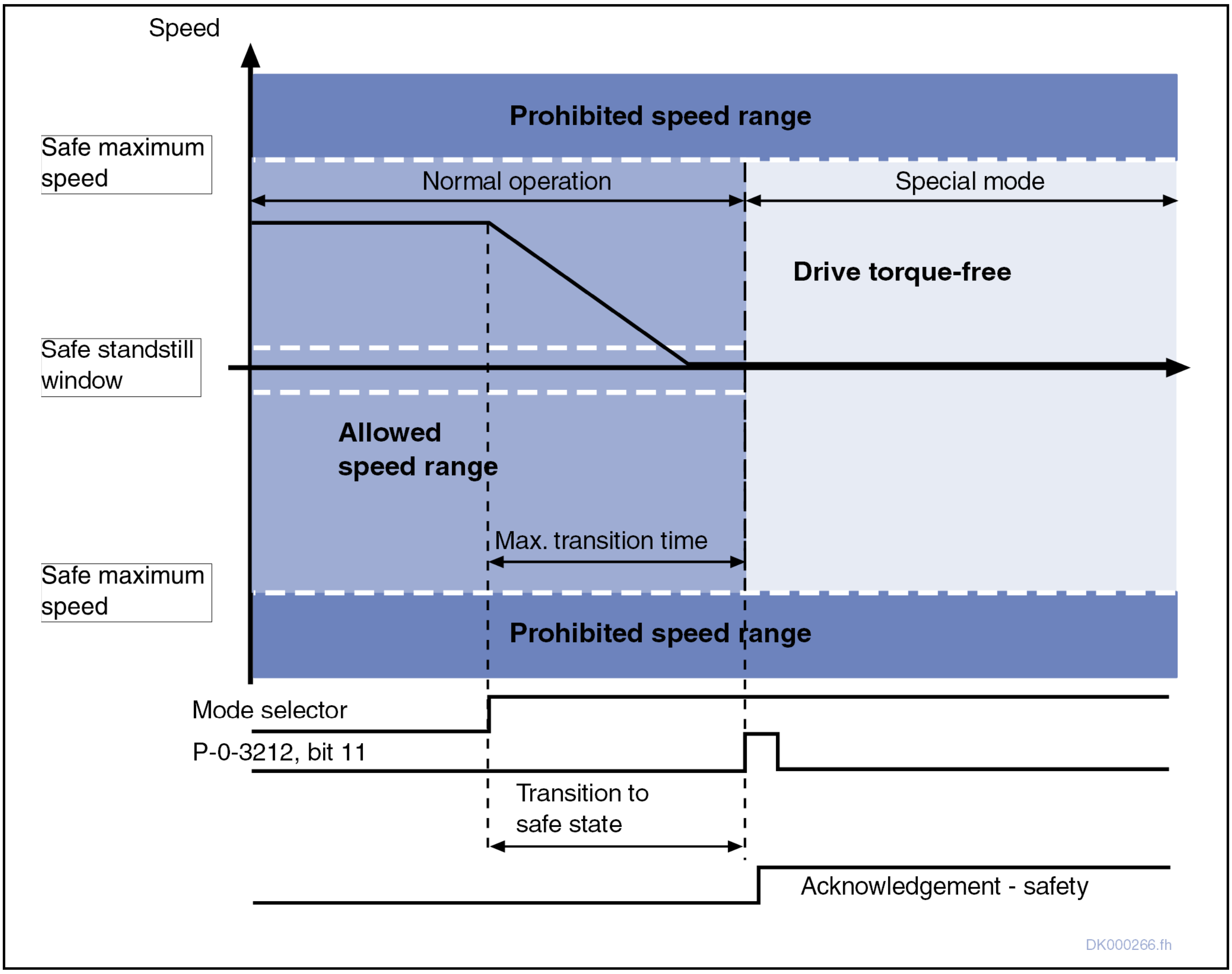


Fig. 5-9: NC-controlled transition from normal operation to "Safe stop 1" with "NC-Ready" bit

Functional principle of integrated safety technology

Selected safety technology operating status	**Safety technology operation mode transitions**	
	NC-controlled	**Drive-controlled**
Safety function "Safe stop 1", "Safe stop 1 (Emergency stop)"	NC-controlled stopping process, - NC removes drive enable, - When t = P-0-3220 or P-0-3225 or P-0-3212/"NC-Ready" bit = 1 and actual velocity < P-0-3233 the safety function "Safe stop 1" or "Safe stop 1 (Emergency stop)" is activated	Drive-controlled stopping process is initiated according to P-0-0119, bit 0...3; at end of stopping process, drive enable is removed - As soon as actual velocity < P-0-3233 the safety function "Safe stop 1" or "Safe stop 1 (Emergency stop)" is activated even if t < P-0-3220 or P-0-3225
Safety function "Safe stop 2"	NC-controlled stopping process - When t = P-0-3220 or P-0-3225 or no drive enable or P-0-3212/"NC-Ready" bit = 1 and actual velocity < P-0-3233 the safety function "Safe stop 2" is activated	Drive-controlled stopping process by means of internally activated "Drive Halt", - As soon as actual velocity < P-0-3233 the safety function "Safe stop 2" is activated, even if t < P-0-3220 or P-0-3225
Special mode "Safe motion"	NC-controlled transition - When t = P-0-3220 or P-0-3225 or no drive enable or P-0-3212/"NC-Ready" bit = 1 the special mode "Safe motion" is activated	NC-controlled operation mode transition is carried out

Tab. 5-1: Actions during the transitions between safety operating states

5.3 Interfaces for selection and acknowledgment

5.3.1 General information

General information

As a basic principle, safety-relevant selection and acknowledgment takes place via two channels; the firmware supports the following possibilities:

- Digital I/Os
- Digital I/Os and master communication
- PROFIsafe

Overview of interfaces

The safety technology operating states can be selected and acknowledged via the following interfaces (via two channels):

- Digital I/Os (channel 1 and channel 2)
- Digital I/Os (channel 2) and master communication (channel 1)
- PROFIsafe (channel 1 and channel 2)

  Note: With PORFIsafe, I/O evaluation does not take place, except for the reference cam!

☞ The available safety functions are independent of the interface used.

Connection system

The interfaces are connected via different terminal connectors (plug-in connectors):

- X41 on optional safety technology module: D-Sub, 9-pin
- X31 on control section: Phoenix connector
- X10 on digital I/O extension: D-Sub, 25-pin
- For master communication
  - SERCOS: Fiber optic cable connections at X20 / X21
  - PROFIBUS: D-Sub, 9-pin at X30

☞ For a drive controller with PROFIBUS master communication, make sure not to confound the 9-pin D-Sub connectors for master communication and the ones for the optional safety technology module!

5.3.2 Safety technology I/O

Brief description

According to the available dual-channel inputs, configurable combinations of safety functions can be selected via two channels via digital I/Os (N/C-N/O combination) on the optional safety technology module (X41) and the control section (X31 / X32 and digital I/O extension).

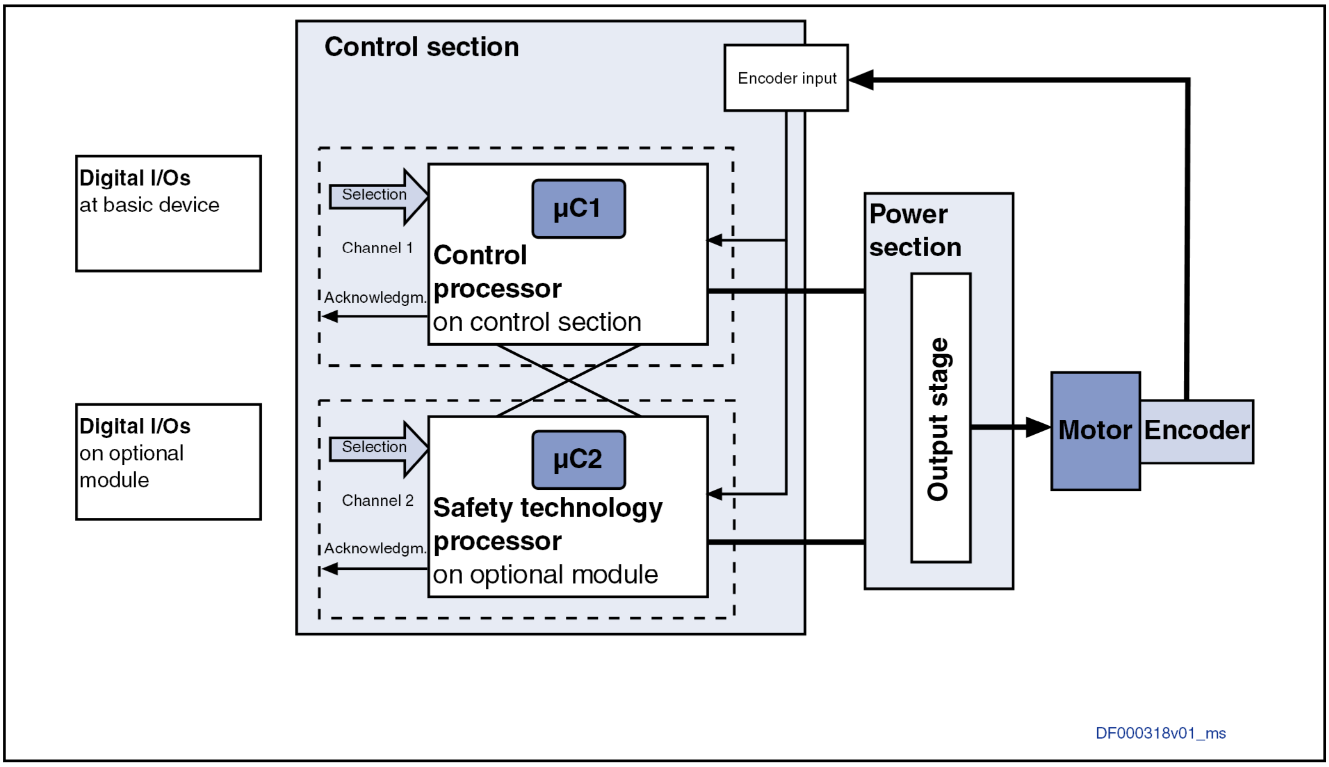


Fig. 5-10: Control via digital I/Os for channel 2 (X41) and channel 1 (X31 / X32 and digital I/O extension) directly at the drive

Features The digital inputs/outputs used for selection and acknowledgment have the following features:

- All I/Os are symbolically named "I1" to "I4", "I1n" to "I4n", "O10", "I10", "IO10n", "IO20" and "IO30".
- The freely configurable digital inputs/outputs (24 V) for channel 1 can be realized in the following way:
  - Using digital I/Os at the control section of the single-axis device (e.g. CSH01.1) at terminal connector X31 / X32
  - Using digital I/Os at the control section of the double-axis device (CDB01.1) at terminal connector X31 / X32 / X33 / X34
  - Using digital I/Os at an I/O extension (MD1) at terminal connector X10
- The digital inputs/outputs (24 V) for channel 2 are situated on the optional safety technology module ("S2") at terminal connector X41.

Pertinent parameters The following parameters are used in conjunction with the function:

- P-0-0300, Digital I/Os, assignment list
- P-0-0301, Digital I/Os, bit numbers
- P-0-0302, Digital I/Os, direction
- P-0-0303, Digital I/Os, status display
- P-0-0304, Digital I/Os, outputs
- P-0-0681, Assignment IDN -> parallel output 1
- P-0-0682, Assignment parallel input 1 -> IDN
- P-0-3210, Safety technology configuration
- P-0-3211, Safety technology I/O configuration list, channel 2

- P-0-3212, Safety technology control word, channel 1
- P-0-3213, Safety technology operating status
- P-0-3214, Safety technology status word, channel 1
- P-0-3215, Selected safety technology operating status
- P-0-3216, Active safety technology signals
- P-0-3217, I/O status channel 2 (optional safety technology module)

Configuring the I/Os

The digital I/Os of the drive controller which are used have to be accordingly configured during safety technology commissioning:

- Digital I/Os on the control section or an I/O extension (channel 1) have to be configured - like all other digital I/Os in the drive - via the following parameters:
  - P-0-0300, 0300, Digital I/Os, assignment list
  - "P-0-0301, Digital I/Os, bit numbers" and "P-0-0302, Digital I/Os, direction" or
  - "P-0-0681, Assignment IDN -> parallel output 1" and "P-0-0682, Assignment parallel input 1 -> IDN"

See also functional description of firmware "Digital inputs/outputs"

- The digital I/Os situated on the optional safety technology module have to be configured by means of "P-0-3211, Safety technology I/O configuration list, channel 2".

☞ To simplify commissioning, the commissioning software IndraWorks provides a safety technology wizard.

Functional principle

The safety technology operating states can be selected and acknowledged via digital I/Os directly at the drive controller.

The figure below shows the pertinent parameters and the basic function:

Functional principle of integrated safety technology

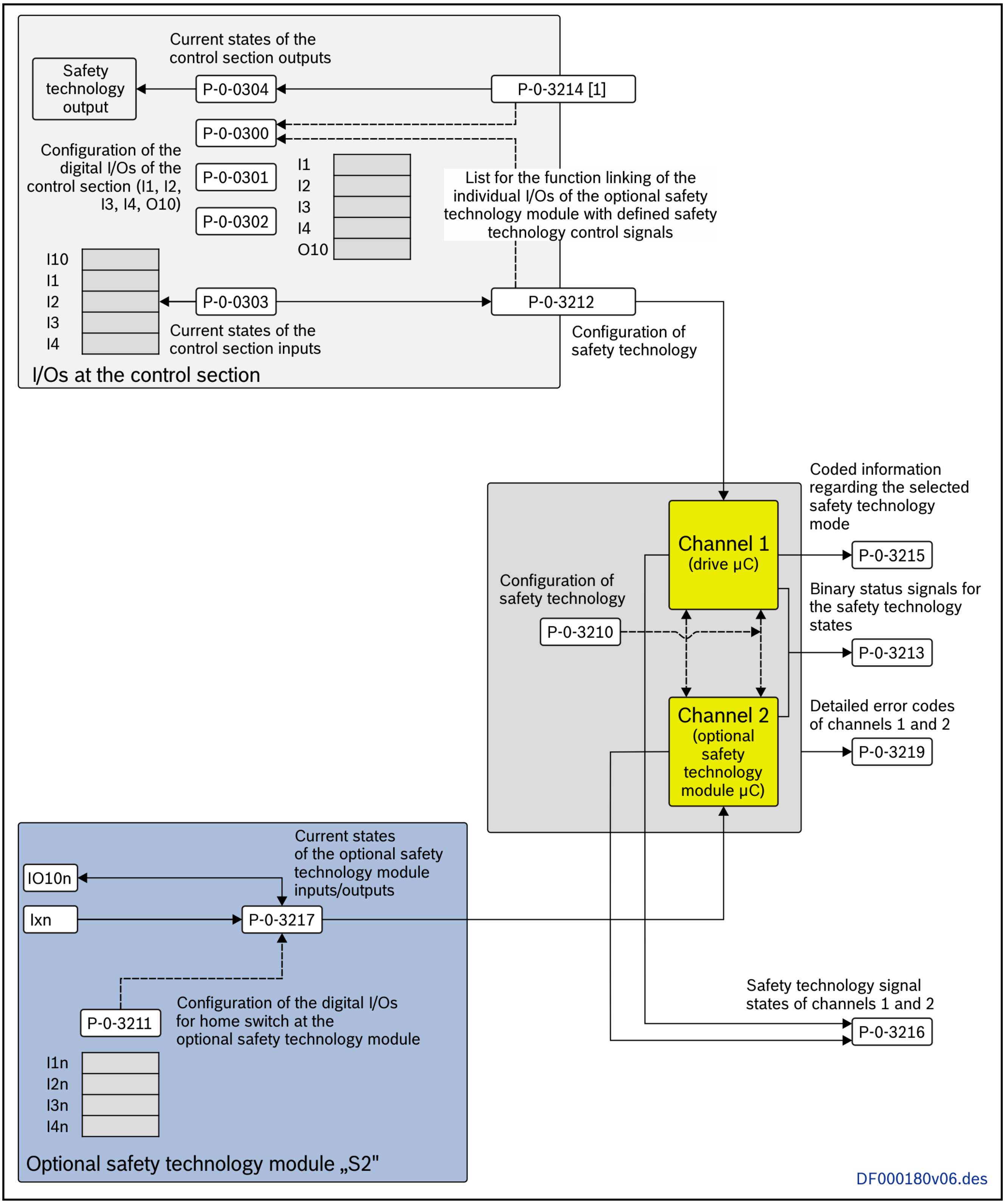

Safety technology output
Current states of the control section outputs
P-0-0304
P-0-3214 [1]
P-0-0300
Configuration of the digital I/Os of the control section (I1, I2, I3, I4, O10)
P-0-0301
P-0-0302
I1
I2
I3
I4
O10
List for the function linking of the individual I/Os of the optional safety technology module with defined safety technology control signals
I10
I1
I2
I3
I4
P-0-0303
P-0-3212
Current states of the control section inputs
Configuration of safety technology
I/Os at the control section
Coded information regarding the selected safety technology mode
Channel 1 (drive µC)
P-0-3215
Configuration of safety technology
Binary status signals for the safety technology states
P-0-3210
P-0-3213
Channel 2 (optional safety technology module µC)
Detailed error codes of channels 1 and 2
P-0-3219
Current states of the optional safety technology module inputs/outputs
IO10n
Ixn
P-0-3217
Configuration of the digital I/Os for home switch at the optional safety technology module
P-0-3211
Safety technology signal states of channels 1 and 2
P-0-3216
I1n
I2n
I3n
I4n
Optional safety technology module „S2"
DF000180v06.des

Fig. 5-11: Communication via digital I/Os

The figure below illustrates the selection of operating states via 24 V inputs at the drive controller.

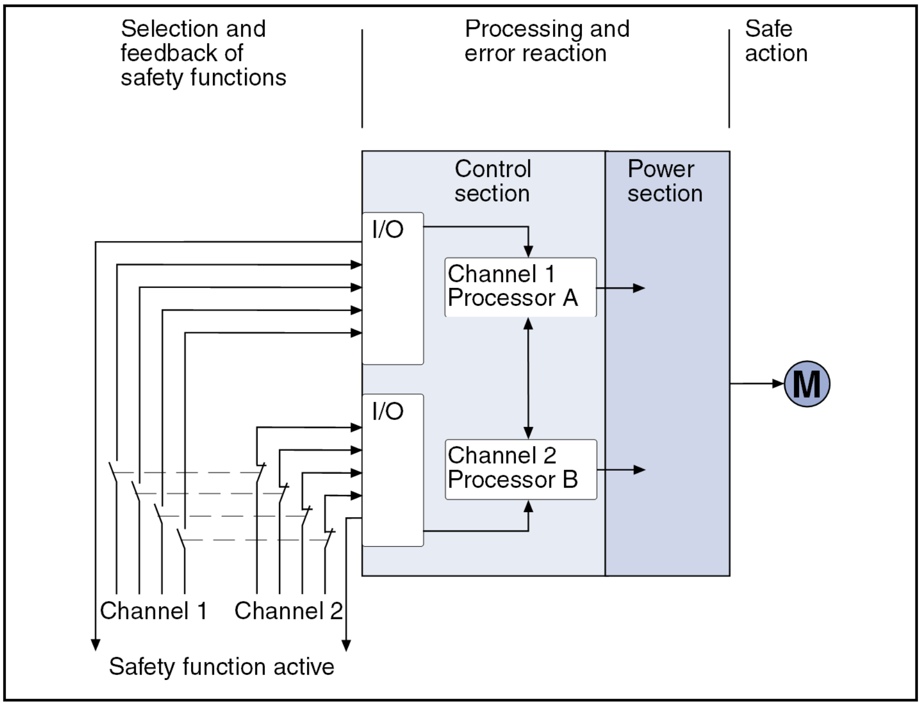


Fig. 5-12: Direct selection of both channels at the drive controller

5.3.3 "Safe Motion" in conjunction with a master communication

Brief description

According to the available dual-channel inputs, configurable combinations of safety functions can be selected via two channels via digital I/Os (N/C-N/O combination) on the optional safety technology module (X41) and the master communication (e.g. SERCOS, PROFIBUS).

Functional principle of integrated safety technology

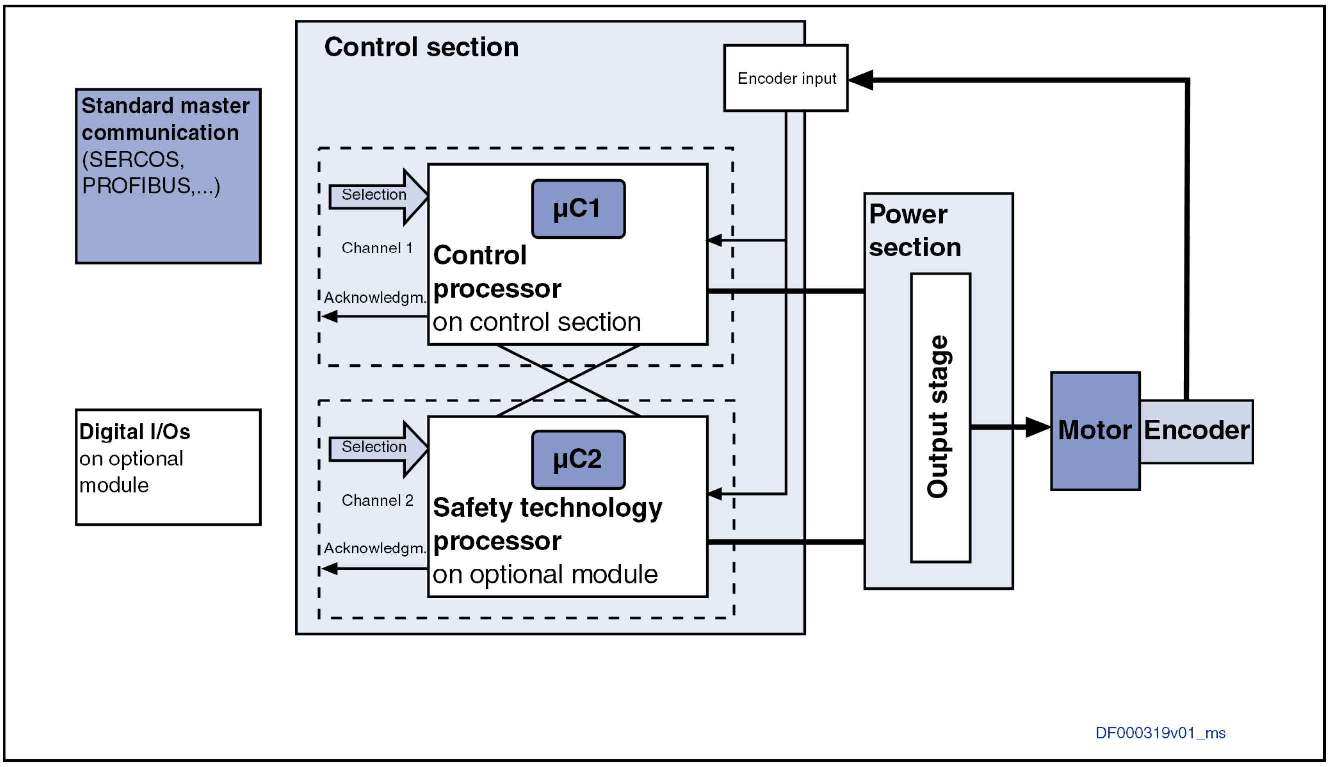

Control section
Encoder input
Standard master communication (SERCOS, PROFIBUS,...)
Selection
Channel 1
Acknowledgm.
µC1
Control processor on control section
Power section
Output stage
Motor
Encoder
Digital I/Os on optional module
Selection
Channel 2
Acknowledgm.
µC2
Safety technology processor on optional module
DF000319v01_ms

Fig. 5-13: Control via digital I/Os for channel 2 (X41) and master communication channel 1 directly at the drive

Features

The inputs/outputs used for selection and acknowledgment have the following features:

- All I/Os are symbolically named "I1" to "I4", "I1n" to "I4n", "O10", "I10", "IO10n", "IO20" and "IO30".
- The inputs/outputs for channel 1 can be realized using digital I/Os of a control unit which are transmitted to the drive via the non-safe standard field bus or SERCOS interface.
- The digital inputs/outputs (24 V) for channel 2 are situated on the optional safety technology module ("S2") at terminal connector X41.

Pertinent parameters

The following parameters are used for communication via "Safe Motion" and master communication:

- P-0-3210, Safety technology configuration
- P-0-3211, Safety technology I/O configuration list, channel 2
- P-0-3212, Safety technology control word, channel 1
- P-0-3213, Safety technology operating status
- P-0-3214, Safety technology status word, channel 1
- P-0-3215, Selected safety technology operating status
- P-0-3216, Active safety technology signals
- P-0-3217, I/O status channel 2 (optional safety technology module)

Configuring the I/Os

The digital I/Os of the drive controller and of the control unit which are used have to be accordingly configured during safety technology commissioning:

- Digital inputs of the control unit (channel 1) have to be transmitted to the drive via the master communication. For this purpose, "P-0-3212, Safety technology control word, channel 1" has to be configured in the cyclic

command value channel of SERCOS (cf. S-0-0024) or the field bus (cf. P-0-4081).

- **Digital outputs** of the control unit (channel 1) have to be transmitted from the drive to the control unit via the master communication. For this purpose, "P-0-3214, Safety technology status word, channel 1" has to be configured in the cyclic **actual value channel** of SERCOS (cf. S-0-0016) or the field bus (cf. P-0-4080).

See also Functional Description of firmware "Master communication"

- The digital inputs situated on the optional safety technology module have to be configured by means of "P-0-3211, Safety technology I/O configuration list, channel 2".

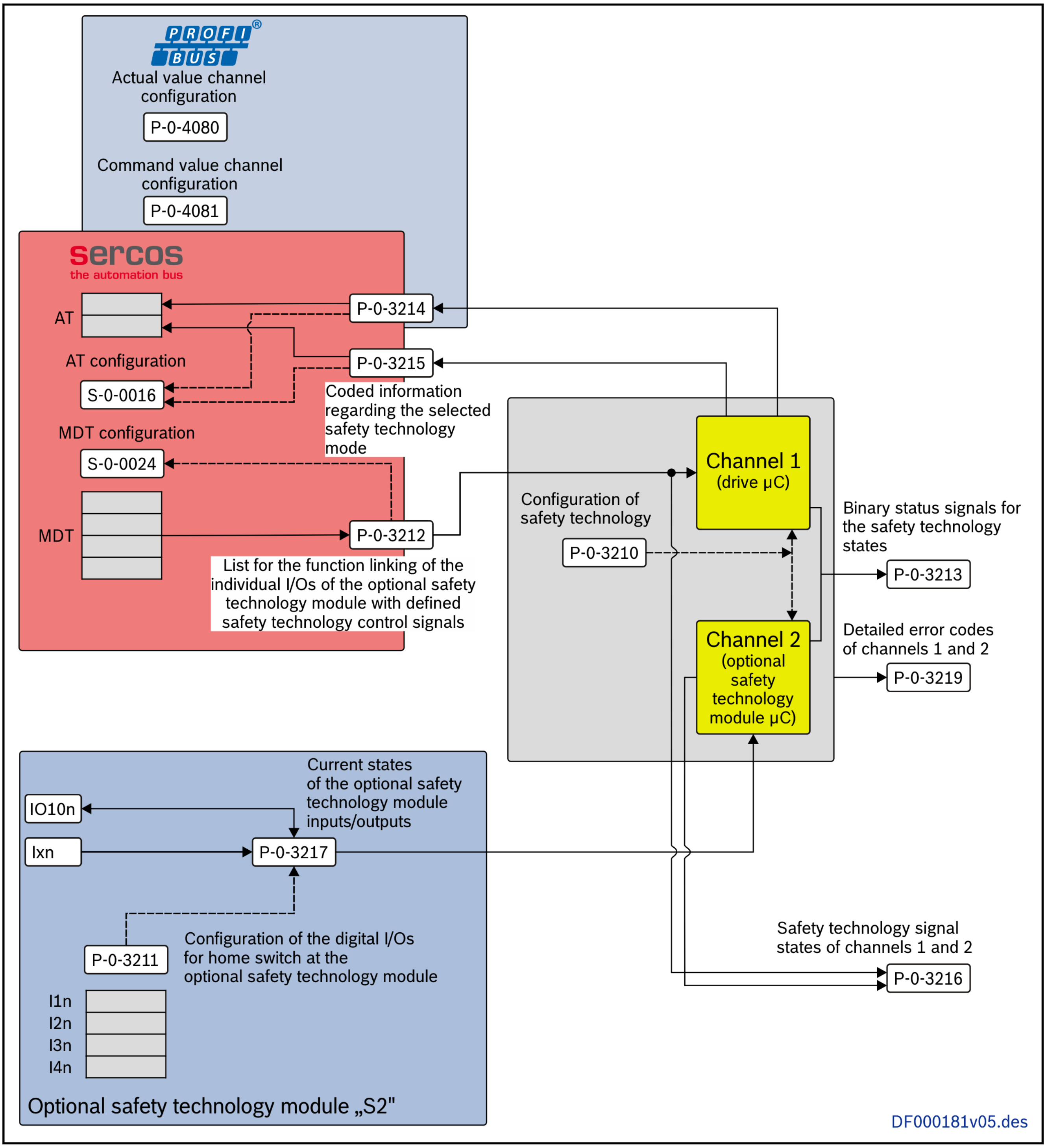
☞ To simplify commissioning, the commissioning software IndraWorks provides a safety technology wizard.

Functional principle

The safety technology operating states are selected and acknowledged via digital I/Os of the optional safety technology module and digital I/Os of the control unit which are transmitted to the drive via the master communication.

The figure below shows the pertinent parameters and the basic function:

Functional principle of integrated safety technology


PROFIBUS
Actual value channel configuration
P-0-4080
Command value channel configuration
P-0-4081
sercos
the automation bus
AT
P-0-3214
P-0-3215
AT configuration
S-0-0016
Coded information regarding the selected safety technology mode
MDT configuration
S-0-0024
MDT
P-0-3212
List for the function linking of the individual I/Os of the optional safety technology module with defined safety technology control signals
Configuration of safety technology
P-0-3210
Channel 1
(drive µC)
Channel 2
(optional safety technology module µC)
Binary status signals for the safety technology states
P-0-3213
Detailed error codes of channels 1 and 2
P-0-3219
Current states of the optional safety technology module inputs/outputs
IO10n
Ixn
P-0-3217
P-0-3211
Configuration of the digital I/Os for home switch at the optional safety technology module
I1n
I2n
I3n
I4n
Optional safety technology module „S2"
Safety technology signal states of channels 1 and 2
P-0-3216
DF000181v05.des

->: Channel 1 is indirectly activated via the master communication interface of the control unit (CNC; PLC)

->: Channel 2 is directly activated via the input interface of the drive controller

Fig. 5-14: Communication via digital I/Os and master communication

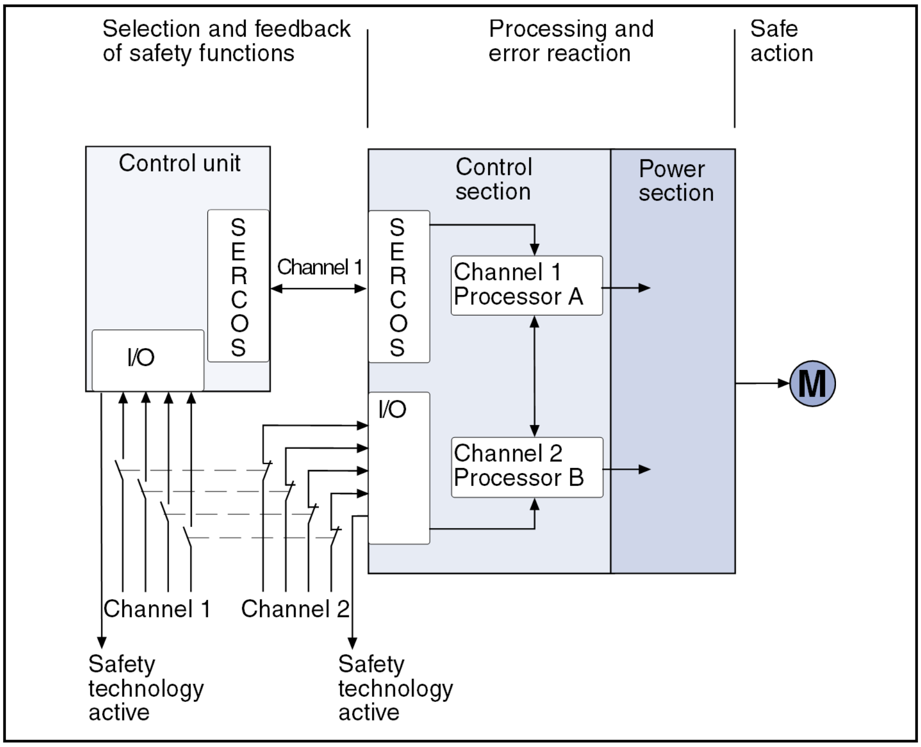


Fig. 5-15: Direct and indirect selection of the channels at the drive controller

5.3.4 PROFIsafe

Brief description

The safety functions can also be selected via a safe channel (PROFIsafe). For this purpose, the PROFIBUS standard protocol was extended by a safe protocol so that, apart from PROFIBUS standard communication, operation mode selection and acknowledgment for integrated safety technology (channel 1 and channel 2) can take place.

Functional principle of integrated safety technology

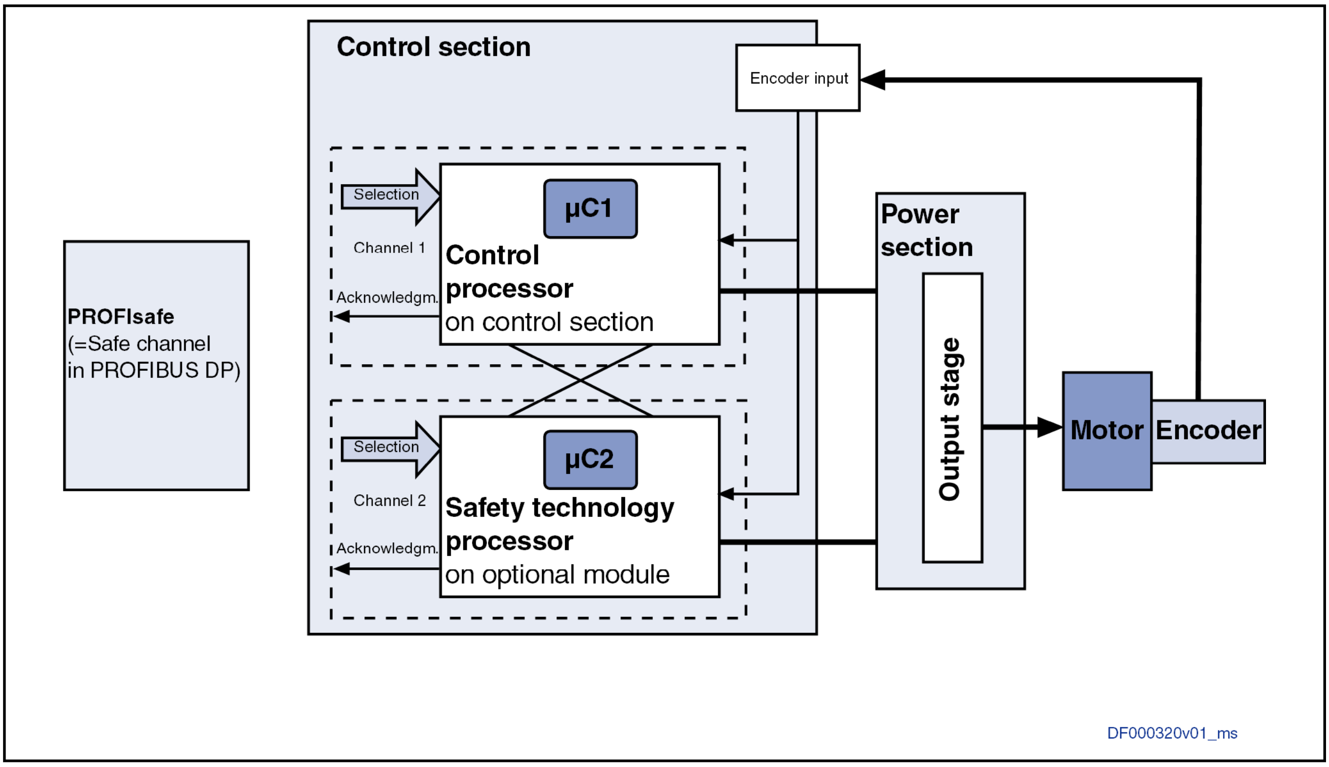


Fig. 5-16: Control via safe channel "PROFIsafe" in PROFIBUS DP

Pertinent parameters

The following parameters are used in conjunction with PROFIsafe:

- P-0-3210, Safety technology configuration
- P-0-3211, Safety technology I/O configuration list, channel 2
- P-0-3212, Safety technology control word, channel 1
- P-0-3213, Safety technology operating status
- P-0-3214, Safety technology status word, channel 1
- P-0-3215, Selected safety technology operating status
- P-0-3216, Active safety technology signals
- P-0-3217, I/O status channel 2 (optional safety technology module)
- P-0-3290, PROFIsafe: F_Destination_Address
- P-0-3291, PROFIsafe: F_Source_Address
- P-0-3292, PROFIsafe: F_Parameters

Configuring PROFIsafe

When using PROFIsafe, there are the following functional differences compared to the function "Safety technology I/O":

- No dynamization of the safe control bits.
- Only the home switch can be defined as input on the optional safety technology module, all other signals are preset by PROFIsafe via the safe control bits.

Configuring the digital I/Os in the drive

With PROFIsafe it is not necessary to configure any I/Os in the drive controller, because channel 1 and channel 2 are transmitted in a safe PROFIBUS channel (PROFIsafe). Only when a reference cam is required for safe homing procedure, the cam has to be configured via "P-0-3211, Safety technology I/O configuration list, channel 2".

Activating PROFIsafe

To use the safe channel in PROFIBUS (=PROFIsafe), make the following parameter setting in the drive:

- "P-0-3290, PROFIsafe: F_Destination_Address": Enter target address under which the axis is administrated in the safety PLC.

☞ P-0-3290="0" deactivates PROFIsafe!

- "P-0-3291, PROFIsafe: F_Source_Address": Enter the source address stored in the safety PLC.
- The parameter "P-0-3292, PROFIsafe: F_Parameters" contains all PROFIsafe parameters that are set via the PLC configuration and is used for display.

Configuring PROFIBUS

Configuring the drive requires a so-called device data sheet:

Firmware version	Device data sheet
MPx-07VRS	RX060107.GSD
MPx-08VRS	RX080107.GSD

Tab. 5-2: Device data sheets

See also Functional Description of firmware "PROFIBUS-DP"

☞ All configuration programs supporting at least GSD revision 04 only allow such modules for the slot which may be configured in these programs.

Functional principle

Control and feedback of the integrated safety technology via PROFIsafe takes place via the F-modules of PROFIBUS (=safe data containers within the PROFIBUS protocol).

The figure below shows the pertinent parameters of PROFIsafe communication and the basic function:

Functional principle of integrated safety technology

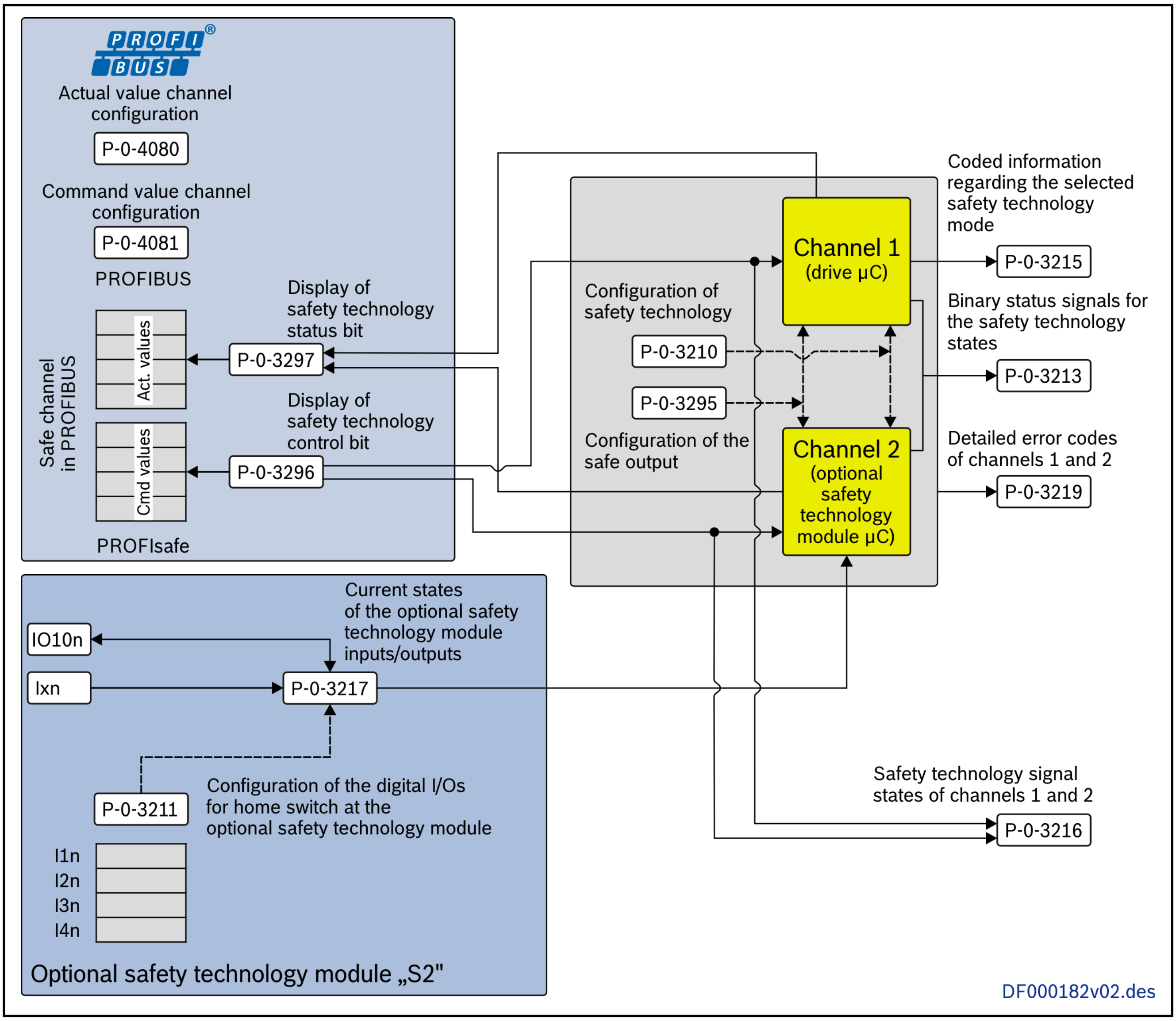

PROFI BUS
Actual value channel configuration
P-0-4080
Command value channel configuration
P-0-4081
PROFIBUS
Safe channel in PROFIBUS
Act. values
Cmd values
Display of safety technology status bit
P-0-3297
Display of safety technology control bit
P-0-3296
PROFIsafe
Configuration of safety technology
P-0-3210
P-0-3295
Configuration of the safe output
Channel 1 (drive µC)
Channel 2 (optional safety technology module µC)
Coded information regarding the selected safety technology mode
P-0-3215
Binary status signals for the safety technology states
P-0-3213
Detailed error codes of channels 1 and 2
P-0-3219
Current states of the optional safety technology module inputs/outputs
IO10n
Ixn
P-0-3217
P-0-3211
Configuration of the digital I/Os for home switch at the optional safety technology module
I1n
I2n
I3n
I4n
Optional safety technology module „S2"
Safety technology signal states of channels 1 and 2
P-0-3216
DF000182v02.des

Fig. 5-17: Communication via safe channel "PROFIsafe" in PROFIBUS DP

Command value channel for selecting safety technology operation modes

In the command value channel, a 16-bit control word is transmitted from master to slave (drive) which is divided into 2 control bytes:

- F control byte 1: Low byte (bit 0...7)
- F control byte 2: High byte (bit 8...15)

☞ At present, only the lowest 8 bits of the 16-bit control word (bit 0...7 in low byte) are used.

Bit	Designation/function
0	**Mode selector** (MS) 0 = Select safe operation (MS) 1 = Deselect safe operation (MS)
1	**SS1 (Emergency stop) switch** (ES) 0 = Select SS1 (Emergency stop) switch (ES) 1 = Deselect SS1 (Emergency stop) switch (ES)
2	**Enabling control** (EC) 0 = Select enabling control (EC) 1 = Deselect enabling control (EC)
3	**Safety switch 1** (S1) 0 = Select safety switch 1 (S1) 1 = Deselect safety switch 1 (S1)
4	**Safety switch 2** (S2) 0 = Select safety switch 2 (S2) 1 = Deselect safety switch 2 (S2)
7	**Control of safe output** 0 = Output not active (safe state) 1 = Output active
15-5	Reserved

Tab. 5-3: Safety technology control bits in PROFIsafe (channels 1+2)

☞ The control bits received by the drive are displayed in "P-0-3212, Safety technology control word, channel 1".

Actual value channel for acknowledging safety

In the actual value channel, a 16-bit status word is transmitted from slave (drive) to master which is divided into 2 control bytes:

- F status byte 1: Low byte (bit 0...7)
- F status byte 2: High byte (bit 8...15)

☞ At present, only the lowest 8 bits of the 16-bit control word (bit 0...7 in low byte) are used.

Bit	Designation/function
0	**Safety technology status output of controller** 0 = Drive is in non-safe state (default value!) 1 = Drive has established safety
1	**Safe drive interlock status** (MPx-06VRS and below) **Safe stop 1 (Emergency stop)** (MPx-07VRS and above) **0**: Not active **1**: Active

Bit	Designation/function
2 (MPx08V12 and above)	**Safety technology error status** **0:** No safety technology error **1:** Safety technology error
4	**Safe input 1 status** 0 = Input not active (safe state) 1 = Input active
5	**Safe input 2 status** 0 = Input not active (safe state) 1 = Input active
6	**Safe input 3 status** 0 = Input not active (safe state) 1 = Input active
7	**Safe input 4 status** 0 = Input not active (safe state) 1 = Input active
15-1	Reserved

Tab. 5-4: Safety technology status bits in PROFIsafe (channels 1+2)

☞ The safety technology status acknowledged by the drive is displayed in "P-0-3214, Safety technology status word, channel 1".

Module 10: F-module I/O

☞ In the following paragraphs, the data transmitted from master to slave are described as "output data" and the data from slave to master as "input data".

With the configuration "module 10: F-module I/O", the telegram structure is as follows:

Byte no.	User data	PROFIsafe protocol
O (n)	F control byte 1	F Process Data
O (n+1)	F control byte 2	(User data)
O (n+2)		Control byte
O (n+3)		Consecutive Number
O (n+4)		CRC2 (16 bit)
O (n+5)		

Tab. 5-5: Output telegram structure with "module 10: F-module I/O", 6 bytes telegram length

Byte no.	User data	PROFIsafe protocol
I (n)	F status byte 1	F Process Data
I (n+1)	F status byte 2	(User data)
I (n+2)		Status byte

Byte no.	User data	PROFIsafe protocol
I (n+3)		Consecutive Number
I (n+4)		CRC2 (16 bit)
I (n+5)		

Tab. 5-6: Input telegram structure with "module 10: F-module I/O", 6 bytes telegram length

5.4 Feedback of safety technology operating states to the peripherals

5.4.1 General information

Safety-relevant feedback is basically transmitted via two channels, whereas feedback for diagnostic purposes can be transmitted via one channel.

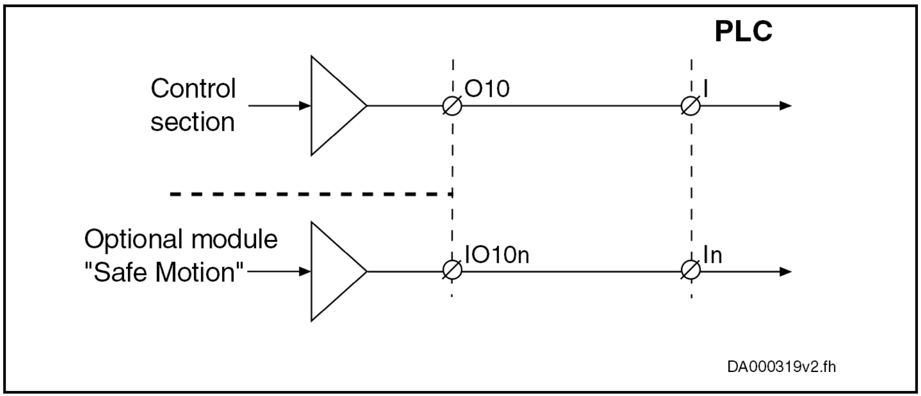
The integrated safety technology of IndraDrive provides the following variants which have to be selected and configured or wired according to the application:

- Safe feedback to a safety PLC
- Safe control of a door locking device (not with PROFIsafe)

☞ For feedback of the second channel, a 24 V driver or a relay contact is available on the optional safety technology module ("S2") (one relay point is internally assigned to 0 V).

Chapter "Interfaces for selection and acknowledgment" describes the interface-dependent differences regarding the configuration and the functions that can be used!

5.4.2 Safe feedback via digital I/Os to a safety PLC



Channel 1: O10 (control section)
Channel 2: IO10n (O10, 24 V driver is active on optional module "Safe Motion")

Fig. 5-18: Safe status message to a safety PLC

☞ The two outputs O10 and IO10n work in inverted form! For safe feedback to a safety PLC, this feedback has to be evaluated in inverted form, too!

Drive status	O10	IO10n
Drive safe	High	Low
Drive not safe	Low	High
Parameter mode (diagnostic/ acknowledgment master)	Low	High
Parameter mode (diagnostic/ acknowledgment slave)	Last state in phase 4	Last state in phase 4

Tab. 5-7: Output signals for controlling a PLC

5.4.3 Safe door locking device via digital I/Os

☞ With PROFIsafe, dynamization of acknowledgment does not take place and there are no door locking functions!

Apart from the feedback to a safety PLC, it is possible to directly control a door locking device in a safe way. For this purpose, the drive has to be configured as "diagnostic master" (cf. "P-0-3210, Safety technology configuration").

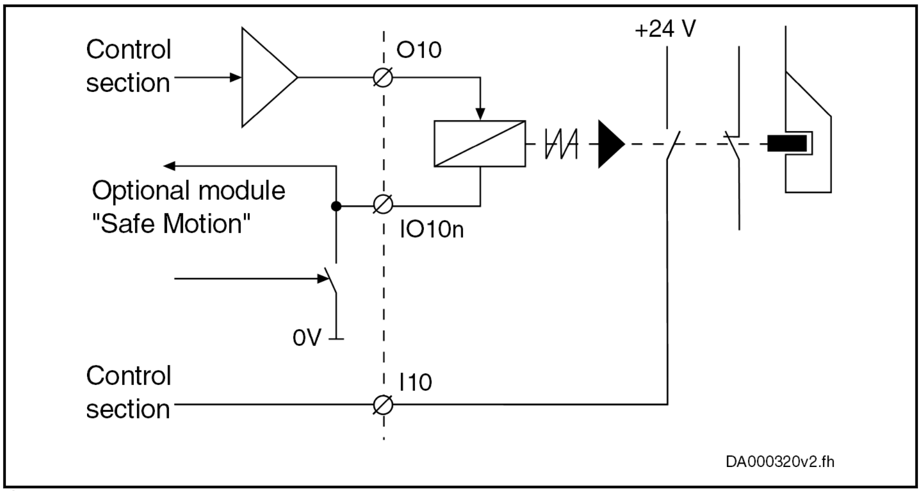
⚠ DANGER **Lethal injury caused by axes / spindles coasting to stop in a torque-free way due to an error!**

⇒ Provide an interlocking guard with guard locking that only allows unlocking the guard when standstill has been reached (see EN 1088).

If the guard is unlocked without standstill having been reached, coasting to stop in a torque-free way has to be prevented by additional measures [e.g., by using a motor holding brake (to be used only in the case of an emergency), an emergency braking resistor or a service brake], or the guard has to be positioned in such a way that spindles / axes have stopped before they can be reached (see EN 999).

The safe state is signaled via the safety technology status output. This output is a dual-channel output (O10, IO10n). The output O10 can be output at the basic device or at the control unit (P-0-3214 transmitted by the drive via master communication). The output IO10n switches internally to 0 V.

For monitoring the interlocking device, a second input (I10) has to be used at the basic device or at a control unit. This input has to be transmitted to the drive via the master communication.



Channel 1: O10, I10 (control section or P-0-3214 via master communication)

Channel 2: IO10n (24 V input and driver for relay contact are active on optional module "Safe Motion")

Fig. 5-19: Control of a door locking device

Drive status	O10	IO10n
Drive safe	High	Low
Drive not safe	Low	High-resistance
Parameter mode	Last state in phase 4	Last state in phase 4

Tab. 5-8: Output signals for controlling a safety door

☞ In the case of an encoder error in the drive, it is impossible to signal a safe state. If the safety technology status (acknowledgment signal of integrated safety technology) is used for direct control of a safety door, the manual safety door unlocking device has to be activated for the corresponding axis (see "P-0-3218, C3700 Manually unlocking the safety door").

⚠ DANGER **Lethal injury caused by axes / spindles coasting to stop in a torque-free way due to an error!**

⇒ When the safety door is manually unlocked, it is not ensured that the faulty axis is in standstill. This is why you have to wait until the axis has coasted to stop and come to standstill before accessing the protection zone.

5.4.4 Setting up a safety zone

General information

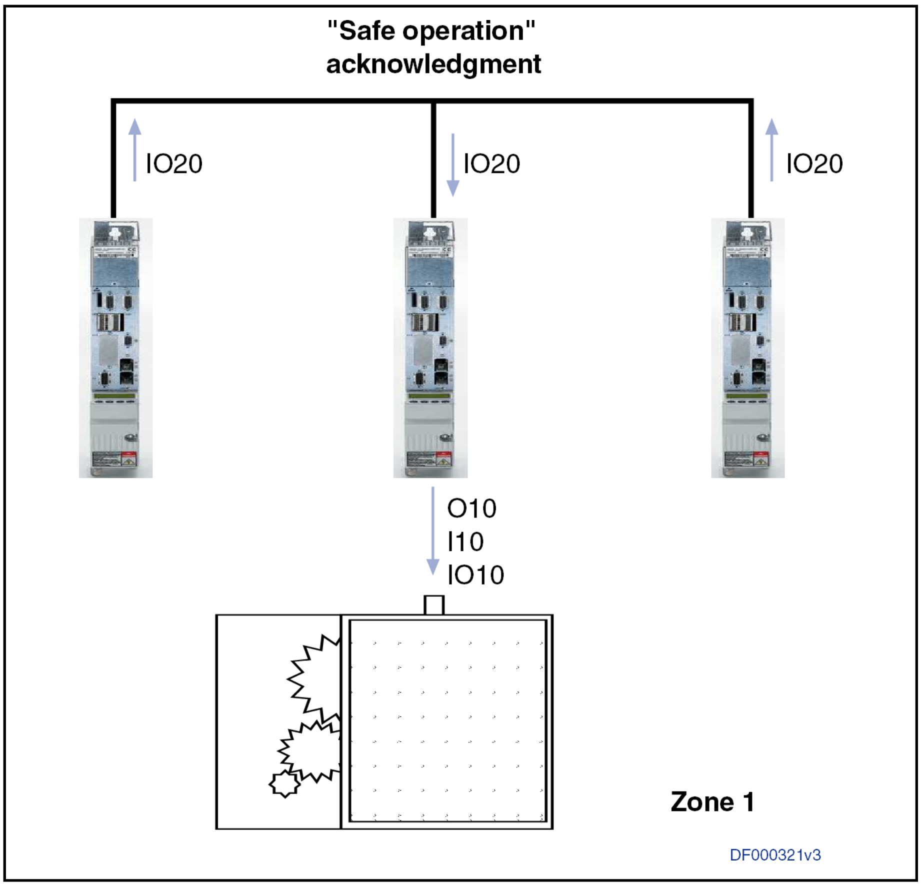
If there are several axes in a danger zone, it is useful to combine them in a safety zone. For this purpose, one drive in the safety zone is configured as "diagnostic master" and all others as "diagnostic slaves" (cf. "P-0-3210, Safety technology configuration").

☞ One diagnostic master has to be available for each safety zone!

Functional principle

All axes of a danger zone (=safety zone) have to be interconnected via IO20 via bus.

The diagnostic master addresses the diagnostic slaves via IO20 and expects the feedback/acknowledgment "safe operation" in order to enable the safety door.



Channel 1: O10, I10 (control section or master communication)

Channel 2: IO10n (24 V input and driver for relay contact are active on optional module "Safe Motion")

Fig. 5-20: Safety zone with control of a door locking device

☞ Due to hardware restrictions, a maximum of 25 drives can be combined in a safety zone!

Notes on commissioning

All axes of a safety zone must have been completely configured for commissioning. In addition, safety technology must have been activated in all axes.

☞ If safety technology has not been activated in a diagnostic slave, the error "F3131 Error when checking acknowledgment signal" appears in the diagnostic master.

Diagnostic master

The so-called "diagnostic master" recognizes the "safe state" of its own drive and other drives which are interconnected via IO20.

All axes have to acknowledge having reached the safe state before the diagnostic master controls the common safety technology status output (e.g. for a door locking device).

☞ In the case of an encoder error in a drive, it is impossible to signal the safe state. If the safety technology status (acknowledgment signal of integrated safety technology) is used for direct control of a safety door, the manual safety door unlocking device has to be activated for the corresponding axis (see "P-0-3218, C3700 Manually unlocking the safety door").

⚠ DANGER **Lethal injury caused by axes / spindles coasting to stop in a torque-free way due to an error!**

⇒ When the safety door is manually unlocked, it is not ensured that the faulty axis is in standstill. This is why you have to wait until the axis has coasted to stop and come to standstill before accessing the protection zone.

Special case: ""SafeTorque Off" and "Safe Motion" in a safety zone"

When setting up safety zones, take the following special case into account:

- This application cannot recognize the state of an axis equipped with the optional module "Safe Torque Off".
- When the optional modules "SafeTorque Off" (option "L2") and "Safe Motion" (option "S2") are used in a common danger zone, the control of the magnet for the locking device has to be connected via the relay contact "STO Q"/"STO Q1" of the option "L2"!

5.4.5 Safe feedback via PROFIsafe to the safety PLC

General information

For diagnostic purposes, the transmitted F-data are displayed in the drive in the corresponding parameters. The figure below contains an overview of how the individual parameters interact:

Functional principle of integrated safety technology

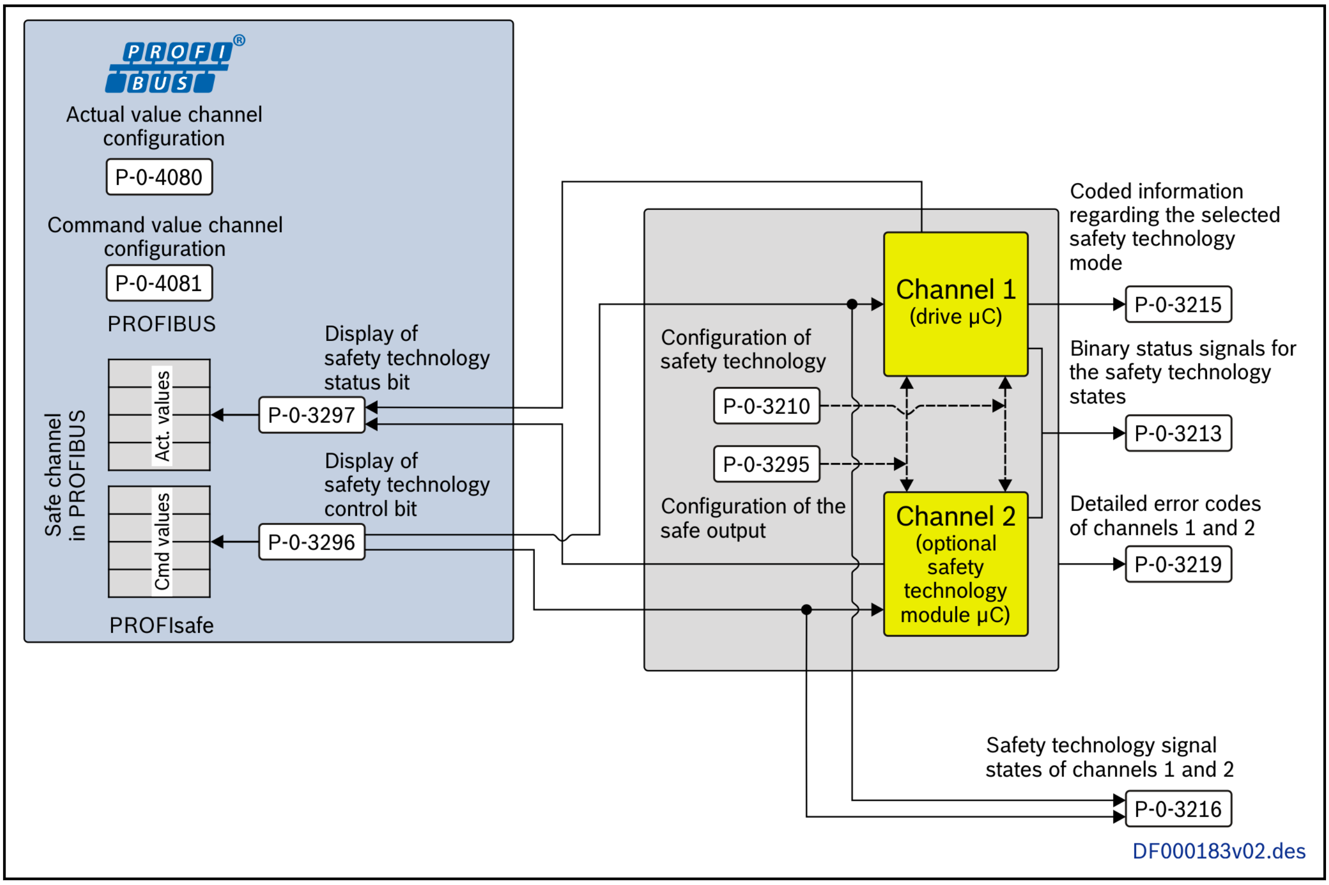

PROFI BUS
Actual value channel configuration
P-0-4080
Command value channel configuration
P-0-4081
PROFIBUS
Safe channel in PROFIBUS
Act. values
Cmd values
PROFIsafe
Display of safety technology status bit
P-0-3297
Display of safety technology control bit
P-0-3296
Configuration of safety technology
P-0-3210
P-0-3295
Configuration of the safe output
Channel 1 (drive µC)
Channel 2 (optional safety technology module µC)
Coded information regarding the selected safety technology mode
P-0-3215
Binary status signals for the safety technology states
P-0-3213
Detailed error codes of channels 1 and 2
P-0-3219
Safety technology signal states of channels 1 and 2
P-0-3216
DF000183v02.des

Fig. 5-21: Status parameters and diagnostic parameters with PROFIsafe

Control bits

The control bits of the two channels that are used can be read via the following diagnostic parameters / display parameters:

- "P-0-3216, Active safety technology signals": Displays the current states of the signals applied via "P-0-3214, Safety technology status word, channel 1"
- "P-0-3215, Selected safety technology operating status": Makes available a hexadecimal value that displays the selected safety technology operating status
- "P-0-3213, Safety technology operating status": Makes available binary status signals for online monitoring of the safety technology states

Status bits

The status bits of the two channels that are used can be read via the following diagnostic parameters / display parameters:

- "P-0-3214, Safety technology status word, channel 1": Makes available binary status signals of the safety technology functions of channel 1

5.5 Advanced settings

5.5.1 Scaling / axis mechanics

Motor-related scaling

For certain applications, it is necessary to set the safety threshold value parameters for velocity, acceleration and relative position in the motor-related format, independent of the drive scaling system. Such applications, for example, are the use of parameter set switching (load gear switching) or gear switching in parameter mode.

Features

The functionality "motor-related scaling" has the following features:

- It is **impossible** to use the safety function "Safely-monitored position" or "Safely-limited position" in conjunction with the "motor-related scaling".
- The safety parameters for velocity, acceleration and relative position have to be input in motor-related format.
- When user-defined scalings for position, velocity, acceleration and torque or force are used, the following parameterizations are **not allowed**:
  - Scaling factors unequal 1
  - Rotational position resolution unequal 360*10^n (n=1, 2, 3…)

Pertinent parameters

The following parameters are used in conjunction with motor-related scaling:

- S-0-0278, Maximum travel range
- P-0-0129, Internal position data format
- P-0-3210, Safety technology configuration
- P-0-3230, Monitoring window for safe stop 2
- P-0-3232, Standstill window for safe direction
- P-0-3233, Velocity threshold for safe standstill
- P-0-3234, Safe maximum speed
- P-0-3243, Safety-limited increment 1
- P-0-3244, Safely-limited speed 1
- P-0-3253, Safety-limited increment 2
- P-0-3254, Safely-limited speed 2
- P-0-3263, Safety-limited increment 3
- P-0-3264, Safely-limited speed 3
- P-0-3273, Safety-limited increment 4
- P-0-3274, Safely-limited speed 4
- P-0-3282, Safely-monitored deceleration

Functional principle

Motor-related scaling has to be activated by the corresponding setting in parameter "P-0-3210, Safety technology configuration". When this was done, the following safety parameters always have to be parameterized with relation to the motor shaft when safety technology is commissioned:

- **Velocity thresholds:**
  - P-0-3233, Velocity threshold for safe standstill
  - P-0-3234, Safe maximum speed
  - P-0-3244, Safely-limited speed 1
  - P-0-3254, Safely-limited speed 2
  - P-0-3264, Safely-limited speed 3
  - P-0-3274, Safely-limited speed 4
- **Acceleration thresholds**:
  - P-0-3282, Safely-monitored deceleration
- **Position thresholds (relative)**:
  - P-0-3229, Tolerance window for safe homing procedure

- P-0-3230, Monitoring window for safe stop 2
- P-0-3232, Standstill window for safe direction
- P-0-3243, Safely-limited increment 1
- P-0-3253, Safely-limited increment 2
- P-0-3263, Safely-limited increment 3
- P-0-3273, Safely-limited increment 4

☞ For general parameterization of the axis, make sure that the setting of "P-0-0129, Internal position data format" remains the same for all parameter sets or gear ratios which are used. Adjust "S-0-0278, Maximum travel range", if necessary.

In case "P-0-0129, Internal position data format" is changed with safety technology active, the error "F3140 Safety parameters validation error" or "F7040 Validation error parameterized - effective threshold" is generated.

Gear independence with safety technology encoder mounted on the load side

According to the application, it can be necessary to mount the encoder relevant to safety technology on the load side. This provides the advantage that the velocity and position information required for safety technology are detected directly where the dangerous movement occurs. If the power transmission between motor and load has a modifiable gear ratio (e.g. switchable gear), the signal detection and evaluation of the safety technology encoder mounted on the load side has to be independent of gear switching. Such independence can be achieved with the functionality "gear independence with safety technology encoder mounted on the load side".

Features

The functionality "gear independence with safety technology encoder mounted on the load side" has the following features:

- The axis has to have been scaled on the load side.
- The acceleration and velocity data have to have rotary scaling.
- The functionality **cannot** be used in conjunction with the safety function "Safe braking and holding system".
- The functionality **cannot** be used in conjunction with the safety function "Safely-monitored position" or the safety function "Safely-limited position".
- When user-defined scalings for position, velocity, acceleration and torque or force are used, the following parameterizations are **not allowed**:
  - Scaling factors unequal 1
  - Rotational position resolution unequal 360*10^n (n=1, 2, 3…)

Pertinent parameters

The following parameters are used in conjunction with the functionality "gear independence with safety technology encoder mounted on the load side":

- S-0-0044, Velocity data scaling type
- S-0-0076, Position data scaling type
- S-0-0086, Torque/force data scaling type
- S-0-0160, Acceleration data scaling type
- P-0-3210, Safety technology configuration
- P-0-3240, Configuration of safe motion 1
- P-0-3250, Configuration of safe motion 2

- P-0-3260, Configuration of safe motion 3
- P-0-3270, Configuration of safe motion 4
- P-0-3239, Configuration of global safety technology functions

Functional principle

The gear independence with safety technology encoder mounted on the load side has to be activated by the corresponding setting in parameter "P-0-3210, Safety technology configuration".

During every switching process to the operating mode, the following configurations are checked:

- The axis has to have been scaled on the load side (S-0-0044, S-0-0076, S-0-0086, S-0-0160).
- The acceleration and velocity data (S-0-0044, S-0-0160) have to have rotary scaling.
- The safety function "Safe braking and holding system" (P-0-3300) should not have been activated.
- The safety function "Safely-limited position" (P-0-3239) should not have been configured.
- The safety function "Safely-monitored position" (P-0-3240, P-0-3250, P-0-3260, P-0-3270) should not have been configured.

In the case of deviations from these configurations, the transition command error "C0256 Safety technology configuration error" is generated.

6 Integrated safety functions

6.1 Overview of safety functions

6.1.1 General information

Application-related safety functions are realized for personal protection in accordance with EN ISO 13849-1 Category 3 PL d and IEC 62061 SIL 2 (Safe Motion) or EN ISO 13849-1 Category 3 PL d/PL e and IEC 62061 SIL 2/SIL 3 (Safe Torque Off).

☞ When a safety function is selected, transition to the corresponding state has to take place for the drive system by means of command value input.

6.1.2 Classification of safety functions

The safety functions can be divided into the following categories:

1. Safety functions in normal operation and in special mode with the following functions
   - Safe maximum speed
   - Safety-limited position
   - Safe direction
2. Safety functions in special mode "safe standstill" with the functions
   - Safe Torque Off
   - Safe stop 1[*1]
   - Safe stop 2[*1]
   - Safe stop 1 (Emergency stop)[*1]
   - Safe braking and holding system
3. Safety functions in special mode "Safe motion" with the following functions
   - Safely-limited speed
   - Safe direction
   - Safely-limited increment
   - Safely-monitored position
4. Additional or auxiliary functions
   - Safely-monitored stopping process
   - Safe homing procedure
   - Safe parking axis
   - Safe brake check
   - Enabling special mode without valid brake status
5. Safe feedback
   - "Safe diagnostic outputs" (acknowledgment)
   - Safe door locking
   - Safe inputs/outputs

☞ Safe door locking is not possible in conjunction with PROFIsafe.

☞ *1The functions "Safe stop 1", "Safe stop 2" and "Safe stop 1 (Emergency stop)" include the "Safely-monitored stopping process".

6.2 Safety functions in normal operation and in special mode

6.2.1 Safe maximum speed (SMS)

Brief description

In the case of the safety function "Safe maximum speed", the dual-channel monitoring prevents the drive from exceeding the preset velocity limit value (P-0-3234, Safe maximum speed).

☞ Using the function "Safe maximum speed" requires the optional safety technology module (S2) which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

Features

The safety function "Safe maximum speed" has the following features:

- Has been realized for personal protection in accordance with EN ISO 13849-1 Category 3 PL d and IEC EN 62061 SIL 2.
- Closed-loop controlled operation is monitored with regard to the exceeding of a defined velocity limit value (cf. "P-0-3234, Safe maximum speed").
- The safety function "Safe maximum speed" is active in normal operation and in special mode.
- The safety function "Safe maximum speed" is selected via the parameter "P-0-3239, Configuration of global safety technology functions" when safety technology is commissioned.
- When a monitor is triggered, this causes an error reaction which shuts down the drive system. The corresponding error message is "F7020 Safe maximum speed exceeded".

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safe maximum speed":

- P-0-3234, Safe maximum speed
- P-0-3239, Configuration of global safety technology functions

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe maximum speed":

- F7020 Safe maximum speed exceeded
- With the safety function "Safe maximum speed" activated, the display of the IndraDrive control panel does not show any specific message, but the standard diagnostic message (e.g., "AF") appears.

Safety function

Selecting the function

The safety function "Safe maximum speed" is selected via the parameter "P-0-3239, Configuration of global safety technology functions" when safety technology is commissioned.

☞ After the safety technology has been activated, "P-0-3234, Safe maximum speed" is write-protected with "P-0-3206, Safety technology password" and cannot be changed by unauthorized persons.

The status of the safety technology password can be seen in "P-0-3207, Safety technology password level".

Monitoring functions

In the case of the safety function "Safe maximum speed", the dual-channel monitoring prevents the drive from exceeding the preset velocity threshold (P-0-3234, Safe maximum speed).

Monitoring of the safe maximum speed (cf. P-0-3234) is active in each safety technology operating status.

When the actual velocity is outside of the limit value (P-0-3234), the fatal safety technology error "F7020 Safe maximum speed exceeded" is generated by the drive and the drive is shut down.

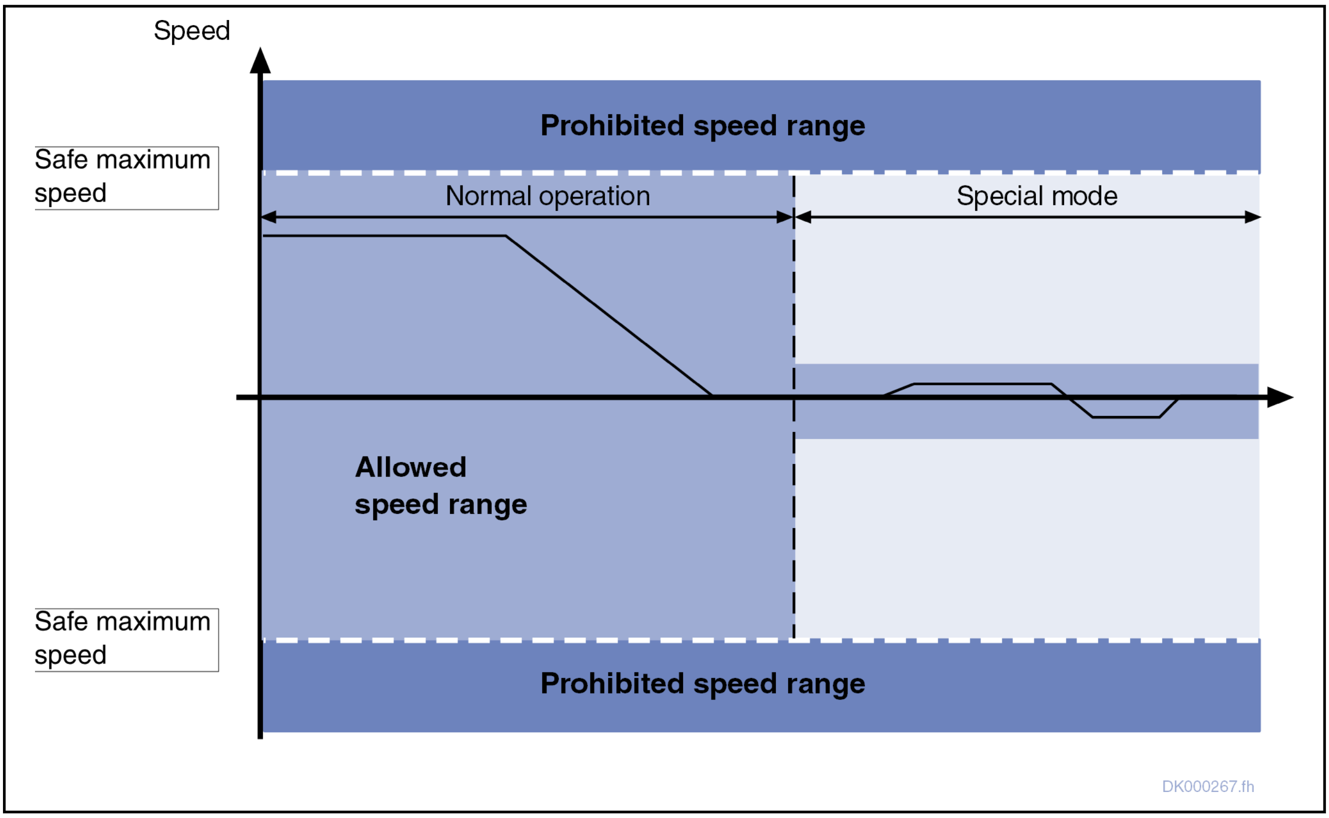


Fig. 6-1: |V_act|<P-0-3234, Safe maximum speed

6.2.2 Safe direction (SDI)

Brief description

☞ The safety function "Safe direction" can be optionally parameterized:

- For the special mode "Safe motion" (see Safety functions in special mode "Safe motion", "Safe direction (SDI)"),
- for normal operation **and** special mode and
- with MPx07V10 and above, explicitly only for normal operation.

The safety function "Safe direction" ensures by dual-channel monitoring that motion is only possible in one direction.

☞ Using the function "Safe direction" requires the optional safety technology module (S2) which can be selected as configuration for the control sections **CSH01.1 or CSH01.3** (ADVANCED) and CDB01.1 (BASIC).

Features

The safety function "Safe direction" for normal operation and special mode has the following features:

- Has been realized for personal protection in accordance with EN ISO 13849-1 Category 3 PL d and IEC EN 62061 SIL 2.
- In the operating mode, the direction of motion is monitored (cf. "P-0-3232, Standstill window for safe direction").
- According to the parameterization, the safety function "Safe direction" is active in normal operation **and** in the special mode or (as of MPx07V10) only in normal operation.
- The safety function "Safe direction" is configured when safety technology is commissioned and afterwards is automatically active in the operating mode (no selection required).
- When the monitor for the direction of motion is triggered, this causes an error reaction which shuts down the drive system. The corresponding error message is "F7031 Incorrect direction of motion".

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safe direction" for normal operation and special mode:

- P-0-3239, Configuration of global safety technology functions
- P-0-3232, Standstill window for safe direction

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe direction":

- F7031 Incorrect direction of motion
- F7040 Validation error parameterized - effective threshold

Safety function

Selecting the function

The safety function "Safe direction" for normal operation and special mode is active after the function has been parameterized and safety technology has been activated; it is not necessary to explicitly select it.

Monitoring function

In the case of the safety function "Safe direction", dual-channel monitoring takes place to make sure that the drive only moves in the enabled direction of motion or, when moving in the non-enabled direction of motion, that it does not exceed P-0-3232; otherwise, the error "F7031 Incorrect direction of motion" is generated and the drive is shut down.

With MPx07V08 and below, it had only been possible to monitor the "Safe direction" in normal operation **and** in the special mode or only in the special mode.

With MPx07V10 and above, it is possible to configure the monitoring of the "Safe direction" in such a way that it is **only** active in normal operation. For this purpose, the parameter P-0-3239 was extended by the bits 10 and 11.

When changing from normal operation to a selected special mode, the configured monitoring of the direction of motion remains active until the new safety technology operating status has been reached. The monitoring of the "Safe direction" for the special modes "Safe motion" can be configured in addition to the monitoring in normal operation.

☞ When the "Safe direction" has been configured for normal operation **and** special mode (P-0-3239, bit 2="1" or bit 3="1"), the direction of motion is also monitored in the following safety functions of the special mode "safe standstill":

- "Safe stop 1" (SS1)
- "Safe stop 2" (SS2)
- "Safe stop 1 (Emergency stop)" (SS1ES)

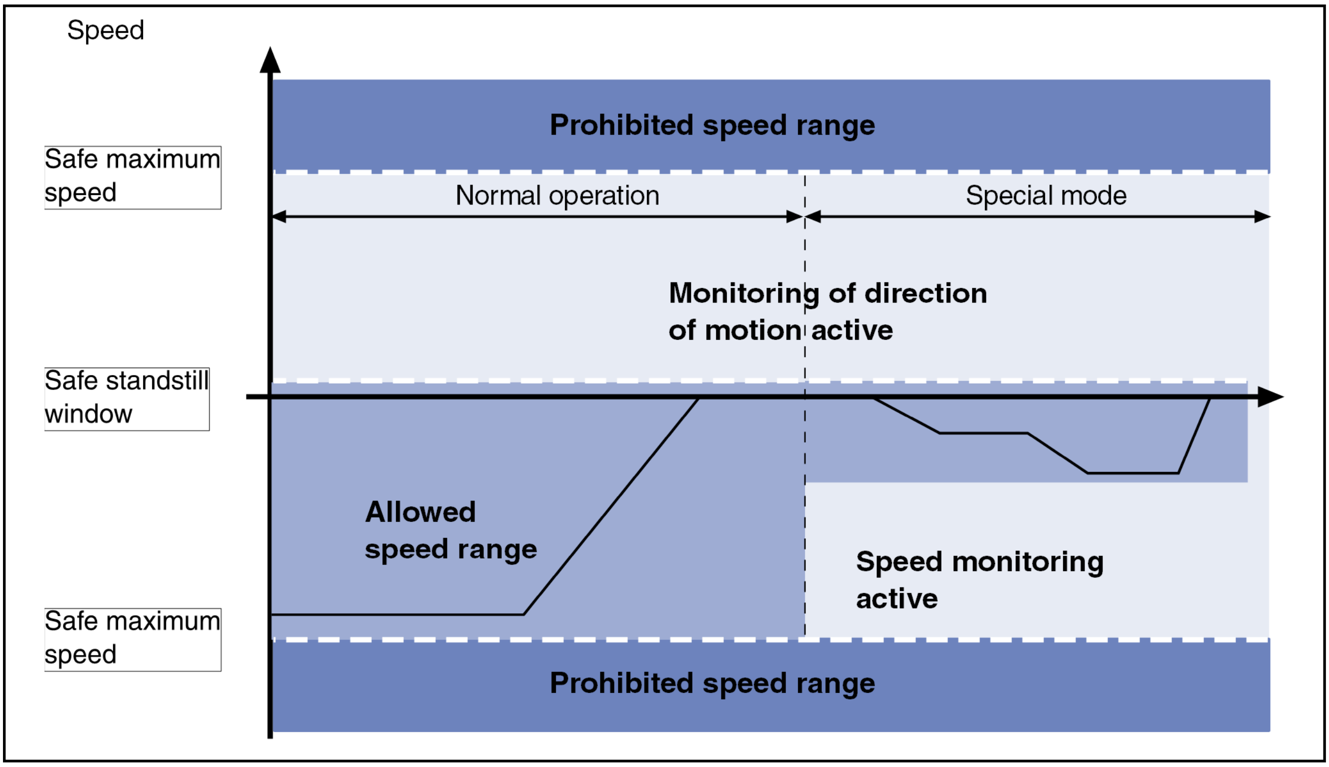


*Fig. 6-2: "Safe direction" for normal operation **and** special mode*

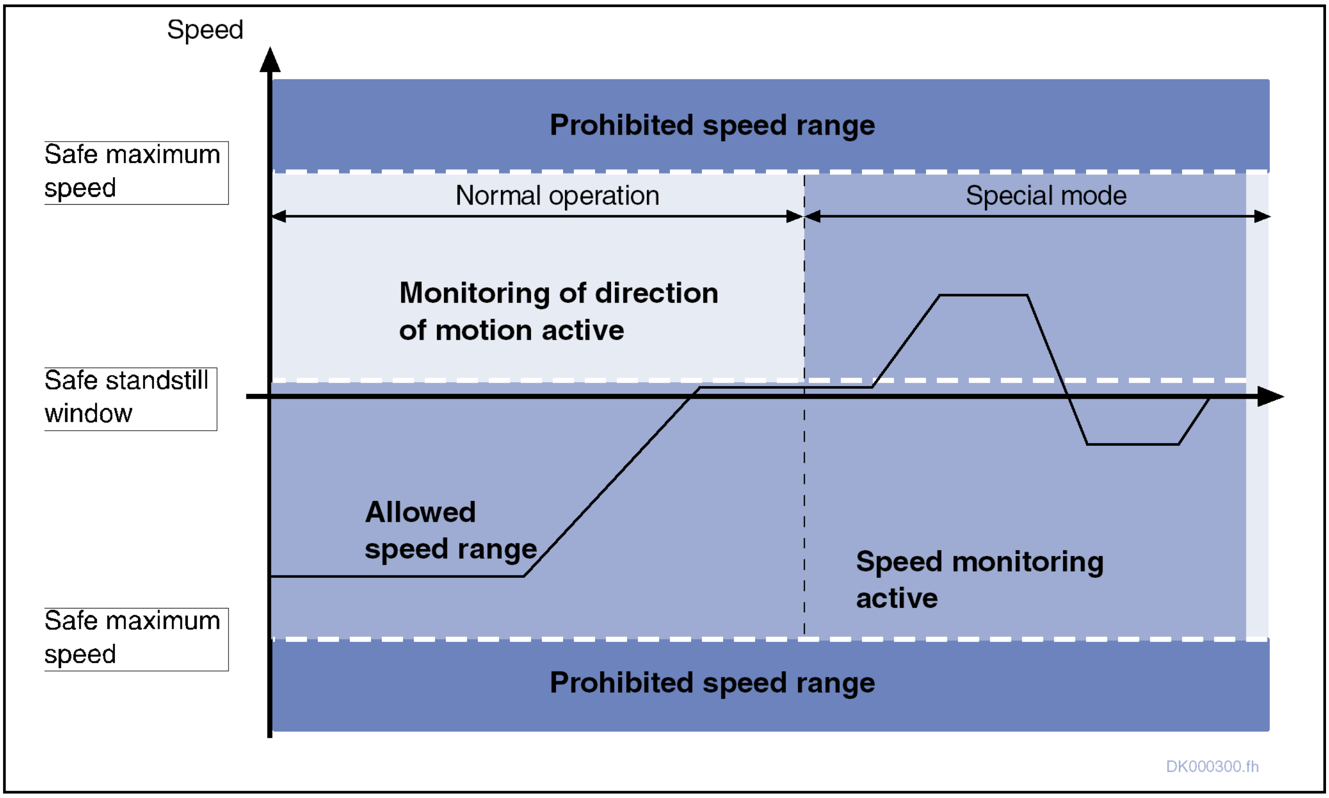


Fig. 6-3: "Safe direction" for normal operation

6.2.3 Safely-limited position (SLP)

Brief description

In the case of the safety function "Safely-limited position", dual-channel monitoring prevents the drive from leaving the preset position range ("P-0-3235, Safely-limited position, positive"; "P-0-3236, Safely-limited position, negative").

☞ Using the safety function "Safely-limited position" requires the optional safety technology module (S2) which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

Features

The safety function "Safely-limited position" has the following features:

- Has been realized for personal protection in accordance with EN ISO 13849-1 Category 3 PL d and IEC EN 62061 SIL 2.
- Closed-loop controlled operation is monitored with regard to the exceeding of the defined positions (cf. "P-0-3235, Safely-limited position, positive"; "P-0-3236, Safely-limited position, negative").
- The safety function "Safely-limited position" is active in normal operation and in special mode.
- The safety function "Safely-limited position" is **selected** via the parameter "P-0-3239, Configuration of global safety technology functions" when safety technology is commissioned.
- When a monitor is triggered, this causes an error reaction which shuts down the drive system. The corresponding error message is "F7021 Safely-limited position exceeded".

Notes on utilization

- The safety function "Safely-limited position" is only allowed in conjunction with the function "Safe maximum speed".
- For the safety function "Safely-limited position", the drive must have been safely homed.

  If Safe reference is not available, the drive may only be moved at a maximum of 20 % of the speed parameterized in P-0-3234. When this speed threshold is exceeded, the drive generates the error F7020.
- The limit values monitored by the safety function "Safely-limited position" always refer to the actual position value of P-0-3280. This value might possibly deviate from the actual position value in S-0-0051 or S-0-0053 (e.g., when encoder corrections or the command C3300/ C3400 are used).
- When the safety function "Safely-limited position" is used and the parameter setting of the error reaction for F7xxx errors is torque disable, it is no longer possible to ensure that the axis does not leave the allowed position range in case the monitors trigger. This, too, must be taken into account for the machine manufacturer's risk analysis.

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safely-limited position":

- P-0-3232, Monitoring window for safe direction
- P-0-3235, Safely-limited position, positive
- P-0-3236, Safely-limited position, negative
- P-0-3239, Configuration of global safety technology functions
- P-0-3280, Actual position value, channel 2
- P-0-3282, Safely-monitored deceleration

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safely-limited position":

- E3107 Safe reference missing
- F3112 Safe reference missing
- F7020 Safe maximum speed exceeded
- F7021 Safely-limited position exceeded
- With "Safely-limited position" activated, the display of the IndraDrive control panel does not show any specific message, but the standard diagnostic message (e.g., "AF") appears.

Safety function

Selecting the function

To use the safety function "Safely-limited position", it has to be activated in the parameter "P-0-3239, Configuration of global safety technology functions"; the safety function is always active after safety technology has been commissioned.

☞ Before the safety function "Safely-limited position" is selected, the "Safe homing procedure" has to be carried out.

Monitoring functions

In the case of the safety function "Safely-limited position", dual-channel monitoring makes sure that the drive ...

- ...only receives such command values (position or velocity) which do not cause the safe position positive or negative ("P-0-3235, Safely-limited position, positive"; "P-0-3236, Safely-limited position, negative") to be exceeded. If the command values are incorrect, the drive generates the error "F7021 Safely-limited position exceeded".

- ...with the current actual velocity and the parameterized deceleration "P-0-3282, Safely-monitored deceleration", can still be stopped within the safe positions. If the actual velocity is too high, the error "F7021 Safely-limited position exceeded" is generated.

Braking distance = actual velocity^2 / (2 × P-0-3282) Braking distance < |P-0-3235 (or P-0-3236) - actual position value|
Legend: P-0-3235, Safely-limited position, positive P-0-3236, Safely-limited position, negative P-0-3282, Safely-monitored deceleration

Tab. 6-1: Calculating the braking distance for monitoring the safety function "Safely-limited position"

☞ The end positions set in P-0-3235 and P-0-3236 relate to the actual position value in P-0-3280. This value might possibly deviate from the actual position value in S-0-0051 or S-0-0053 (e.g., when encoder corrections or the command C3300/C3400 are used).

☞ The deceleration ramp defined in parameter "P-0-3282, Safely-monitored deceleration" should be set such that the drive has the deceleration capacity to come to standstill before the safe positions set in "P-0-3235, Safely-limited position, positive" or "P-0-3236, Safely-limited position, negative" are reached.

- ...is homed in a safe way after having reached the operating mode. As long as "Safe reference" has not been established, the warning "E3107 Safe reference missing" is output. After the warning has occurred, the drive can be operated for 15 minutes without "Safe reference", then the error "F3112 Safe reference missing" will be generated.

⚠ DANGER

Lethal injury / property damage caused by drive operation without reference, as the safe positions (positive / negative) can be exceeded!

⇒ Establish Safe reference

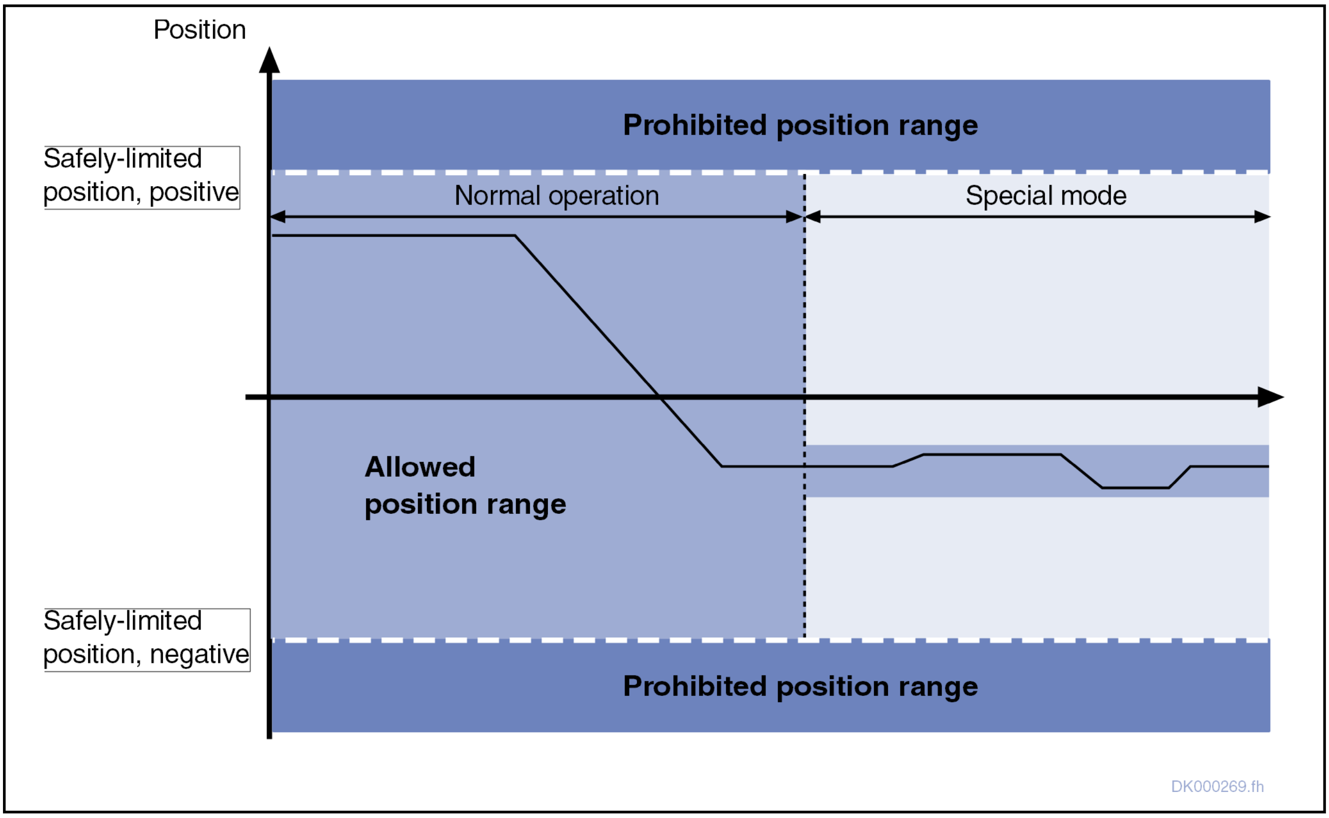

Position
Safely-limited position, positive
Prohibited position range
Normal operation
Special mode
Allowed position range
Safely-limited position, negative
Prohibited position range
DK000269.fh

Fig. 6-4: "Safely-limited position"

Return motion to allowed position range

When the axis is outside of the allowed position range, the error "F7021 Safely-limited position exceeded" is generated. This error can be reset by executing the command "S-0-0009, C0500 Reset class 1 diagnostics". Afterwards it is possible to move the axis back to the allowed position range; when this is done the drive only allows motion in the direction of the allowed position range. Motion in the other direction is only possible within the tolerance window (P-0-3232, Monitoring window for safe direction), otherwise the error "F7021 Safely-limited position exceeded" is immediately generated again.

6.3 Safety functions in special mode "Safe standstill"

6.3.1 Safe torque off (STO)

Brief Description

☞ Using the function "Safe torque off" requires the optional safety technology module "L2".

The energy supply to the drive is safely interrupted with the safety function "Safe torque off". The drive cannot generate any torque/force and, as a consequence, it cannot generate any dangerous motions, either.

☞ Before activating the safety function "Safe torque off", the drive system must be decelerated via the command value input; there is no drive-controlled deceleration!

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ If external force influences are to be expected with the safety function "Safe torque off", e.g. in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation; for such axes, Bosch Rexroth recommends that you use the safe braking and holding system.

Features

The safety function "Safe torque off" has the following features:

- Corresponds to stop category 0 according to EN 60204-1
- Is suited for safety-relevant applications up to Category 1 PL c and Category 3 PL d/PL e according to EN ISO 13849-1 or up to SIL 1/SIL 2/SIL 3 according to IEC EN 62061.
- The energy supply to the motor is safely interrupted via two channels.
- The **selection** is made via two channels using either an N/C-N/O or an N/C-N/C combination.

  To attain SIL 3/PL e, selection must take place via a higher-level safety master which also attains SIL 3/PL e.
- The safe state is **acknowledged** by an N/C-N/O contact; to attain SIL 2/PL d and SIL 3/PL e, the acknowledgment must always be evaluated.
- For **dynamization of the safety function selection**, the function must be activated at least every 168 hours (SIL 2/PL d) or 24 hours (SIL 3/PL e). For this reason, the operating hours of the power section at which the safety function "Safe torque off" was selected the last time are stored in the parameter "P-0-0102, Oper. hours power section at last activation of STO".

  To attain SIL 1/PL c, the dynamization of the safety function selection is not required.
- Monitoring the validity of the selection: 100 ms after selection was changed.
- The time intervals for activating the safety function "Safe torque off" have to be set via "P-0-0103, Time interval of forced dynamization".
- The history of the time intervals that were set is displayed in the parameter "P-0-0104, Change history time interval of forced dynamization".
- The status of the safety function "Safe torque off" is displayed via the parameter "P-0-0106, Operating status of STO".

Pertinent Parameters

The following parameters are used in conjunction with the safety function "Safe torque off":

- P-0-0101, Configuration for STO selector
- P-0-0102, Oper. hours power section at last activation of STO
- P-0-0103, Time interval of forced dynamization
- P-0-0104, Change history time interval of forced dynamization
- P-0-0106, Operating status of STO

Pertinent Diagnostic Messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe torque off":

- F8027 Safe torque off while drive enabled
- F7043 Error of output stage interlock

- F3130 Error when checking input signals
- F3131 Error when checking acknowledgement signal
- E3110 Time interval of forced dynamization exceeded
- E8027 Safe torque off while drive enabled
- With the safety function "Safe torque off" activated, the display of the IndraDrive control panel shows "STO".

Safety function

On the optional safety technology module "L2", there are 24 V inputs available for dual-channel selection and a floating changeover contact for dual-channel feedback (all 3 connections can be accessed).

> ☞ For pin assignments and technical data of the optional safety technology module, please see the Project Planning Manual of the control section.

The safety function "Safe torque off" can be divided into the following topics which are described in detail below:

- Forced dynamization
- Selection of the safety function "Safe torque off"
- Requirements on the command value input

Forced dynamization

Forced dynamization is to detect static error states, so-called "sleeping errors", during safety function selection and in the interrupting circuits. Both the control section in standard design and the optional safety technology module "L2" have their own interrupting circuits.

> ☞ After drive enable has been set and within, for example, 8 hours, manual dynamization is required (activate safety function "Safe torque off") which is initiated by removing drive enable.

> ☞ To attain SIL 3/PL e, forced dynamization must take place via a higher-level safety master which also attains SIL 3/PL e. The test must take place at least every 24 hours or - when guards are used - directly before the safety area is enabled. The test procedure to be carried out is described under "Requirements on the control unit".

Setting drive enable starts the lifecounter which runs as long as the drive is in control. When drive enable is reset, the lifecounter is stopped and the current value is stored. The lifecounter is only reset when the safety function "Safe torque off" is selected.

"P-0-0103, Time interval of forced dynamization" is used to set the time interval for the lifecounter. When the time interval is exceeded, the drive generates the warning "E3110 Time interval of forced dynamization exceeded" and thereby signals that forced dynamization has to be carried out. This is done by simple selection of the safety function "Safe torque off".

The operating hours of the power section at which the safety function "Safe torque off" was selected the last time are stored in the parameter "P-0-0102, Oper. hours power section at last activation of STO".

A history of the time intervals set by the user in "P-0-0103, Time interval of forced dynamization" is stored in the parameter "P-0-0104, Change history time interval of forced dynamization".

Selecting the safety function "Safe torque off"

The safety function "Safe torque off" is selected via two channels, either by means of a switch with two N/C contacts, or a switch with one N/C contact and one N/O contact, at the 9-pin D-Sub connector on the optional module "L2".

See also "L2 - Safe torque off"

With parameter "P-0-0101, Configuration for STO selector", it is possible to configure the selection via N/C contacts or N/C-N/O contacts.

The firmware checks the selection signals for validity. In the case of states which are not allowed, the drive generates the error "F3130 Error when checking input signals".

The status of the safety function "Safe torque off" and the selection signal validation can be read via the parameter "P-0-0106, Operating status of STO".

☞ The tolerance time for different selection of channel 1 and channel 2 is 100 ms; the parameter setting of the tolerance time cannot be changed.

One channel of the switch can be connected via PLC I/O, the second channel then should be directly connected to the optional safety technology module.

Both channels of the switch can be connected via I/Os of a safety PLC.

Both channels can be connected via the safety contacts of a door monitoring device. For feedback to the monitoring device, there is a floating contact available.

☞ For applications according to EN ISO 13849-1 Category 3 PL d/PL e and IEC 62061 SIL 2/SIL 3, the acknowledgment must be evaluated via STO Q - STO Q1 or STO Q - STO Q2.

☞ For applications according to EN ISO 13849-1 Category 3 PL d/PL e and IEC 62061 SIL 2/SIL 3 it is not allowed to route both channels via a standard PLC!

Requirements on the command value input

☞ Before selecting the safety function "Safe torque off", the drive system has to be decelerated via the command value input; there is no drive-controlled deceleration!

☞ The safety function "Safe torque off" corresponds to stop category 0 according to EN 60204-1.

When drive enable has been set and the safety function "Safe torque off" is selected at the same time, the drive generates the error "F8027 Safe torque off while drive enabled", because the drive first has to be shut down before it is allowed to activate the safety function "Safe torque off".

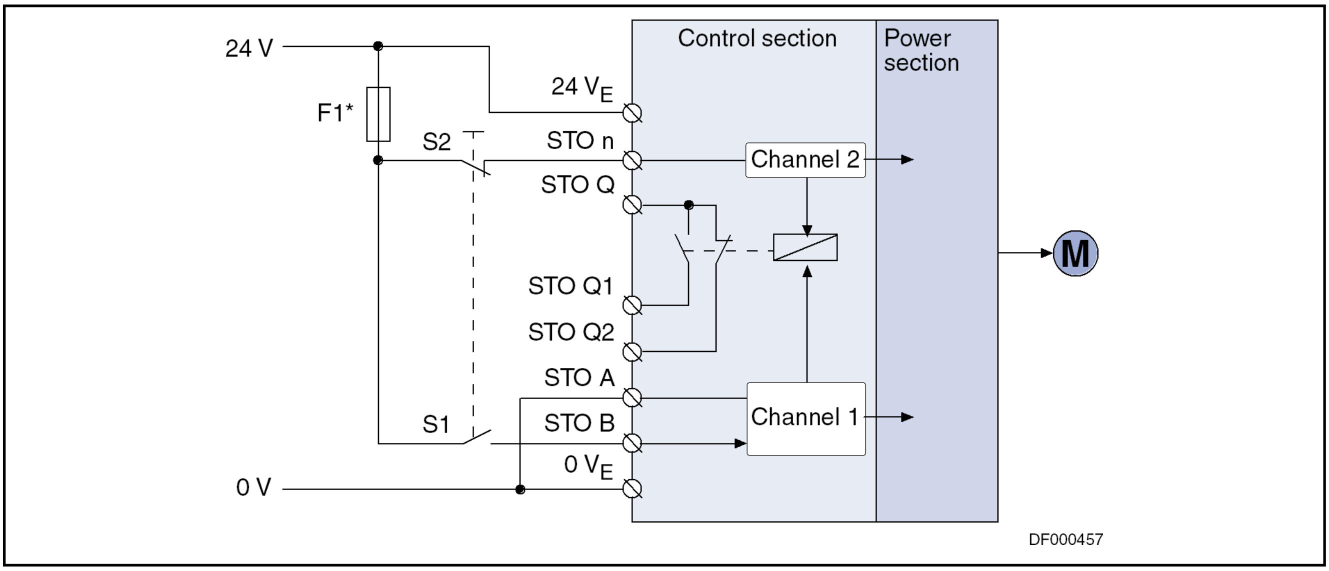
Via the parameter "P-0-0101, Configuration for STO selector", the diagnostic message displayed can be changed from the fatal error "F8027 Safe torque off while drive enabled" to the fatal warning "E8027 Safe torque off while drive enabled". The warning is automatically cleared, when drive enable is removed. In the diagnostic message memory, however, the fatal warning remains entered.

⚠ DANGER **Lethal injury and/or property damage caused by coasting axes!**

⇒ If the safety function"Safe torque off" is selected with drive enable having been set, the drive torque, independent of the diagnostic message which was set, is immediately disabled and the drive coasts to stop; the shutdown process is relatively slow and, above all, not safe!

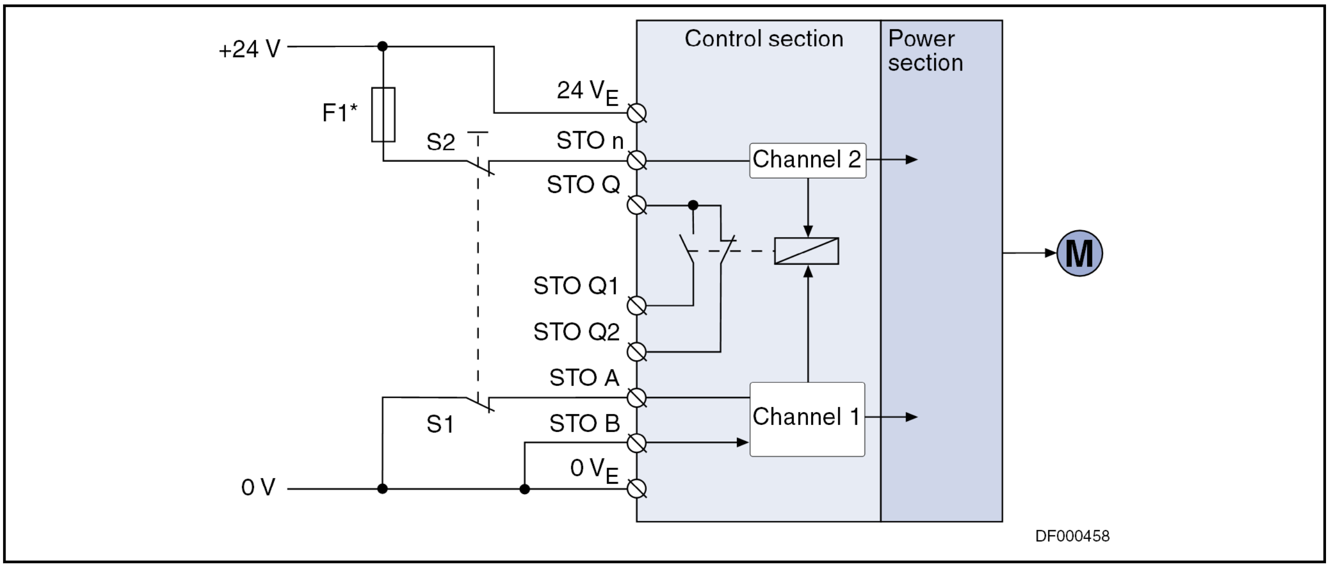
Notes on commissioning

☞ For applications according to EN ISO 13849-1 Category 3 PL d/PL e and IEC 62061 SIL 2/SIL 3, the acknowledgment must be evaluated via STO Q - STO Q1 or STO Q - STO Q2.



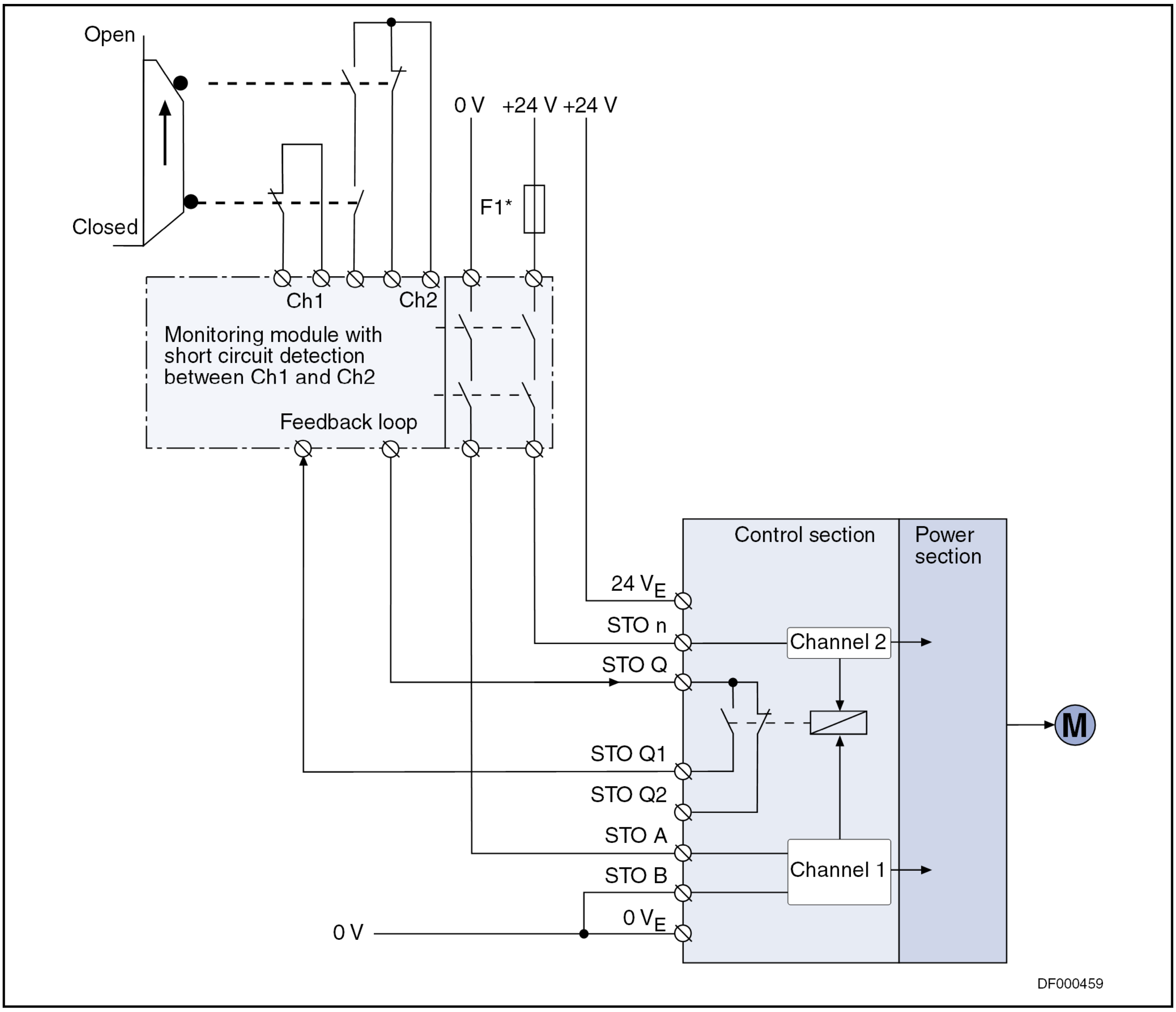
Data for F1*, see switch contacts S1/S2

Fig. 6-5: Selecting the safety function "Safe torque off" via switch with N/C-N/O contacts



Data for F1*, see switch contacts S1/S2

Fig. 6-6: Selecting the safety function "Safe torque off" via switch with two N/C contacts



Data for F1*, see switch contacts of safety module

Fig. 6-7: Selecting the safety function "Safe torque off" using a safety module

☞ In terms of EN ISO 13849-1 and IEC 62061, the signal processing of a standard PLC has to be regarded as single-channel, the circuit illustrated below therefore is not allowed!

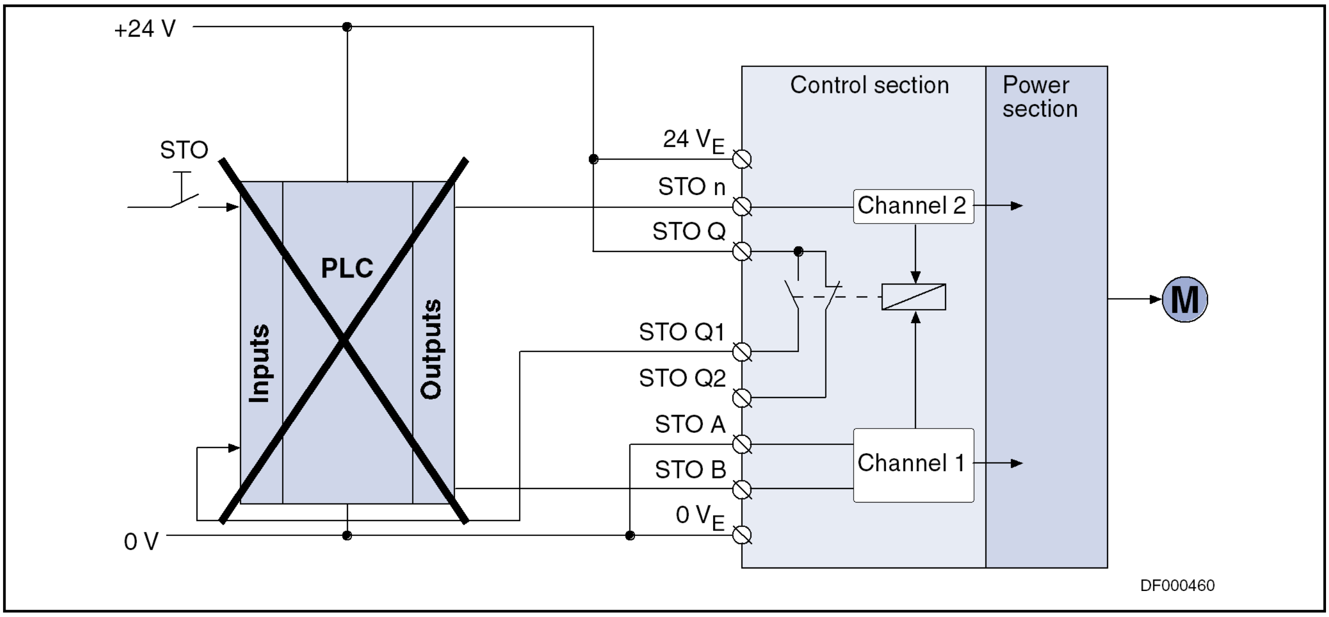
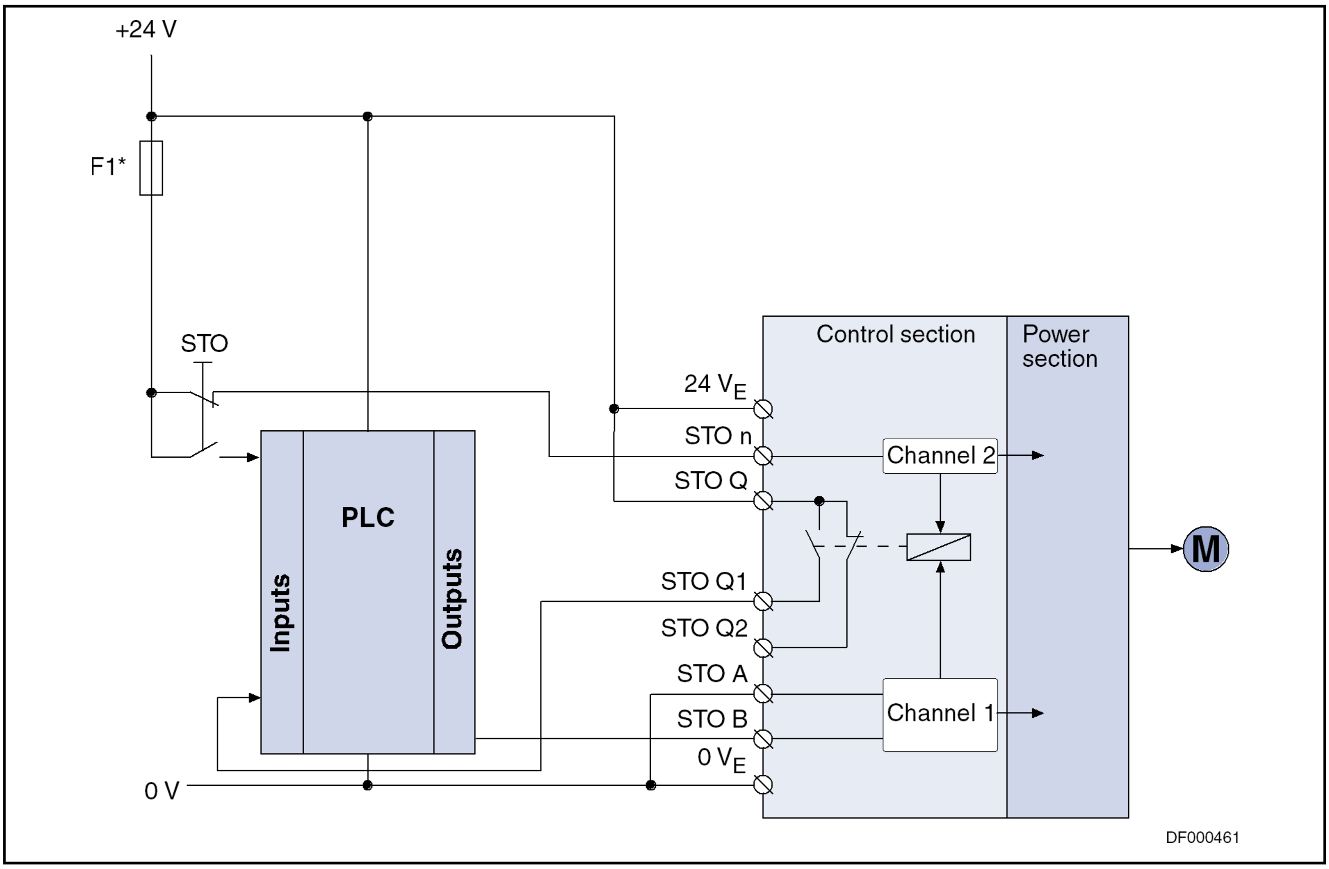
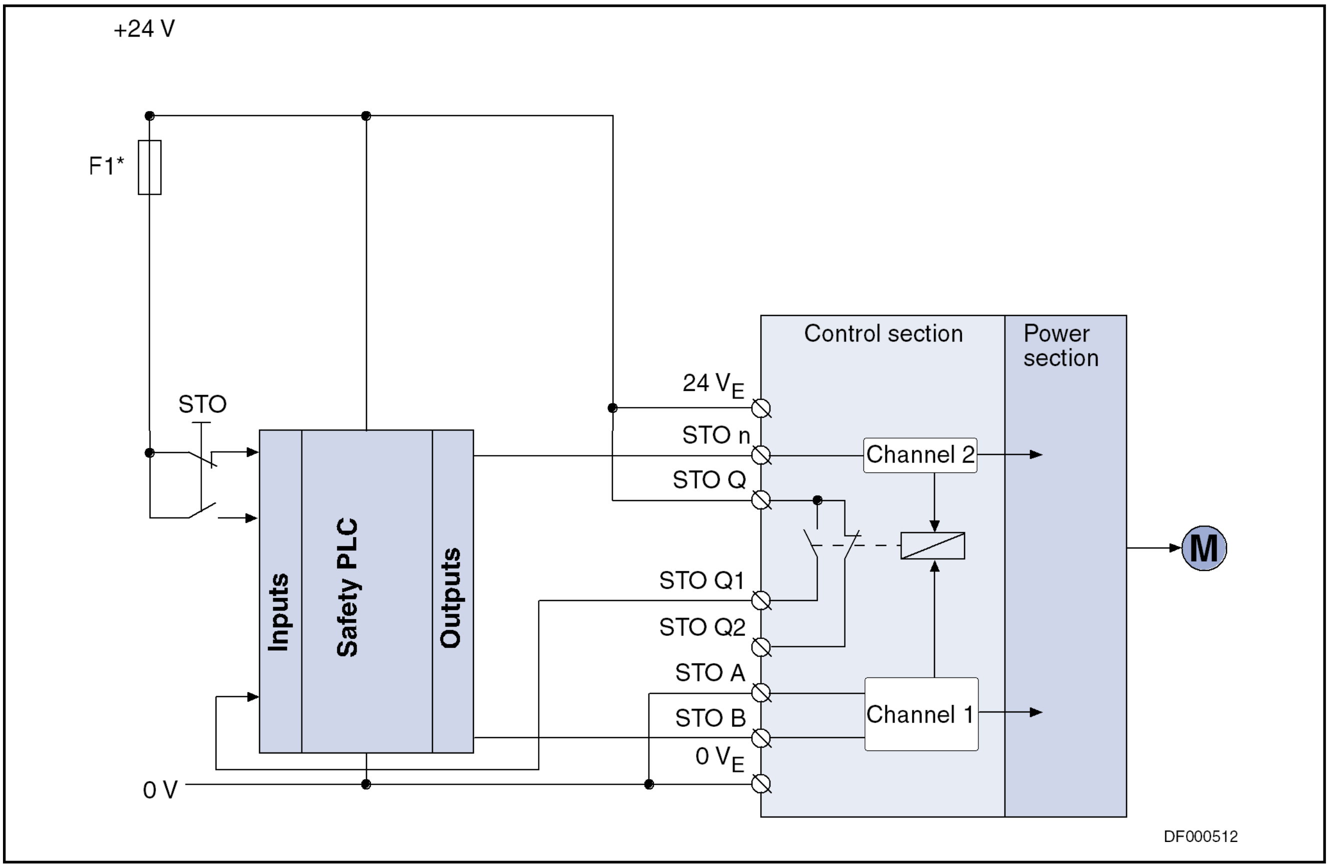


Fig. 6-8: Selecting the safety function "Safe torque off" via standard PLC (negative example)



F1* Data for F1*, see switch contacts of optional safety technology module "L2"

Fig. 6-9: Selecting the safety function "Safe torque off" via switch with N/C-N/O contacts and ***standard PLC (SIL 2/PL d)***



F1* Data for F1*, see switch contacts of optional safety technology module "L2"

*Fig. 6-10: Selecting the safety function "Safe torque off" via switch with N/C-N/O contacts and **safety technology master (e.g., safety PLC) (SIL 3/PL e)***

Notes on project planning

When configuring the safety function "Safe torque off", it is absolutely necessary to observe the following safety instructions:

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ If external force influences are to be expected with the safety function "Safe torque off", e.g. in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation. For such axes, Bosch Rexroth recommends using the safe braking and holding system.

⚠ WARNING **Injury and/or property damage caused by deviation from standstill position!**

⇒ Even if the control of the power section has been safely locked, momentary axis motion, depending on the number of poles of the motor, can be triggered, when two errors are occurring simultaneously in the power section with the voltage DC bus being active:

- Breakdown of a power semiconductor **and**
- Breakdown of another semiconductor

In this case, two of six semiconductors are affected in such a way that the motor shaft is aligning.

Synchronous motor example: In the case of a synchronous motor with 6 pole pairs, the motion can be a maximum of 30 degrees. For a directly driven ball screw, e.g. 20 mm per revolution, this corresponds to a one-time maximum linear motion of 1.67 mm.

When an asynchronous motor is used, the short circuits in two separate circuits of the power section have almost no effect, because the exciter field breaks down when the inverter is shut down and has completely died down after approx. 1 s.

6.3.2 Safe stop 1 (SS1)

Brief description

With the safety function "Safe stop 1", the energy supply to the motor is safely interrupted. The motor cannot generate any torque/any force and therefore no dangerous movements.

☞ Using the safety function "Safe stop 1" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ Please observe the safety instructions in section "Notes on project planning".

☞ The safety function "Safe stop 1" is deselected by selecting "SS1 (Emergency stop) switch" or actuating the enabling control or by deselecting the mode selector!

Features

The function has the following features:

- Corresponds to stop category 1 according to EN 60204-1.
- Is suited for safety-relevant applications up to PL d according to EN ISO 13849-1 Category 3 or up to SIL 2 according to IEC 62061.
- The energy supply to the motor is safely interrupted via two channels.
- The duration of the transition to safe stop 1 is monitored (cf. "P-0-3220, Tolerance time transition from normal operation" or "P-0-3225, Tolerance time transition from safe operation").
- With "Safe stop 1", there aren't any monitoring functions active.

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safe stop 1":

- P-0-3210, Safety technology configuration
- P-0-3212, Safety technology control word, channel 1
- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation
- P-0-3233, Velocity threshold for safe standstill

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe stop 1":

- F7040 Validation error parameterized - effective threshold
- F7050 Time for stopping process exceeded
- F8030 Safe stop 1 while drive enabled
- With the safety function "Safe stop 1" activated, the display of the IndraDrive control panel shows "SS1".

Safety function

Basic principle

With the safety function "Safe stop 1", the energy supply to the motor is safely interrupted. The motor cannot generate any torque/any force and therefore no dangerous movements.

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ Please observe the safety instructions in section "Notes on project planning".

Transition to the safe state

The type of transition to the safe state can be set in the parameter "P-0-3210, Safety technology control word". It is possible to select either "drive-controlled safety technology operation mode transitions" or "NC-controlled operation mode transitions" (see "Transition to safe state"). In both cases, the safety function "Safely-monitored stopping process" becomes active for transition (see "Safely-monitored stopping process").

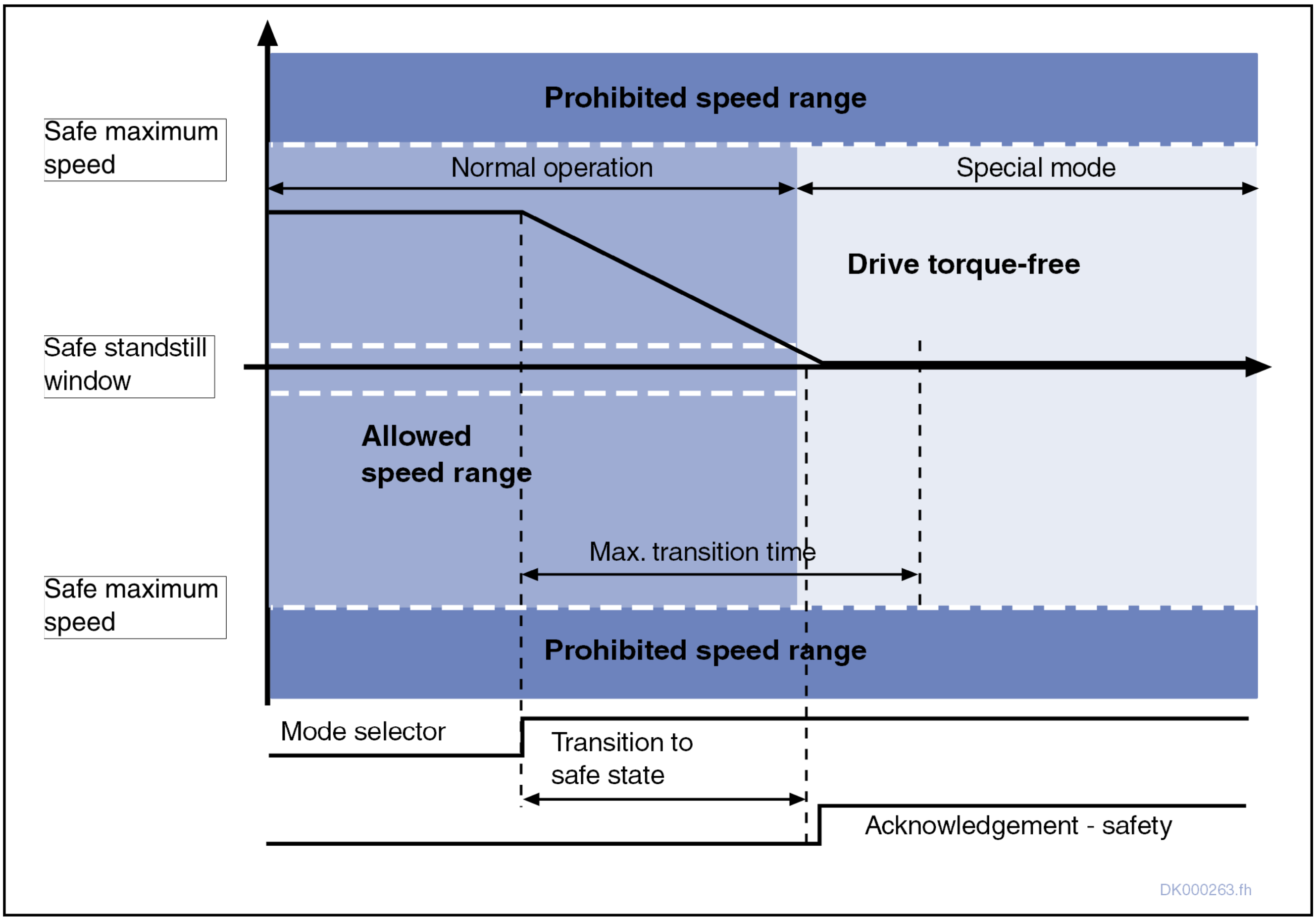


Fig. 6-11: Drive-controlled transition to "Safe stop 1" from normal operation

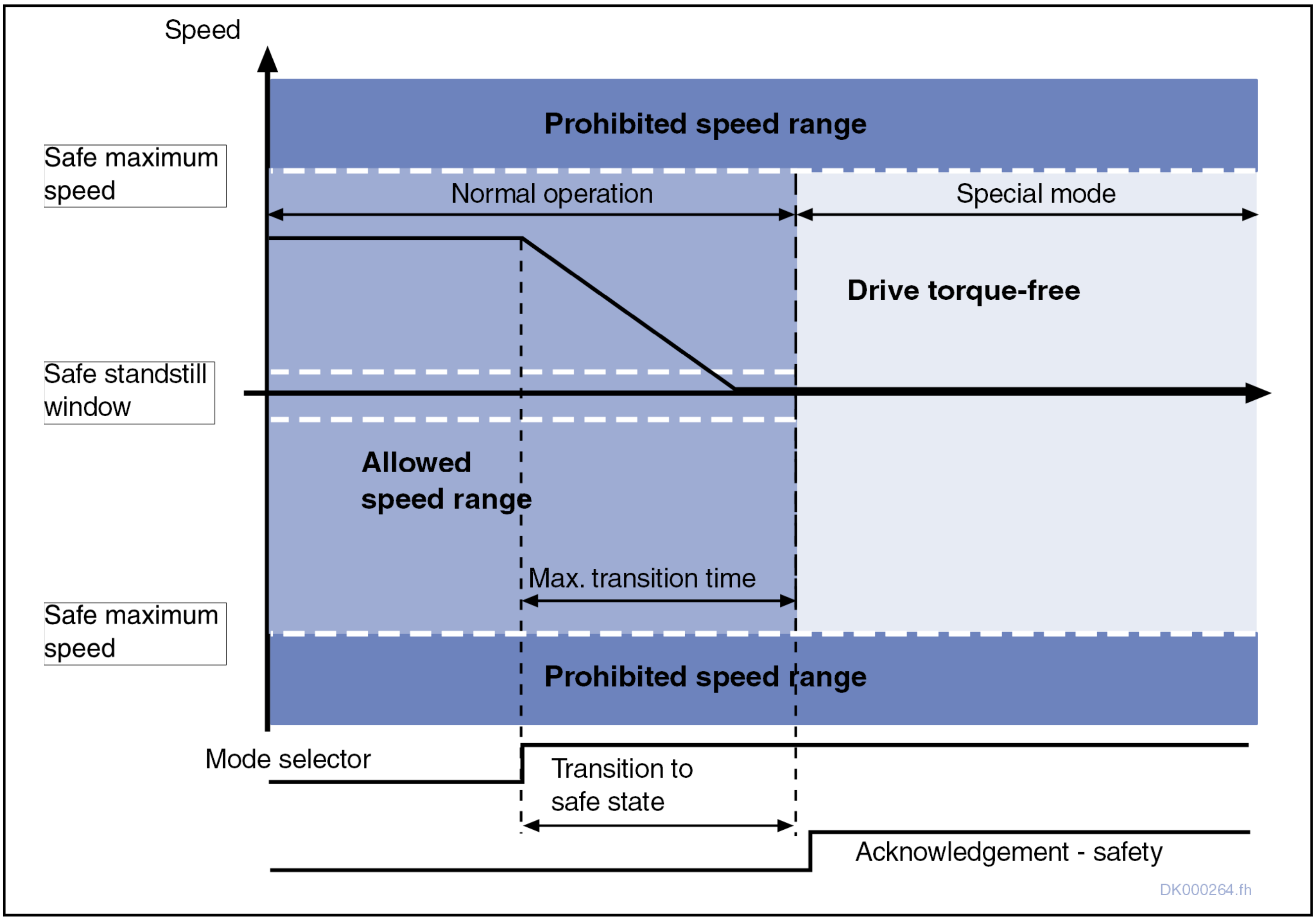


Fig. 6-12: NC-controlled transition to "Safe stop 1" from normal operation

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ In "Safe stop 1", the drive cannot generate any torque/any force and therefore no dangerous movements which has to be taken into account above all for vertical axes. Please observe the safety instructions in section "Notes on project planning".

Monitoring functions

If the safety function "Safe stop 1" has been activated and drive enable is set, the error "F8030 Safe stop 1 while drive enabled" is generated.

Terminating Safe stop 1

The function "Safe stop 1" is deselected by selecting "Safe stop 1 (Emergency stop)" or actuating the enabling control or by deselecting the mode selector!

Notes on project planning

When configuring the safety function "Safe stop 1", it is absolutely necessary to observe the following safety instructions:

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ If external force influences are to be expected with the safety function "Safe stop 1", e.g. in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation. For such axes, Bosch Rexroth recommends using the safe braking and holding system.

⚠ WARNING **Injury and/or property damage caused by deviation from standstill position!**

⇒ Even if the control of the power section has been safely locked, momentary axis motion, depending on the number of poles of the motor, can be triggered, when two errors are occurring simultaneously in the power section with the voltage DC bus being active:

- Breakdown of a power semiconductor **and**
- Breakdown of another semiconductor

In this case, two of six semiconductors are affected in such a way that the motor shaft is aligning.

Synchronous motor example: In the case of a synchronous motor with 6 pole pairs, the motion can be a maximum of 30 degrees. For a directly driven ball screw, e.g. 20 mm per revolution, this corresponds to a one-time maximum linear motion of 1.67 mm.

When an asynchronous motor is used, the short circuits in two separate circuits of the power section have almost no effect, because the exciter field breaks down when the inverter is shut down and has completely died down after approx. 1 s.

6.3.3 Safe stop 2 (SS2)

Brief description

In the case of the safety function "Safe stop 2", the drive is in controlled standstill, i.e. all control functions between the electronic control unit and the drive are maintained. The dual-channel monitoring prevents the drive from carrying out dangerous movements due to errors although the energy supply is not interrupted.

☞ Using the safety function "Safe stop 2" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ Please observe the safety instructions in section "Notes on project planning".

Features

The safety function "Safe stop 2" has the following features:

- Corresponds to stop category 2 according to EN 60204-1.

- Is suited for safety-relevant applications up to PL d according to EN ISO 13849-1 Category 3 or up to SIL 2 according to IEC 62061.
- Standstill monitoring after "Safe operating stop" (SOS).
- The energy supply to the motor is **not** interrupted.
- Closed-loop controlled operation in standstill is monitored (cf. "P-0-3230, Monitoring window for safe stop 2").
- The duration of the transition to safe operating stop is monitored (cf. "P-0-3220, Tolerance time transition from normal operation" or "P-0-3225, Tolerance time transition from safe operation").
- When a monitor is triggered, this causes an error reaction which shuts down the drive system. The corresponding error message is "F7030 Position window Safe stop 2 exceeded".

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safe stop 2":

- P-0-3210, Safety technology configuration
- P-0-3212, Safety technology control word, channel 1
- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation
- P-0-3230, Monitoring window for safe stop 2
- P-0-3233, Velocity threshold for safe standstill

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe stop 2":

- F7030 Position window Safe stop 2 exceeded
- F7040 Validation error parameterized - effective threshold
- F7050 Time for stopping process exceeded
- With the safety function "Safe stop 2" activated, the display of the IndraDrive control panel shows "SS2".

Safety function

Basic principle

In the case of the safety function "Safe stop 2", the drive is in controlled standstill, i.e. all control functions between the electronic control unit and the drive are maintained. The drive, however, cannot generate any dangerous movement although the energy supply is not interrupted.

☞ When the safety function "Safe stop 2" has been selected, the control unit can reset drive enable and set it again. The monitoring of the standstill position always remains active.

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ Please observe the safety instructions in section "Notes on project planning".

Transition to the safe state

The type of transition to the safe state can be set in the parameter "P-0-3210, Safety technology control word". It is possible to select either "drive-controlled safety technology operation mode transitions" or "NC-controlled operation mode transitions" (see "Transition to safe state"). In both cases, the safety function "Safely-monitored stopping process" becomes active for transition (see "Safely-monitored stopping process").

For transition to the safe state, there is a programmable time (P-0-3220 from normal operation and P-0-3225 from special mode) available. After the time is over, the drive is shut down with velocity command value reset and energy supply is safely (i.e. via two channels) interrupted. The error "F7050 Time for stopping process exceeded" is generated.

In "Safe stop 2", the energy supply is not interrupted; all control functions between the electronic control unit and the drive are maintained.

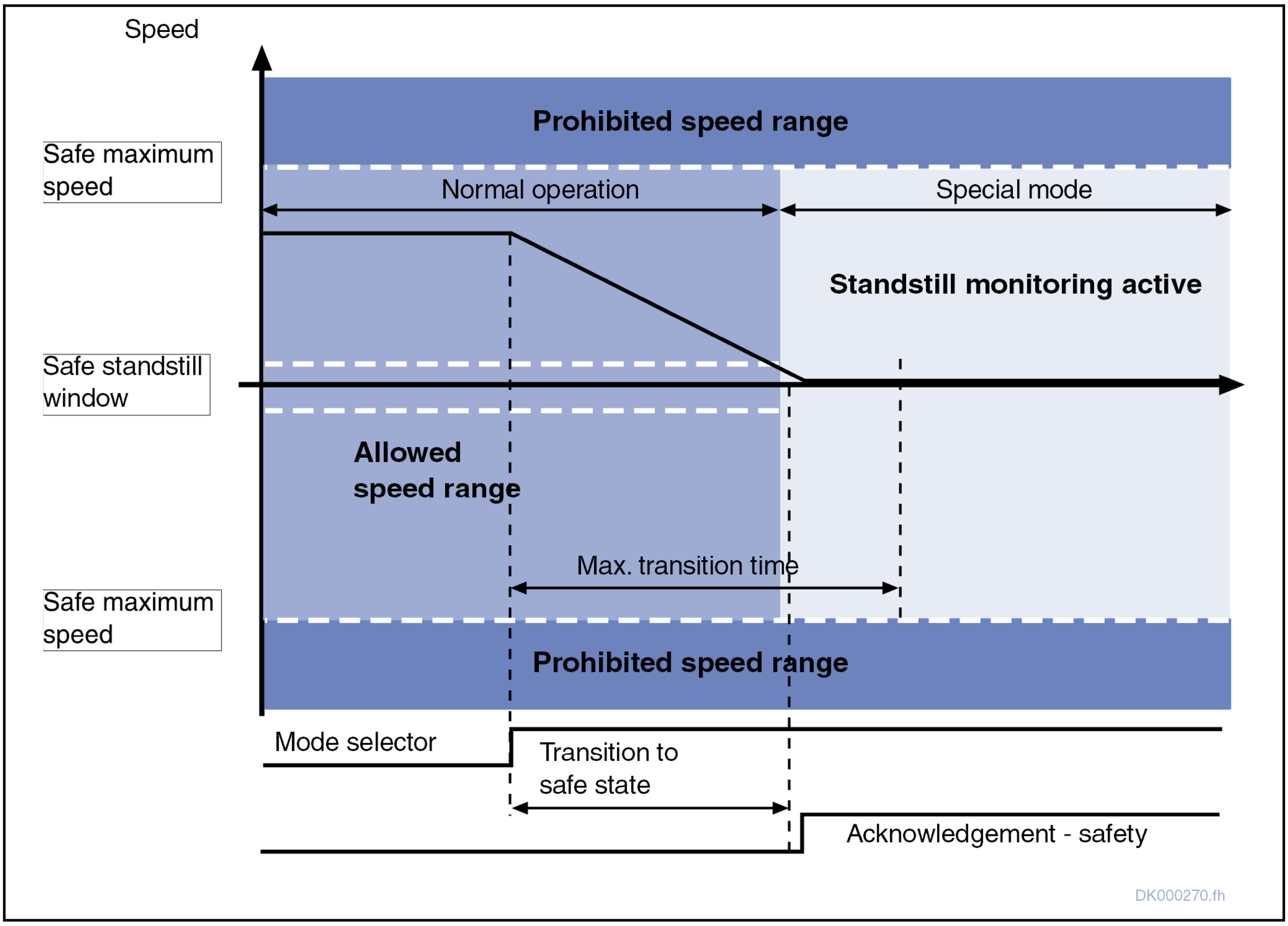


Fig. 6-13: Drive-controlled transition to "Safe stop 2" from normal operation

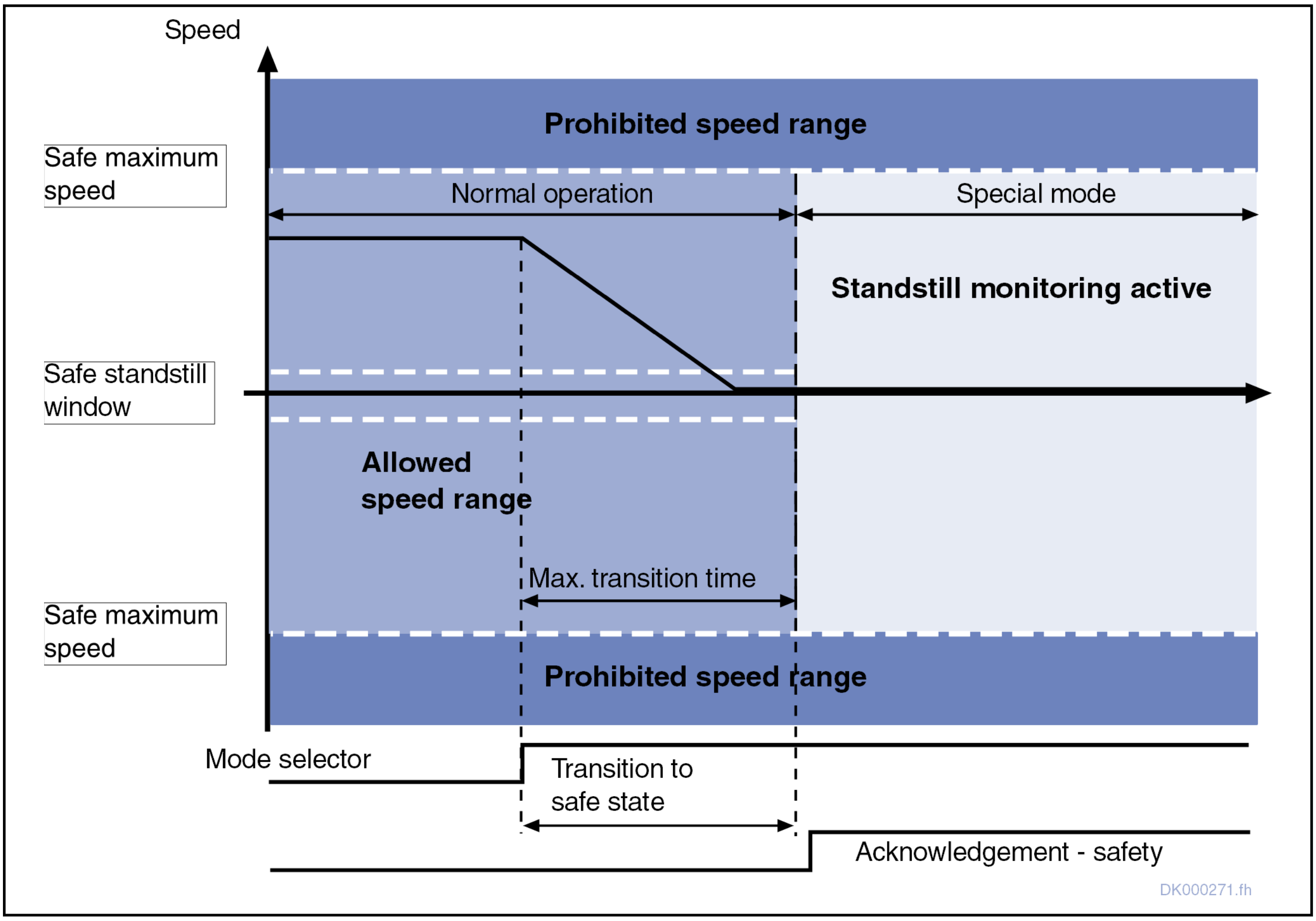


Fig. 6-14: NC-controlled transition to "Safe stop 2" from normal operation

Monitoring functions

With the safety function "Safe stop 2" activated, dual-channel monitoring of the actual position or the travel distance prevents the drive from carrying out dangerous movements due to errors.

In addition, monitoring makes sure that there aren't any command values preset for the drive during "Safe stop 2" which would cause the drive to leave the monitoring window for "Safe stop 2" (P-0-3230).

When the travel distance is greater than the value parameterized in "P-0-3230, Monitoring window for safe stop 2", the drive generates the error "F7030 Position window Safe stop 2 exceeded" and is shut down.

☞ After the safety technology has been activated, "P-0-3230, Monitoring window for safe stop 2" is write-protected with "P-0-3206, Safety technology password" and cannot be changed by unauthorized persons.

The status of the safety technology password can be seen in "P-0-3207, Safety technology password level".

Terminating Safe stop 2

After the safe stop 2 has been removed, e.g. by closing a protective device and executing the start command, the working motion of the drive can be immediately continued at the point of interruption.

The function "Safe stop 2" is deselected by selecting "Safe stop 1 (Emergency stop)" or actuating the enabling control or by deselecting the mode selector!

Notes on project planning

When using the safety function "Safe stop 2", it is absolutely necessary to observe the following safety instructions:

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ If external force influences are to be expected with the safety function "Safe stop 2", e.g. in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation. For such axes, Bosch Rexroth recommends using the safe braking and holding system.

⚠ WARNING **Injury and/or property damage caused by deviation from standstill position!**

⇒ When using the safety function "Safe stop 2" for axes with external force influences, error situations (e.g., mains failure, controller defect) can occur in which the drive controller can no longer keep the axis in position. In this case, the axis must be kept in position by additional measures (e.g. mechanical brake). In the time between the occurrence of the error and the triggering of the "additional holding device", axis motion can occur. This has to be taken into account for the risk assessment of the installation.

For such axes, Bosch Rexroth recommends using the safe braking and holding system.

Make sure that the value parameterized in "P-0-3233, Velocity threshold for safe standstill" is sufficiently small, because during transition to the safe state, the standstill monitor ("P-0-3230, Monitoring window for safe stop 2") becomes active immediately after the velocity has fallen below this value, and the drive then must have come to standstill.

6.3.4 Safe stop 1 (Emergency stop) (SS1ES)

Brief description

The safety function "Safe stop 1 (Emergency stop)" corresponds to the safety function "Safe stop 1", but is not disabled by activating an enabling control.

☞ Using the safety function "Safe stop 1 (Emergency stop)" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

☞ The selection of the function "Safe stop 1 (Emergency stop)" takes effect in normal operation, too.

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ Please observe the safety instructions in section "Notes on project planning".

Features

The safety function "Safe stop 1 (Emergency stop)" has the following features:

- Corresponds to stop category 1 according to EN 60204-1.
- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC 62061.
- The energy supply to the motor is safely interrupted.
- The duration of the transition to the safety function "Safe stop 1 (Emergency stop)" is monitored (cf. "P-0-3220, Tolerance time transition from normal operation" or "P-0-3225, Tolerance time transition from safe operation").

Examples of application

The safety function "Safe stop 1 (Emergency stop)" can be used, for example, for manual tool change in the case of spindle drives or handling axes which are to be manually moved.

According to EN 60204-1, purely electrical devices (such as the safety function "Safe stop 1 (Emergency stop)") are allowed for emergency stop in addition to electromechanical devices.

⚠ WARNING **Death or serious injury might possibly be caused by restart!**

If an electrical device is used for emergency stop, restart must be prevented using an emergency stop device.

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safe stop 1 (Emergency stop)":

- P-0-3210, Safety technology control word
- P-0-3212, Safety technology control word, channel 1
- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation
- P-0-3233, Velocity threshold for safe standstill

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe stop 1 (Emergency stop)":

- F7040 Validation error parameterized - effective threshold
- F7050 Time for stopping process exceeded
- F8030 Safe stop 1 while drive enabled
- With the safety function "Safe stop 1 (Emergency stop)" activated, the display of the IndraDrive control panel shows "SS1ES".

Safety function

Basic principle

With the safety function "Safe stop 1 (Emergency stop)", the energy supply to the motor is safely interrupted. The motor cannot generate any torque/any force and therefore no dangerous movements.

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ Please observe the safety instructions in section "Notes on project planning".

Transition to the safe state

The type of transition to the safe state can be set in the parameter "P-0-3210, Safety technology control word". It is possible to select either "drive-controlled safety technology operation mode transitions" or "NC-controlled operation mode transitions" (see "Transition to safe state"). In both cases, the safety function "Safely-monitored stopping process" becomes active for transition (see "Safely-monitored stopping process").

☞ After successful transition to "Safe stop 1 (Emergency stop)", safety is only acknowledged if "control of a PLC" has been projected for the diagnostic output.

After successful transition to "Safe stop 1 (Emergency stop)" and with parameterization "control of a safety door", the safety door is only controlled if the mode selector is additionally actuated.

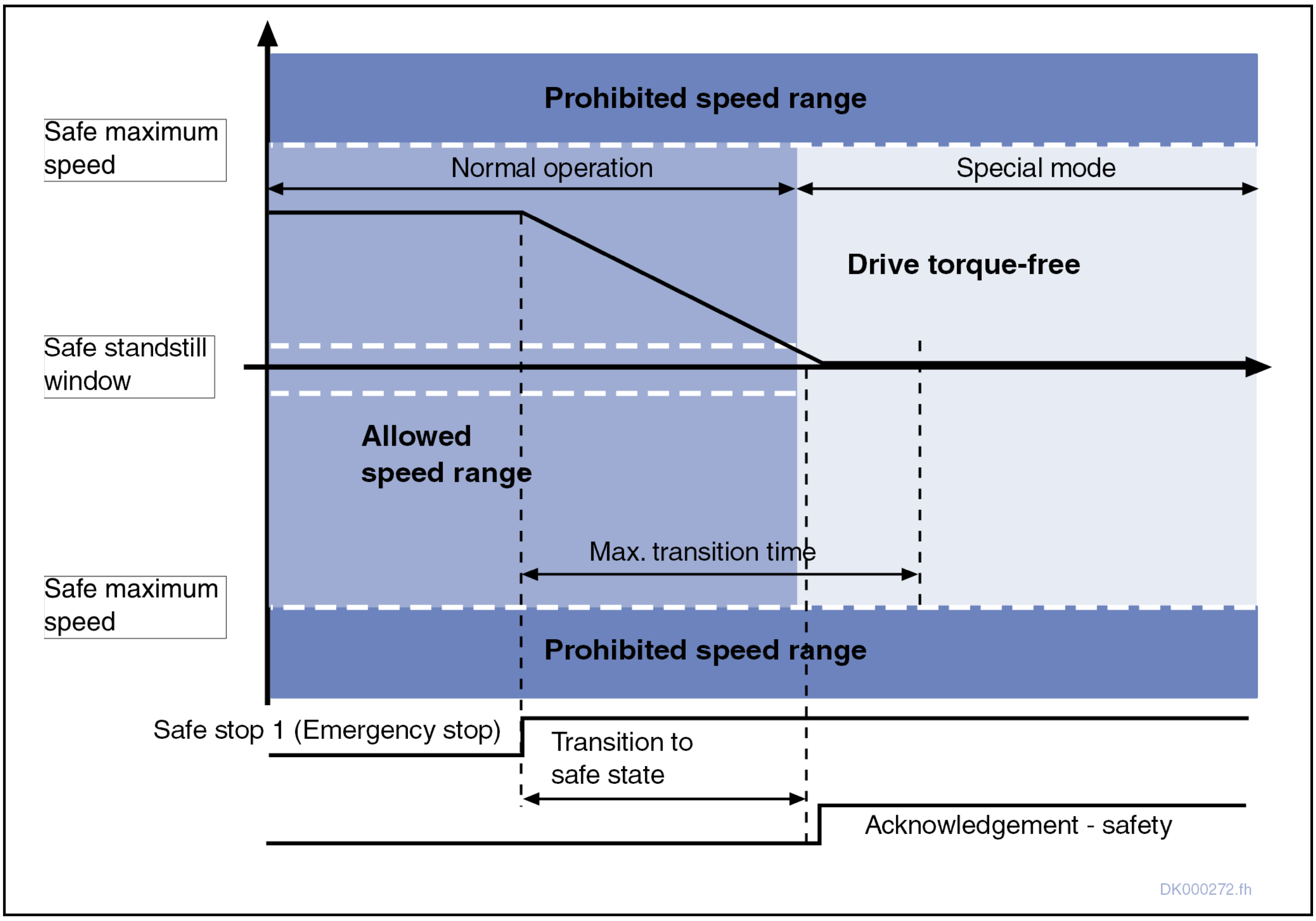


Fig. 6-15: Drive-controlled transition to "Safe stop 1 (Emergency stop)" from normal operation

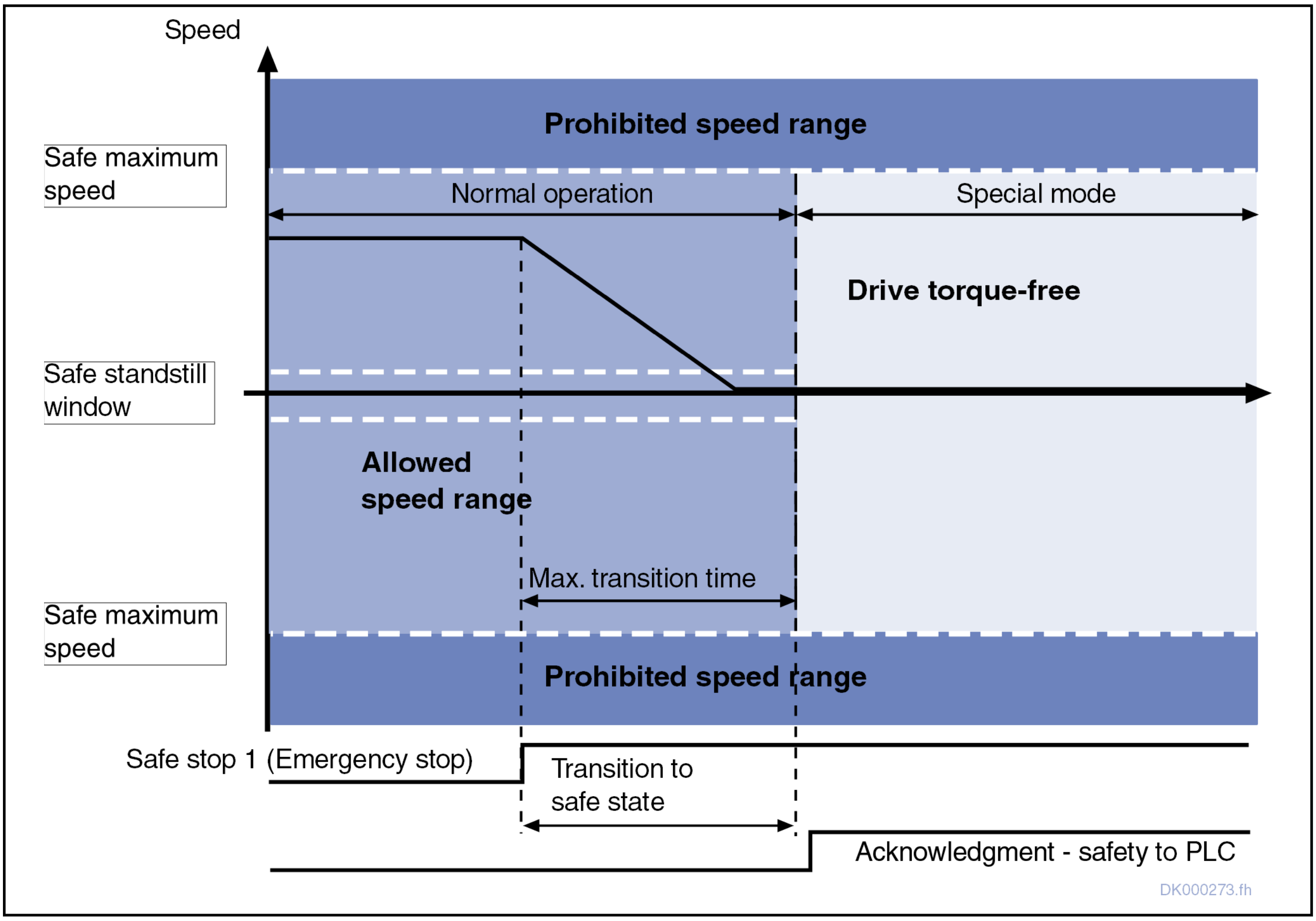


Fig. 6-16: NC-controlled transition to "Safe stop 1 (Emergency stop)" from normal operation

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ In "Safe stop 1 (Emergency stop)", the drive cannot generate any torque/any force and therefore no dangerous movements which has to be taken into account above all for vertical axes. Please observe the safety instructions in section "Notes on project planning".

Monitoring functions

If the safety function "Safe stop 1 (emergency stop)" has been activated and drive enable is set, the error "F8030 Safe stop 1 while drive enabled" is generated.

Terminating the safety function "Safe stop 1 (Emergency stop)"

The safety function "Safe stop 1 (Emergency stop)" can only be deselected by resetting the selection of "Safe stop 1 (Emergency stop)".

Notes on project planning

When using the safety function "Safe stop 1 (Emergency stop)", it is absolutely necessary to observe the following safety instructions:

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ If external force influences are to be expected with the safety function "Safe stop 1 (Emergency stop)", e.g. in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation. For such axes, Bosch Rexroth recommends using the safe braking and holding system.

⚠ WARNING **Injury and/or property damage caused by deviation from standstill position!**

⇒ Even if the control of the power section has been safely locked, momentary axis motion, depending on the number of poles of the motor, can be triggered, when two errors are occurring simultaneously in the power section with the voltage DC bus being active:

- Breakdown of a power semiconductor **and**
- Breakdown of another semiconductor

In this case, two of six semiconductors are affected in such a way that the motor shaft is aligning.

Synchronous motor example: In the case of a synchronous motor with 6 pole pairs, the motion can be a maximum of 30 degrees. For a directly driven ball screw, e.g. 20 mm per revolution, this corresponds to a one-time maximum linear motion of 1.67 mm.

When an asynchronous motor is used, the short circuits in two separate circuits of the power section have almost no effect, because the exciter field breaks down when the inverter is shut down and has completely died down after approx. 1 s.

6.3.5 Safe braking and holding system (SBS)

Brief description

The safety function Safe braking and holding system safely prevents unintended axis motion (e.g. of vertical axes), even if the drive is not in control. The safe holding of the axis is realized by two brakes which can be controlled independently of each other.

The function of the brakes should be cyclically checked.

⚠ WARNING **Serious injury caused by possible errors in the brake system during safe operation!**

⇒ The drive system resets the acknowledgment of safety of the axes. The user must take appropriate measures for personal protection.

Features

The safety function "Safe braking and holding system" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- The safe braking and holding system consists of two brakes which take effect independently of each other:

  - Brake 1: Only electrically releasing friction surface brakes allowed, such as the motor holding brake.
  - Brake 2: Redundant holding brake, designed either as external electrically releasing friction surface brake or as external electrically releasing, form-fitting brake.
- Redundant holding brake controlled via "control module (HAT)"
- Redundant holding of the axis also present after energy has been switched off (emergency stop, emergency off)
- Quick reaction on error: Escalation strategy with a total of three channels for deceleration
- Command "C5900 Command Resurfacing of redundant holding brake" is not accepted or executed when using a toothed brake

Pertinent parameters

The following parameters can be used in conjunction with the safety function "Safe braking and holding system":

- P-0-0525, Holding brake control word
- P-0-0539, Holding brake status word
- P-0-0540, Torque of motor holding brake
- P-0-0541, C2100 Holding system check command
- P-0-0542, C2000 Command Release motor holding brake
- P-0-0543, C3800 Command Apply motor holding brake
- P-0-0544, C3900 Command Holding brake resurfacing
- P-0-0545, Test torque for releasing motor holding brake
- P-0-0546, Starting torque for releasing motor holding brake
- P-0-0547, Nominal load of holding system
- P-0-0549, Oper. hours control section at last successful brake check
- P-0-0550, Time interval brake check
- P-0-0551, Current load torque
- P-0-3211, Safety technology I/O configuration list, channel 2
- P-0-3218, C3700 Command Manually unlocking the safety door
- P-0-3300, Redundant holding brake: Configuration
- P-0-3301, Redundant holding brake: Status word
- P-0-3302, SBS: Time interval brake check
- P-0-3303, SBS: Nominal load
- P-0-3304, SBS: Torque/force constant
- P-0-3306, SBS: Delay time motor holding brake
- P-0-3307, SBS: Safety technology - drive off delay time
- P-0-3310, SBS: Travel range brake check
- P-0-3311, SBS: Duration test torque injection brake check
- P-0-3313, C5800 Command Apply redundant holding brake
- P-0-3314, C5900 Command Resurfacing of redundant holding brake
- P-0-3315, C6200 Comm. Enabling SM without valid brake status

Additionally in MPx08 and above:

- P-0-3305, SBS: Safety technology drive On delay time
- P-0-3316, SBS: Test torque factor motor holding brake

- P-0-3317, SBS: Test torque factor redundant holding brake

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe braking and holding system":

- E3115 Prewarning, end of brake check time interval
- F3115 Brake check time interval exceeded
- E3116 Nominal load torque of holding system reached
- F3116 Nominal load torque of holding system exceeded
- F3122 SBS: System error
- F3123 SBS: Brake check missing
- F7051 Safely-monitored deceleration exceeded
- F8134 SBS: Fatal error
- C0256 Safety technology configuration error
- C2000 Command Release motor holding brake
- C2001 Command not enabled
- C2100 Command Holding system check
- C2101 Holding system check only possible with drive enable
- C2103 Motor holding brake: Torque too low
- C2104 Command execution impossible
- C2105 Load of holding system greater than test torque
- C2106 Test torque of holding system not reached
- C2107 Redundant holding brake: Torque too low
- C2108 Error when releasing the holding system
- C2109 SBS: Test torque invalid
- C3700 Command Manually unlocking the safety door
- C3701 Error when manually unlocking the safety door
- C3800 Command Apply motor holding brake
- C3900 Command Brake resurfacing
- C3901 Resurfacing of brake only possible with drive enable
- C3902 Error when resurfacing the brake
- C3903 Command execution impossible
- C5800 Command Apply redundant holding brake
- C5801 Command Apply redundant holding brake not possible
- C5900 Command Resurfacing of redundant holding brake
- C5901 Comm. Resurfacing of red. holding brake only possible AF
- C5902 Error when resurfacing redundant holding brake
- C5903 Command execution impossible
- C6200 Comm. Enabling SM without valid brake status
- C6201 Command execution impossible

Functional description

General information

The Safe braking and holding system consists of the motor holding brake, an external holding brake, called "redundant holding brake" in the following chapters, a control module for the redundant holding brake and the drive controller with the corresponding firmware.

NOTICE **Damage to the brake in the case of 24V loss**

24V loss causes the brake systems to be immediately applied. To avoid this, it is highly recommended to you use an independent power supply (UPS) for voltage buffering, especially for form-fitting brakes.

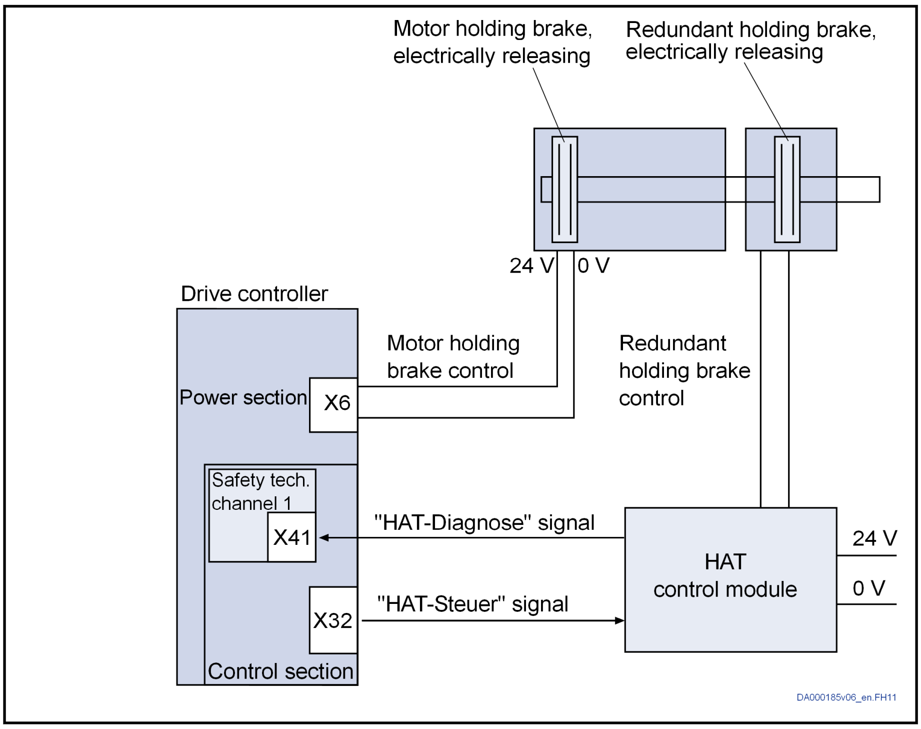


Fig. 6-17: System overview of the Safe braking and holding system

As motor holding brake, only an electrically releasing friction surface brake is allowed; it is controlled like a standard motor brake and can be designed as an **external** or as a **motor-integrated holding brake.**

Two designs are allowed for the redundant holding brake:

- External electrically releasing form-fitting brakes
- External electrically releasing friction surface brakes

The **redundant holding brake** can be mounted either on the motor side or on the load side. If the mounting position of the redundant holding brake is arbitrary, load-side mounting is preferred, as the remaining risk due to errors in the transmission path from motor to load is reduced in the case of load-side mounting. Control does not take place directly via the controller, but via the corresponding control module (HAT01.1-002-NNN-NN).

☞ It is not allowed to connect any additional switch contacts (e.g., a safety PLC) between the "HAT01.1" control module and the brake.

An **external brake** must at least comply with the specifications of the motor holding brake. Each of the two holding brakes must have been **sized such** that it can safely hold **the maximum weight of the load of the axis** (P-0-0547). For a point of reference for the sizing, see, for example, the Information

Sheet 5 of the "Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau" (Committee of experts for mechanical engineering, manufacturing systems, structural steel engineering) of the institution for statutory accident insurance and prevention ("Berufsgenossenschaft Metall Süd") ["Gravity-loaded axes (Vertical axes)", issue 02/2004]. The Information Sheet contains the following specification for the dimensioning of the brakes:

"The mechanical parts of power transmission and those of the safety devices shall be at least designed to withstand the occurring static and dynamic stresses at dual weight of the load."

Thus, there are the following possible combinations of the two brakes:

- The motor holding brake and the redundant holding brake are designed as electrically releasing friction surface brakes.
- The motor holding brake is designed as electrically releasing friction surface brake and the redundant holding brake is designed as electrically releasing, form-fitting brake.

Three operating states change by the use of the "Safe braking and holding system":

- The safety operating status "Safe stop 1" (SS1) becomes "Safe stop 1 (braked)" (SS1 B).
- The safety operating status "Safe stop 1 (Emergency stop)" (SS1ES) becomes "Safe stop 1 (braked Emergency stop)" (SS1 BES).
- The operating status "halt" (AH) becomes "braked halt" (GH).

Safe stop 1 (braked)

When the "Safe braking and holding system" is used, the axis always is in the safety operating status "Safe stop 1 (braked)" (SS1 B), when

- the "status of holding brake check" of both holding brakes, P-0-0539 and P-0-3301, is "carried out successfully",
- the special mode "Safe standstill" has been selected,
- the holding torques of both holding brakes take effect,
- standstill is detected,
- the feedback of the redundant holding brake is available and
- restart is successfully prevented.

In this state, the axis acknowledges safety.

In the parameter mode, the drive is in "Safe stop 1 (braked)-Parameterization" and in the case of error in "Safe stop 1 (braked)-Error". Safety is then acknowledged depending on several conditions (see "Acknowledgment of safety").

Safe stop 1 (braked Emergency stop)

When the "Safe braking and holding system" is used, the axis always is in the safety operating status "Safe stop 1 (braked Emergency stop)" (SS1 BES), when

- the "status of holding brake check" of both holding brakes, P-0-0539 and P-0-3301, is "carried out successfully",
- the special mode "Safe standstill" has been selected via the SS1 (Emergency stop) switch,
- the holding torques of both holding brakes take effect,
- standstill is detected,
- the feedback of the redundant holding brake is available and
- restart is successfully prevented.

Braked halt

In normal operation, the holding torques of both holding brakes also take effect to increase the machine safety. When the safe braking and holding system is used, this state is called "braked halt" (GH). In this state, the axis does not acknowledge safety.

> ☞ The "Safe braking and holding system" is always controlled in the case of error, independent of whether the axis is in normal operation or in special mode.
>
> In this case, an escalation strategy is carried out (see "Safety technology error reaction").

Measures to avoid states of torque disable

The user has to carry out or take into account the following measures to increase the availability or independence of drive control as "service braking device":

- Suppression of "torque disable without delay" by the "drive enable" bit in one of the following control words:
  - P-0-0116, Device control: Control word
  - S-0-0134, Master control word
  - P-0-4028, Device control word
  - P-0-4068, Field bus: Control word IO
  - P-0-4077, Field bus: Control word
- Suppression of application-side torque limitations (except for "P-0-0109, Torque/force peak limit"):
  - S-0-0082, Torque/force limit value positive
  - S-0-0083, Torque/force limit value negative
  - S-0-0092, Bipolar torque/force limit value

Risk analysis

For the risk analysis of an installation in which the safe braking and holding system is used, it is necessary to know how far the corresponding axis moves as a maximum in the case of error.

The greatest axis motion occurs, when

- the axis is in "Special mode Safe motion" (SMM) with downward travel direction and an F8xxx error occurs during this axis motion **and**
- the motor holding brake has been applied and no braking torque is generated **and**
- the redundant holding brake is applied and the axis decelerates until standstill has been reached.

The traveled distance is divided into two steps. In the first step, the axis falls down in a torque-free way (x_{free}) and in the second step, the axis is decelerated by the redundant holding brake (x_{decel}).

For the following calculations, we assume that the axis is a vertical axis with recirculating ball screw and directly connected motor. The friction which is present in the system is not taken into account, as it cannot be considered as being constant over the service life of such a mechanical system. Existing friction has a positive effect on the braking distance, i.e. the travel distance calculated below will in reality be shorter due to the existing friction.

$$t_{\text{error reaction}} = t_{\text{free}} + t_{\text{decel}}$$

$$t_{\text{free}} = \text{P-0-3306} + t_{\text{clamp, red}} + t_{\text{system}}$$

$$t_{\text{decel}} = -(((T \times t_{\text{free}}) / (T_L - T_{\text{red}})) + ((2\pi \times J \times (V_{\text{SMM}}/h)) / (T_L - T_{\text{red}})))$$
$$= ((T_L \times t_{\text{free}}) + ((2\pi \times J \times V_{\text{SMM}}/h)) / (T_{\text{red}} - T_L))$$

Legend:

$t_{\text{error reaction}}$: Total time of error reaction

t_{free}: Time during which axis is torque-free

t_{decel}: Deceleration time of axis

$t_{\text{clamp,red}}$: Clamping delay of redundant holding brake

t_{system}: Internal processing time of drive (typically 49 ms)

T_L: Load torque

T_{red}: Braking torque of redundant holding brake

J: Total inertia with relation to the motor shaft

h: Spindle lead

v_{SMM}: Parameterized velocity threshold for SMMx

Tab. 6-2: Calculating the error reaction time

$$x_{\text{error reaction}} = x_{\text{free}} + x_{\text{decel}}$$
$$=(v_{\text{SMM}} + ((T_L \times h \times t_{\text{free}}) / (4\pi \times J))) \times t_{\text{free}} + ½ \times (v_{\text{SMM}} + ((T_L \times h \times t_{\text{free}}) / (2\pi \times J))) \times t_{\text{decel}}$$
$$=(t_{\text{free}} + (t_{\text{decel}} / 2)) \times v_{\text{SMM}} + (t_{\text{free}} + t_{\text{decel}}) \times ((T_L \times h \times t_{\text{free}}) / (4\pi \times J))$$

Legend:

$x_{\text{error reaction}}$: Traveled distance of axis during error reaction

x_{free}: Traveled distance of axis while it is torque-free

x_{decel}: Traveled distance of axis while holding torque of the redundant holding brake takes effect

t_{free}: Time during which axis is torque-free

t_{decel}: Deceleration time of axis

T_L: Load torque

J: Total inertia with relation to the motor shaft

h: Spindle lead

v_{SMM}: Parameterized velocity threshold for SMMx

Tab. 6-3: Calculating the error reaction distance

Example:

When using a Rexroth motor with the order code MSK071D-300-NN-M1-UG2-NNNN, a spindle (40 mm diameter, 20 mm lead) and a redundant brake (26 Nm holding torque, 26 ms clamping delay), the error reaction distance is calculated as follows:

Data for exemplary calculation:
$d = 40\ \text{mm} = 0.04\ \text{m}$ $h = 20\ \text{mm} = 0.02\ \text{m}$ $t_L = 340\ \text{kg} \rightarrow T_L = 10.6\ \text{Nm}$ $T_{red} = 26\ \text{Nm}$ $t_{clamp,\ red} = 26\ \text{ms} = 0.026\ \text{s}$ $J = 0.011\ \text{kgm}^2$ $v_{SMM} = 2.0\ \text{m/min} \triangleq 0.0333\ \text{m/s}$ $\text{P-0-3306} = 35\ \text{ms} = 0.035\ \text{s}$ $t_{system} = 49\ \text{ms} = 0.049\ \text{s}$
Exemplary calculation: $t_{free} = \text{P-0-3306} + t_{clamp,\ red} + t_{system} = 110\ \text{ms} = 0.11\ \text{s}$ $t_{decel} = (T_L \times t_{free} + 2\pi \times J \times (V_{SMM}/h)) / (T_{red} - T_L) = 0.083\ \text{s} = 83\ \text{ms}$ $x_{error\ reaction} = (t_{free} + (t_{decel} / 2)) \times v_{SMM} + (t_{free} + t_{decel}) \times ((T_L \times h \times t_{frer}) / (4\pi \times J)) = 37.55\ \text{mm}$
Legend: $x_{error\ reaction}$: Traveled distance of axis during error reaction x_{free}: Traveled distance of axis while it is torque-free x_{decel}: Traveled distance of axis while holding torque of the redundant holding brake takes effect t_{free}: Time during which axis is torque-free t_{decel}: Deceleration time of axis T_L: Load torque T_{red}: Braking torque of redundant holding brake J: Total inertia with relation to the motor shaft h: Spindle lead v_{SMM}: Parameterized velocity threshold for SMMx

Tab. 6-4: Calculating the error reaction distance

This means that after an error was detected, the axis moves by a maximum of 37.55 mm before it is shut down.

Monitoring functions

The following monitoring functions are active with the safe braking and holding system:

- Monitoring of configuration errors
- Monitoring of the actual load torque
- Monitoring of the brake status

Monitoring of configuration errors

With active safety function "Safe braking and holding system", the following configuration restrictions are monitored via two channels at every change to the operating mode (OM):

- Torque disable should not have been configured as best possible deceleration (P-0-0119), because otherwise control would be deactivated regardless of the brake delay time.
- Torque disable should not have been configured as error reaction to F7 errors (P-0-3210), because otherwise control would be deactivated regardless of the brake delay time.

- NC or MLD error reaction should not be configured in P-0-0117.
- The motor holding brake should not have been configured as main spindle brake (P-0-0525), because in this case the brake is only applied at an actual velocity <10 rpm.

In the case of incorrect configuration setting, the command error "C0256 Safety technology configuration error" is generated.

Monitoring of the actual load torque

To exclude overload of the safe braking and holding system, the load torque of the axis is monitored via two channels during operation.

The prerequisites for monitoring are:

- Monitoring was not deactivated in P-0-3300.

  WARNING! Possible injury and property damage caused by overload of axis and brakes! By deactivating the load torque monitoring, it is no longer possible to detect overload of axis, holding brake and mechanical system.
- The drive is in control.
- Standstill is detected, i.e. the actual velocity is smaller than 5 to 20 rpm (depending on the encoder which is used).

The currently determined load torque is displayed in P-0-0551. Both safety technology channels monitor this value. If the value of P-0-0551 is above the parameterized nominal load of the holding system (P-0-3303), the warning "E3116 Nominal load torque of holding system reached" is generated. If the parameterized value of P-0-3303 is exceeded by the 1.3-fold value, the error "F3116 Nominal load torque of holding system exceeded" is generated.

Monitoring of the brake status

As long as the "status of holding brake check" (P-0-0539, P-0-3301) of one of the two brakes is "carried out without success", the axis does not acknowledge safety. The selection of the special mode is acknowledged with the error message "F3123 SBS: Brake check missing".

☞ If such states can occur at the installation in which the axis must be moved in special mode before the brake check, the axis can be moved under defined conditions via the command "C6200 Command Enabling SM without valid brake status" (see "Enabling the Special Mode Without Valid Brake Status") .

Acknowledgment of safety

In the following states, the axis acknowledges safety in conjunction with the safe braking and holding system:

Operating status	Brake status	Acknowledgment of safety
Normal operation	x	No
Safe stop 1 (braked)	Successful	Yes
Safe stop 1 (braked Emergency stop)	Successful	No
Safe stop 1 (braked)-Parameterization	Successful	Only when safety door had been opened in OM
	Not successful	No
Safe stop 1 (braked)-Error	Successful	Only with selection of special mode and without encoder error
	Not successful	No

Tab. 6-5: Acknowledgment of safety with the safe braking and holding system

Commissioning

⚠ WARNING **Dangerous movements! Danger to life, risk of injury, serious injury or property damage! Remaining risk due to errors in the brake system during safe operation. The acknowledgment of safety of the axes is removed!**

⇒ The user must take appropriate measures (e.g., warning, leave the working area)

When the safety function "Safe braking and holding system" (P-0-3300) is activated, the following inputs/outputs are permanently assigned:

- P-0-3301, bit 0 → output: X32.9
- P-0-3301, bit 0 → input: X32.8 (axis 2 of HMD type controllers)

☞ The diagnostic signal "HAT-Diagnose" (P-0-3211) has to be assigned to an input (I1n to I4n) on X41. It is recommended to use the input I4n (X41.7), because otherwise the connector wiring of X1 of the cable RKS0007 has to be changed.

Commissioning with deactivated safety technology

For initial commissioning, it is necessary to move the axis without active safety technology. When this is done, an existing redundant holding brake must be controlled. This operating status is called "setting-up mode".

⚠ WARNING **Injury caused by moving the axis without active safety technology during initial commissioning!**

Measures for personal protection must be taken, as long as safety technology is deactivated.

To set the axis to the setting-up mode, carry out the following steps:

- Safety technology must have been deactivated. If this is not the case, carry out the command "C7_2 Load defaults procedure command (load defaults procedure for safety technology)".
- The redundant holding brake has to be configured in P-0-3300.

Afterwards, the axis is in the setting-up mode and the redundant holding brake is controlled synchronously to the motor holding brake.

Double parameters

Apart from the "Safe braking and holding system", there is a non-safety-relevant holding brake check for Rexroth IndraDrive controllers. That is why some parameters have been implemented both as "normal" parameters (standard parameters) and as safety technology parameters.

Standard parameters	Safety technology parameter
S-0-0206, Drive on delay time	"P-0-3305, SBS: Safety technology drive On delay time" (MPx08 and above)
S-0-0207, Drive off delay time	P-0-3307, SBS: Safety technology - drive off delay time
P-0-0051, Torque/force constant	P-0-3304, SBS: Torque/force constant
P-0-0547, Nominal load of holding system	P-0-3303, SBS: Nominal load
P-0-0550, Time interval brake check	P-0-3302, SBS: Time interval brake check

Tab. 6-6: Double parameters

☞ The parameters contained in the table should be written with identical values, unless a good reason prohibits this.

Safety technology error reaction

When the integrated safety technology is used with activated safe braking and holding system, the drive is shut down in the case of error; when this happens, an escalation strategy is run. This strategy is used to make sure that the drive is shut down in an optimum way and that wear of existing holding brakes, as well as load of the mechanical system, are minimized. According to the initial situation, shutdown in the case of error takes place on several levels. Each of the levels is monitored via two channels.

Error reaction

Normally, the escalation strategy is not run completely; this means that depending on the currently present error message and the resulting error reaction, the drive jumps to the corresponding escalation level. This can be one of the following levels:

- Escalation strategy, level 1: Velocity command value reset with ramp and filter
- Escalation strategy, level 2: Velocity command value reset at the torque limit
- Escalation strategy, level 3: Torque disable and control of the motor holding brake
- Escalation strategy, level 6: Control of the motor holding brake and of the redundant holding brake without trend monitoring

On level 6 of the escalation strategy, the axis is shut down with the mechanisms used on this level and afterwards both holding brakes are applied.

Escalation strategy

Within the individual levels of the escalation strategy, the effectiveness of the escalation level is monitored via dual-channel, parameterizable trend monitoring. When the trend monitoring triggers and thereby has detected that the axis cannot be decelerated in the desired time / the desired distance, the error reaction is taken to the next escalation level until the axis has been decelerated.

The figure below shows the escalation strategy with its individual levels:

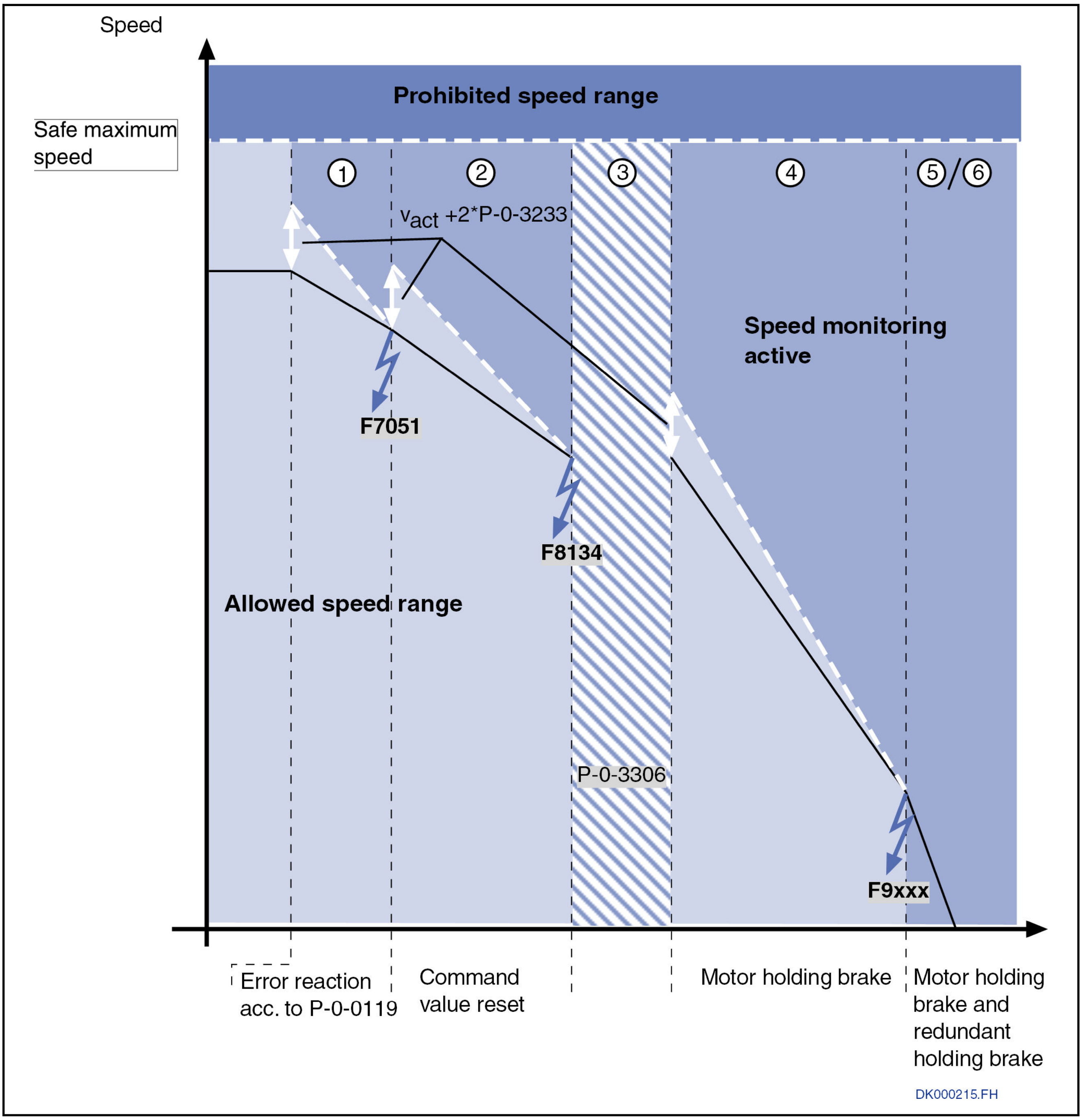


Fig. 6-18: Safety technology error reaction, escalation strategy

Escalation strategy, level 1

(Velocity) command value reset with ramp and filter

Level 1 of the escalation strategy is activated under the following conditions:

- Parameterized best possible deceleration (P-0-0119) with velocity command value reset with ramp and filter **and**
  - "drive off" **or**
  - F2, F3 or F4 error **or**
  - Drive-controlled transition to the "Special mode safe standstill" (SS1ES, SS1 B, SS1 BES, SS1, SS2, SS1 B error)

The drive is shut down with the values parameterized in S-0-0372 and S-0-0349. Safety technology trend monitoring takes place with the ramp parameterized in P-0-3282. If shutdown is not successful, i.e. trend monitoring triggers, the error F7051 is generated and switching to the next level of the escalation strategy takes place.

Escalation strategy, level 2

(Velocity) command value reset at the torque limit

Level 2 of the escalation strategy is activated under the following conditions:

- Parameterized best possible deceleration (P-0-0119) with velocity command value reset **and**
  - "drive off" **or**
  - F2, F3 or F4 error **or**
  - Drive-controlled transition to the special mode standstill (SS1ES, SS1 B, SS1 BES, SS1, SS2, SS1 B error) **or**
  - F6 or F7 error

The drive is shut down taking the torque limit value into account. Safety technology trend monitoring takes place with the ramp parameterized in P-0-3282. If shutdown is not successful, i.e. trend monitoring triggers, the error F8134 is generated and switching to the next level of the escalation strategy takes place.

Escalation strategy, level 3

Torque disable and control of the motor holding brake

Level 3 of the escalation strategy is activated under the following condition:

- Previous escalation levels were unsuccessful

The drive applies the motor holding brake and switching to escalation level 4 takes place after the time parameterized in P-0-3306 is over.

Escalation strategy, level 4

Holding torque of motor holding brake takes effect

Level 4 of the escalation strategy is activated under the following condition:

- Level 3 of the escalation strategy was run

The drive is shut down by the applied motor holding brake. Safety technology trend monitoring takes place with the ramp parameterized in P-0-3282. If shutdown is not successful, i.e. trend monitoring triggers, switching to the next level of the escalation strategy takes place before standstill of the axis.

Escalation strategy, level 5

Control of redundant holding brake

Level 5 of the escalation strategy is activated under the following condition:

- Level 4 of the escalation strategy was run **or**
- trend monitoring of level 4 has triggered

The drive is shut down by applying the motor holding brake and the redundant holding brake.

Escalation strategy, level 6

Control of the motor holding brake and of the redundant holding brake without trend monitoring

Level 6 of the escalation strategy is activated under the following condition:

- F9xxx error

The drive torque is disabled and the drive is shut down by applying the motor holding brake and the redundant holding brake.

6.4 Safety functions in special mode "Safe motion" (SMM)

6.4.1 Safely-limited speed (SLS)

Brief description

In the case of the safety function "Safely-limited speed", dual-channel monitoring prevents the drive from exceeding the preset velocity limit value (P-0-3244, P-0-3254, P-0-3264, P-0-3274); the effective threshold can be selected via two additional safety switches (S1, S2).

☞ Using the safety function "Safely-limited speed" requires the optional safety technology module "S2" which can be selected as configuration for the control sections **CSH01.1 or CSH01.3** (ADVANCED) and **CDB01.1** (BASIC).

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

Please observe the safety instructions in the chapter "Commissioning the safety technology".

Features

The safety function "Safely-limited speed" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- Dual-channel monitoring for exceeding the velocity limit values (P-0-3244, P-0-3254, P-0-3264, P-0-3274); when a velocity limit value is exceeded, the drive switches off with the error message "F7013 Safely-limited speed exceeded".
- The safety function is always active when special mode "Safe motion" is selected.
- The safety function "Safely-limited speed" can be combined with the other safety functions of the special mode "Safe motion".
- The special mode "Safe motion" with the safety function "Safely-limited speed" is selected by actuating an enabling control and the mode selector.
- The activation time of the enabling control which can be set is monitored.

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safely-limited speed":

- P-0-3210, Safety technology configuration
- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation
- P-0-3222, Max. Activation time of enabling control
- P-0-3240, Configuration of safe motion 1
- P-0-3244, Safely-limited speed 1
- P-0-3250, Configuration of safe motion 2
- P-0-3254, Safely-limited speed 2
- P-0-3260, Configuration of safe motion 3
- P-0-3264, Safely-limited speed 3

- P-0-3270, Configuration of safe motion 4
- P-0-3274, Safely-limited speed 4
- P-0-3239, Configuration of global safety technology functions
- P-0-3246, Max. activation time of enabling control 1
- P-0-3256, Max. activation time of enabling control 2
- P-0-3266, Max. activation time of enabling control 3
- P-0-3276, Max. activation time of enabling control 4

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safely-limited speed":

- F3142 Activation time of enabling control exceeded
- F7013 Safely-limited speed exceeded
- F7040 Validation error parameterized - effective threshold
- With motion monitoring activated, the display of the IndraDrive control panel shows "SMM".

Safety function

Selecting the function

The safety function "Safely-limited speed" becomes active by selecting the special mode "Safe motion".

Safe motion can be selected via

- Digital inputs/outputs for both safety channels
- Digital inputs/outputs of the optional safety technology module "S2" for safety channel 2 and master communication (SERCOS, PROFIBUS) for safety channel 1
- PROFIBUS (or PROFIsafe)

For transition from normal operation / special mode to the safe state, there is one programmable time available for each kind of transition:

- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation

After the respective tolerance time is over, velocity monitoring is activated.

Monitoring functions

In the case of the safety function "Safely-limited speed", dual-channel monitoring prevents the drive from exceeding the preset velocity limit values (P-0-3244, P-0-3254, P-0-3264, P-0-3274).

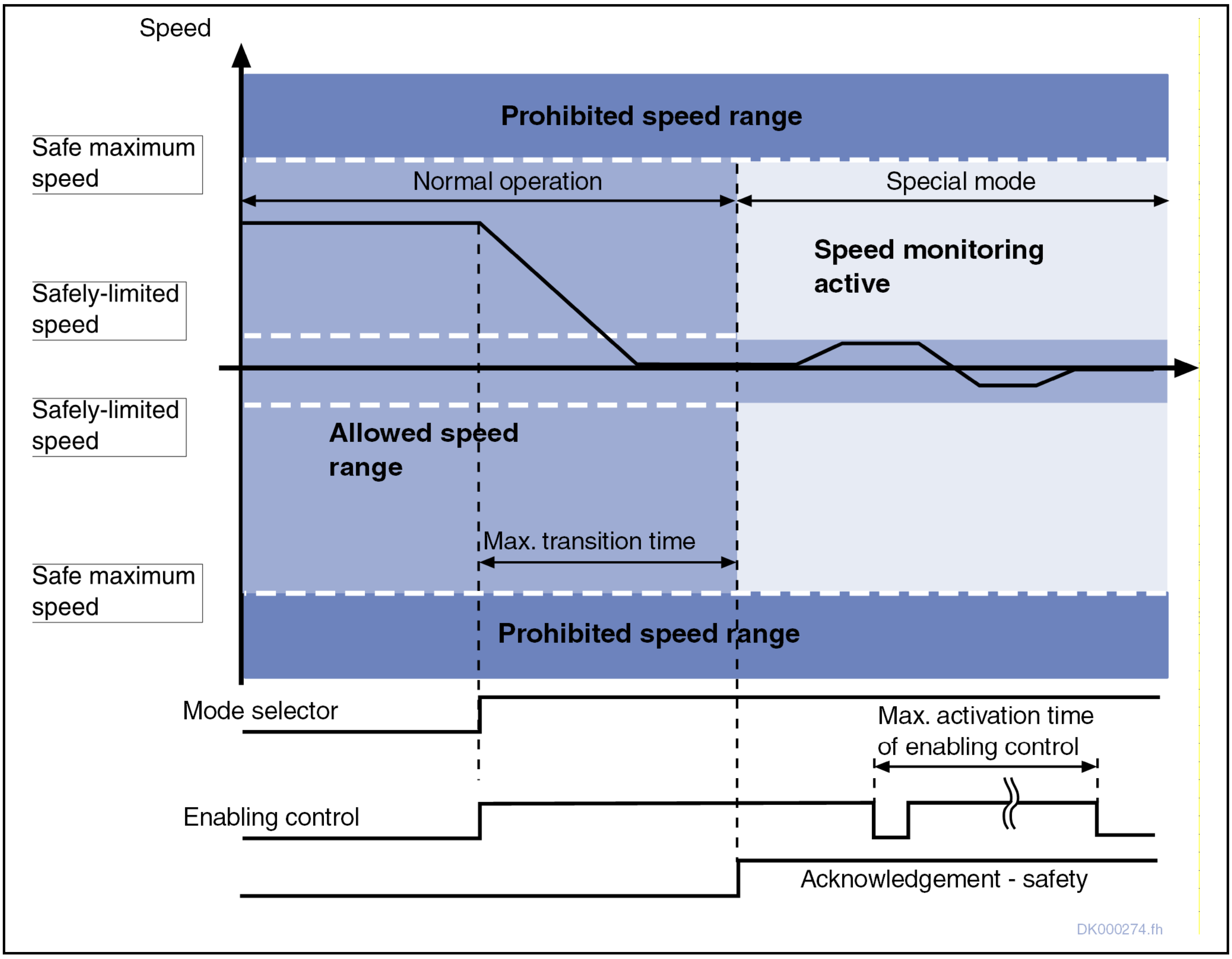


Fig. 6-19: |V_act| < safely-limited speed (NC-controlled transition to Safe motion from normal operation)

When the actual velocity is outside of the respective velocity limit value (P-0-3244, P-0-3254, P-0-3264, P-0-3274), the error "F7013 Safely-limited speed exceeded" is generated by the drive and the drive is shut down.

☞ After the safety technology has been activated, the velocity limit values (P-0-3244, P-0-3254, P-0-3264, P-0-3274) are write-protected with "P-0-3206, Safety technology password" and cannot be changed by unauthorized persons.

The status of the safety technology password can be seen in "P-0-3207, Safety technology password level".

The special mode "Safe motion" with the safety function "Safely-limited speed" is selected by actuating an enabling control and the mode selector. The activation time of the enabling control is cyclically monitored; it can be set using "P-0-3222, Max. activation time of enabling control". If this time is exceeded, the error message "F3142 Activation time of enabling control exceeded" is generated.

Individual activation times of enabling control are possible for the special modes "Safe motion". For commissioning, it is possible to select in "P-0-3239, Configuration of global safety technology functions" whether a common maximum activation time of enabling control (P-0-3222) is active for all special modes "Safe motion", or whether an individual activation time of enabling control (P-0-3246, P-0-3256, P-0-3266, P-0-3276) is active for each special mode "Safe motion 1..4".

⚠ WARNING

Dangerous movements!

Danger to life, risk of injury, serious injury or property damage by switching off the monitoring of activation time!

You can do without the monitoring of the activation time, if it is not common practice to use an enabling control in your industrial sector and if constant motion does not represent any danger.

The machine manufacturer is responsible for the monitoring of the activation time and his risk analysis has to show his responsibility.

"P-0-3222, Max. activation time of enabling control"="0" deactivates the time monitoring of the special mode "safe motion"; this also applies to the individual activation times of enabling control P-0-3246, P-0-3256, P-0-3266 and P-0-3276.

Selecting the effective limit value

Using two additional safety switches (S1, S2), the four different "Safe motions" (SMM) can be selected with the corresponding velocity limit values:

- S2="0", S1="0": SMM1 ("P-0-3244, Safely-limited speed 1" takes effect)
- S2="0", S1="1": SMM2 ("P-0-3254, Safely-limited speed 2" takes effect)
- S2="1", S1="0": SMM3 ("P-0-3264, Safely-limited speed 3" takes effect)
- S2="1", S1="1": SMM4 ("P-0-3274, Safely-limited speed 4" takes effect)

Notes on utilization

When using the safety function "Safely-limited speed", it is absolutely necessary to observe the following safety instructions:

⚠ DANGER

Lethal injury and/or property damage caused by unintended axis motion!

⇒ If external force influences are to be expected with the safety function "Safely-limited speed", e.g. in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation.

⚠ WARNING

Injury and/or property damage caused by deviation from standstill position!

⇒ When using the safely-limited speed for axes with external force influences, error situations (e.g., mains failure, controller defect) can occur in which the drive controller can no longer keep the axis in position. In this case, the axis must be kept in position by additional measures (e.g. mechanical brake). In the time between the occurrence of the error and the triggering of the "additional holding device", axis motion can occur. This has to be taken into account for the risk assessment of the installation.

For such axes, Bosch Rexroth recommends using the safe braking and holding system.

Values for "Safely-limited speed"

In accordance with the Machinery Directive [98/37/EC or 2006/42/EC (after 2009-12-29)], the machine manufacturer has to carry out a risk analysis or hazard analysis and afterwards a risk assessment. With these data, the values for limited speeds have to be determined.

The following list contains guide values for different types of machines (excerpt from standards and working papers on safety measures for special mode). The abbreviation "SLS" means "Safely-limited speed", the abbreviation "SLI" means "Safely-limited increment".

Machining centers

- Axes: SLS=2 m/min + hold-to-run control
- Spindle: SLS=nn rpm + hold-to-run control + enabling control (choose nn in such a way that standstill is reached after 2 revolutions)

Automatic lathes

- Axes: SLS=2 m/min + hold-to-run control, SLI=6 mm + hold-to-run control
- Spindle: SLS=50 rpm (1 rps) + hold-to-run control + enabling control

Drilling and milling machines

- Axes: SLS=2 m/min + hold-to-run control
- Spindle: SLS=nn rpm + hold-to-run control + enabling control (choose nn in such a way that standstill is reached after 2 revolutions)

Robots

- SLS=15 m/min + hold-to-run control

Automated manufacturing systems

- SLS=2 m/min (15 m/min) + hold-to-run control + emergency stop

Printing and paper converting machines

- General: SLI=25 mm+ hold-to-run control - **or** - SLS=5 m/min (max. 10 m/min) + hold-to-run control
- "In particular": SLI=75 mm+ hold-to-run control - **or** - SLS=5 m/min (max. 10 m/min) + hold-to-run control

Safely-monitored transient oscillation (SMO)

Brief description

To take transient oscillation processes into account, another monitoring variant, the "Safely-monitored transient oscillation" is provided **with firmware MPx-08VRS and above** within the scope of the safety function "Safely-limited speed (SLS)".

In the case of "Safely-monitored transient oscillation", dual-channel monitoring prevents the drive from exceeding the preset velocity limit value (P-0-3247, P-0-3257, P-0-3267, P-0-3277) for more than a preset time (P-0-3248, P-0-3258, P-0-3268, P-0-3278).

Using of two additional safety switches (S1, S2), up to four parameter sets for the special mode "Safe motion" can be selected.

☞ Using the safety function "Safely-limited speed" requires the optional safety technology module "S2" which can be selected as configuration for the control sections **CSH01.1 or CSH01.3** (ADVANCED) and **CDB01.1** (BASIC).

⚠ WARNING **Dangerous movements!**

Danger to life, risk of injury, serious injury or property damage, because the monitoring function is switched off with a delay!

When using the safety function "Safely-monitored transient oscillation", it is necessary to take into account that exceeding the parameterized "Safely-reduced speed" (P-0-3247, P-0-3257, P-0-3267, P-0-3277) might be recognized as a regular "transient oscillation" in the case of error. In this case, the error reaction will only be triggered after the "Safely-limited speed" (P-0-3244, P-0-3254, P-0-3264, P-0-3274) has been exceeded. This must be taken into account in the risk analysis of the machine.

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

Please observe the safety instructions in the chapter "Commissioning the safety technology".

Features

The "Safely-monitored transient oscillation" has the following features:

- Is available with the firmware MPx-08VRS and above
- Is active when the special mode "Safe motion" is selected, if it has been parameterized for this mode
- Can be used together with other safety functions of the special mode "Safe motion"
- Is selected by activating an enabling control and the mode selector
- When the actual velocity value exceeds the velocity limit value after the tolerance time for overshooting is over, the drive switches off with the error message "F7014 Timeout safely-monitored transient oscillation"

Pertinent parameters

The following parameters are used in conjunction with the "Safely-monitored transient oscillation":

- P-0-3240, Configuration of safe motion 1
- P-0-3244, Safely-limited speed 1
- P-0-3247, Safely-reduced speed 1
- P-0-3248, Tolerance time 1 for overshooting
- P-0-3250, Configuration of safe motion 2
- P-0-3254, Safely-limited speed 2
- P-0-3257, Safely-reduced speed 2
- P-0-3258, Tolerance time 2 for overshooting
- P-0-3260, Configuration of safe motion 3
- P-0-3264, Safely-limited speed 3
- P-0-3267, Safely-reduced speed 3
- P-0-3268, Tolerance time 3 for overshooting
- P-0-3270, Configuration of safe motion 4
- P-0-3274, Safely-limited speed 4
- P-0-3277, Safely-reduced speed 4
- P-0-3278, Tolerance time 4 for overshooting

Pertinent diagnostic messages

The following diagnostic message can be generated in conjunction with the "Safely-monitored transient oscillation":

- F7014 Timeout safely-monitored transient oscillation

With motion monitoring activated, the display of the IndraDrive control panel shows "SMM".

Safety function

Selecting the function

The "Safely-monitored transient oscillation" becomes active by selecting the special mode "Safe motion".

Monitoring functions

In the case of "Safely-monitored transient oscillation", dual-channel monitoring prevents the drive from exceeding the preset velocity limit value (P-0-3247, P-0-3257, P-0-3267, P-0-3277) for more than a preset time (P-0-3248, P-0-3258, P-0-3268, P-0-3278).

The velocity limit value has to be smaller than the value of the safely-limited speed (P-0-3244, P-0-3254, P-0-3264, P-0-3274) parameterized in the selected special mode.

When the parameterized velocity limit value (P-0-3247, P-0-3257, P-0-3267, P-0-3277) is exceeded for the first time, the parameterized time window of the allowed time (P-0-3248, P-0-3258, P-0-3268, P-0-3278) is opened. After the parameterized time is over, dual-channel monitoring takes place to make sure that velocity is below the parameterized velocity limit value; otherwise, the drive generates the error "F7014 Timeout safely-monitored transient oscillation". Afterwards, it is immediately possible to exceed the velocity limit value again. The time window will then be activated again. Retriggering during the running time window is impossible.

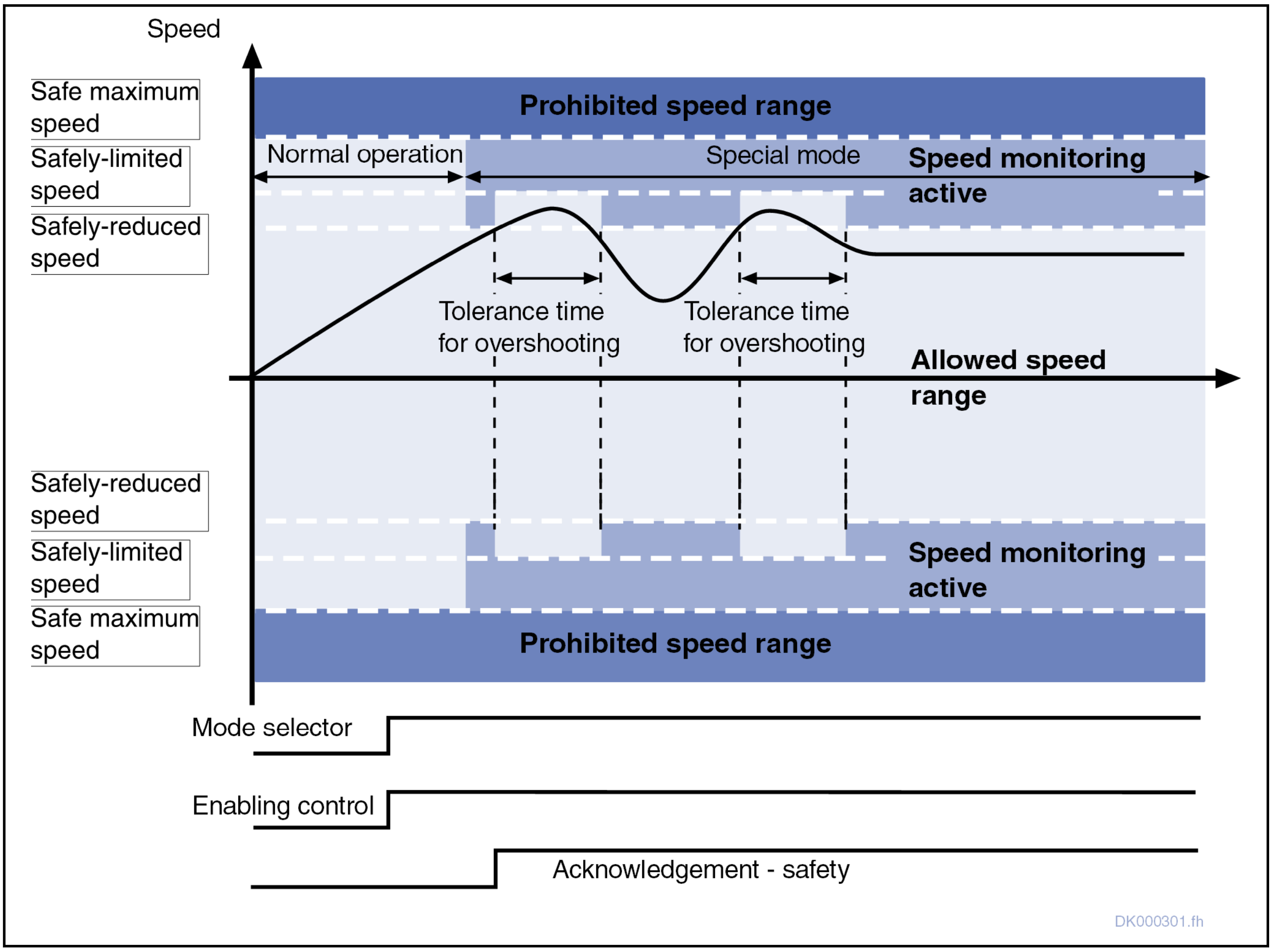


Fig. 6-20: Safely-monitored transient oscillation

☞ The velocity limit values (P-0-3247, P-0-3257, P-0-3267 and P-0-3277) and the tolerance times (P-0-3248, P-0-3258, P-0-3268, P-0-3278) are write-protected with "P-0-3206, Safety technology password" after the safety technology has been activated and cannot be changed by unauthorized persons.

The status of the safety technology password can be seen in "P-0-3207, Safety technology password level".

The special mode "Safe motion" with the safety function "Safely-monitored transient oscillation" is selected by actuating an enabling control and the mode selector. The activation time of the enabling control is cyclically monitored; it can be set using "P-0-3222, Max. activation time of enabling control". If this time is exceeded, the error message "F3142 Activation time of enabling control exceeded" is generated.

Individual activation times of enabling control are possible for the special modes "Safe motion". For commissioning, it is possible to select in "P-0-3239, Configuration of global safety technology functions" whether a common maximum activation time of enabling control (P-0-3222) is active for all special modes "Safe motion", or whether an individual activation time of enabling control (P-0-3246, P-0-3256, P-0-3266, P-0-3276) is active for each special mode "Safe motion 1..4".

⚠ WARNING

Dangerous movements!

Danger to life, risk of injury, serious injury or property damage by switching off the monitoring of activation time!

You can do without the monitoring of the activation time, if it is not common practice to use an enabling control in your industrial sector and if constant motion does not represent any danger.

The machine manufacturer is responsible for the monitoring of the activation time and his risk analysis has to show his responsibility.

"P-0-3222, Max. activation time of enabling control"="0" deactivates the time monitoring of the special mode "safe motion"; this also applies to the individual activation times of enabling control P-0-3246, P-0-3256, P-0-3266 and P-0-3276.

Selecting the effective limit value

Using two additional safety switches (S1, S2), the four different "Safe motions" (SMM) can be selected with the corresponding velocity limit values and tolerance times:

- S2="0", S1="0": SMM1 ("P-0-3247, Safely-reduced speed 1" and "P-0-3248, Tolerance time 1 for overshooting" take effect)
- S2="0", S1="1": SMM2 ("P-0-3257, Safely-reduced speed 2" and "P-0-3258, Tolerance time 2 for overshooting" take effect)
- S2="1", S1="0": SMM3 ("P-0-3267, Safely-reduced speed 3" and "P-0-3268, Tolerance time 3 for overshooting" take effect)
- S2="1", S1="1": SMM4 ("P-0-3277, Safely-reduced speed 4" and "P-0-3278, Tolerance time 4 for overshooting" take effect)

6.4.2 Safe direction (SDI)

Brief description

The safety function "Safe direction" ensures that motion is only possible in one direction.

Using two additional safety switches (S1, S2), up to four parameter sets for the special mode "Safe motion" can be selected.

☞ Using the function "Safe direction" requires the optional safety technology module "S2" which can be selected as configuration for the control sections **CSH01.1 or CSH01.3** (ADVANCED) and CDB01.1 (BASIC).

☞ In addition to the function "Safe direction", the safety function "Safely-limited speed" is active.

Features

The safety function "Safe direction" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- The direction of motion is monitored (P-0-3240, P-0-3250, P-0-3260, P-0-3270 und P-0-3232).
- The safety function "Safe direction" is active when the special mode "Safe motion" is selected, if it has been parameterized for this mode.
- The safety function "Safe direction" can be used together with the other safety functions of the special mode "Safe motion".

- The special mode "Safe motion" with the safety function "Safe direction" is selected by actuating an enabling control and the mode selector.
- For transition from normal operation / special mode to the safe state there is one programmable time available for each kind of transition.
- When the monitor for the direction of motion is triggered, this causes an error reaction which shuts down the drive system. The corresponding error message is "F7031 Incorrect direction of motion".

Pertinent parameters

The following parameters can be used in conjunction with the safety function "Safe direction":

- P-0-3210, Safety technology configuration
- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation
- P-0-3222, Max. Activation time of enabling control
- P-0-3232, Standstill window for safe direction
- P-0-3239, Configuration of global safety technology functions
- P-0-3240, Configuration of safe motion 1
- P-0-3244, Safely-limited speed 1
- P-0-3246, Max. Activation time of enabling control 1
- P-0-3250, Configuration of safe motion 2
- P-0-3254, Safely-limited speed 2
- P-0-3256, Max. Activation time of enabling control 2
- P-0-3260, Configuration of safe motion 3
- P-0-3264, Safely-limited speed 3
- P-0-3266, Max. Activation time of enabling control 3
- P-0-3270, Configuration of safe motion 4
- P-0-3274, Safely-limited speed 4
- P-0-3276, Max. Activation time of enabling control 4

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe direction":

- F7031 Incorrect direction of motion
- F3142 Activation time of enabling control exceeded
- F7013 Safely-limited speed exceeded
- With motion monitoring activated, the display of the IndraDrive control panel shows "SMM".

Safety function

Selecting the function

The safety function "Safe direction" becomes active by selecting the special mode "Safe motion".

Safe motion can be selected via

- Digital inputs/outputs for both safety channels
- Digital inputs/outputs of the optional safety technology module "S2" for safety channel 2 and master communication (SERCOS, PROFIBUS) for safety channel 2 or
- PROFIBUS (or PROFIsafe).

For transition from normal operation / special mode to the safe state, there is one programmable time available for each kind of transition:

- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation

After the respective tolerance time is over, the velocity monitoring and the monitoring of the direction of motion are activated (dual-channel monitoring).

Monitoring functions

In the case of the safety function "Safe direction", dual-channel monitoring makes sure that the drive ...

- ...does not exceed the preset velocity limit values (P-0-3244, P-0-3254, P-0-3264, P-0-3274) in the enabled direction of motion, otherwise the drive generates the error "F7013 Safely-limited speed exceeded".
- ...only moves in the enabled direction of motion (cf. P-0-3240, P-0-3250, P-0-3260, P-0-3270) or does not exceed "P-0-3232, Standstill window for safe direction" when moving in the non-enabled direction of motion, otherwise the drive generates the error "F7031 Incorrect direction of motion".

☞ The direction of motion has to be set in the corresponding control word:

- P-0-3240, Configuration of safe motion 1
- P-0-3250, Configuration of safe motion 2
- P-0-3260, Configuration of safe motion 3
- P-0-3270, Configuration of safe motion 4

☞ The velocity limit values P-0-3244, P-0-3254, P-0-3264 and P-0-3274, as well as the control words / configuration parameters P-0-3240, P-0-3250, P-0-3260 and P-0-3270 and "P-0-3232, Standstill window for safe direction" are write-protected with "P-0-3206, Safety technology password" after the safety technology has been activated and cannot be changed by unauthorized persons.

The status of the safety technology password can be seen in "P-0-3207, Safety technology password level".

The special mode "Safe motion" with the safety function "Safe direction" is selected by actuating an enabling control and the mode selector. The activation time of the enabling control (P-0-3222, Max. activation time of enabling control) can be parameterized and is cyclically monitored. If this time is exceeded, the error message "F3142 Activation time of enabling control exceeded" is generated.

⚠ WARNING

Dangerous movements!

Danger to life, risk of injury, serious injury or property damage by switching off the monitoring of activation time!

You can do without the monitoring of the activation time, if it is not common practice to use an enabling control in your industrial sector and if constant motion does not represent any danger.

The machine manufacturer is responsible for the monitoring of the activation time and his risk analysis has to show his responsibility.

"P-0-3222, Max. activation time of enabling control"="0" deactivates the time monitoring of the special mode "safe motion"; this also applies to the individual activation times of enabling control P-0-3246, P-0-3256, P-0-3266 and P-0-3276.

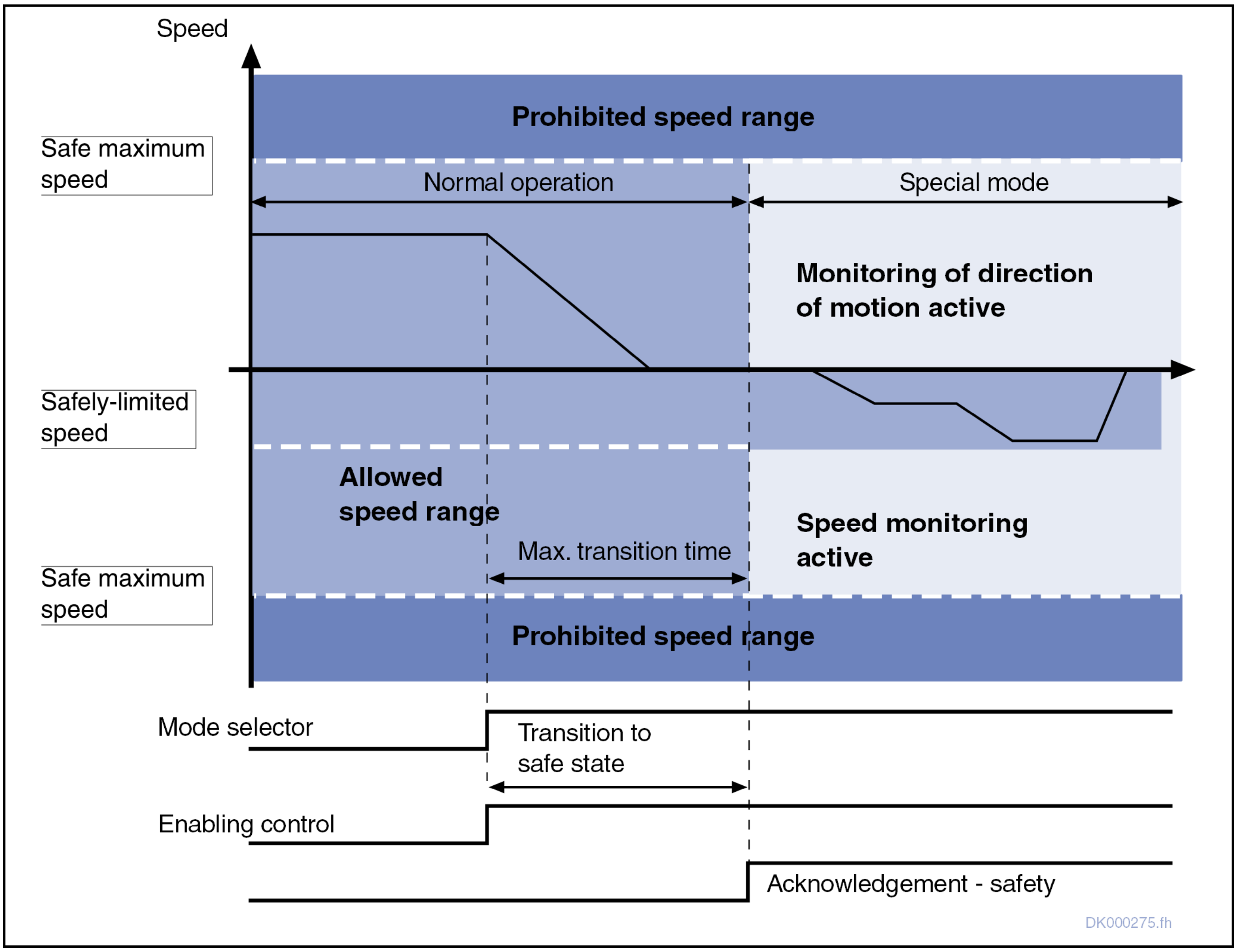


Fig. 6-21: Safe direction (NC-controlled transition to Safe motion from normal operation)

Selecting the effective limit value

Using two additional safety switches (S1, S2), the four different "Safe motions" (SMM) can be selected with the corresponding velocity limit values and directions of motion:

- S2="0", S1="0": SMM1 ("P-0-3240, Configuration of safe motion 1" and "P-0-3244, Safely-limited speed 1" take effect)

- S2="0", S1="1": SMM2 ("P-0-3250, Configuration of safe motion 2" and "P-0-3254, Safely-limited speed 2" take effect)
- S2="1", S1="0": SMM3 ("P-0-3260, Configuration of safe motion 3" and "P-0-3264, Safely-limited speed 3" take effect)
- S2="1", S1="1": SMM4 ("P-0-3270, Configuration of safe motion 4" and "P-0-3274, Safely-limited speed 4" take effect)

Notes on commissioning

In preparation

6.4.3 Safely-limited increment (SLI)

Brief description

In the case of the safety function "Safely-limited increment", the dual-channel monitoring prevents the drive from moving by more than one maximum increment. In addition, the safety function "Safely-limited speed" is always active. By means of two additional safety switches (S1, S2), up to four parameter sets for the special mode "Safe motion" can be selected.

☞ Using the safety function "Safely-limited increment" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

Within the position window (maximum increment) it is possible to move in both directions.

To define a new position window it is necessary

- to either leave the special mode "Safe motion" and select it again or
- to change to another parameter set of Safe motion and then go back again.

☞ In the case of transition to different operation (special mode or normal operation), the mode selected before and the corresponding monitoring functions are active until the end of the transition process.

Features

The safety function "Safely-limited increment" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- The maximum increment (P-0-3243, P-0-3253, P-0-3263, P-0-3273) is monitored.
- The safety function is active when Safe motion is selected, if it has been parameterized for this mode.
- The safety function "Safely-limited increment" can be combined with the other safety functions of the special mode "Safe motion".
- The special mode "Safe motion" with the safety function "Safely-limited increment" is selected by actuating an enabling control and the mode selector.
- When a monitor is triggered, this causes an error reaction which shuts down the drive system. The corresponding error message is "F7010 Safely-limited increment exceeded".

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safely-limited increment":

- P-0-3210, Safety technology configuration
- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation
- P-0-3222, Max. Activation time of enabling control
- P-0-3239, Configuration of global safety technology functions
- P-0-3240, Configuration of safe motion 1
- P-0-3243, Safely-limited increment 1
- P-0-3244, Safely-limited speed 1
- P-0-3246, Max. activation time of enabling control 1
- P-0-3250, Configuration of safe motion 2
- P-0-3253, Safety-limited increment 2
- P-0-3254, Safely-limited speed 2
- P-0-3256, Max. activation time of enabling control 2
- P-0-3260, Configuration of safe motion 3
- P-0-3263, Safety-limited increment 3
- P-0-3264, Safely-limited speed 3
- P-0-3266, Max. activation time of enabling control 3
- P-0-3270, Configuration of safe motion 4
- P-0-3273, Safely-limited increment 4
- P-0-3274, Safely-limited speed 4
- P-0-3276, Max. activation time of enabling control 4

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safely-limited increment":

- F7010 Safely-limited increment exceeded
- F3142 Activation time of enabling control exceeded
- F7013 Safely-limited speed exceeded
- With motion monitoring activated, the display of the IndraDrive control panel shows "SMM".

Safety function

Selecting the function

The safety function "Safely-limited increment" becomes active by selecting the special mode "Safe motion".

Safe motion can be selected via

- Digital inputs/outputs for both safety channels
- Digital inputs/outputs of the optional safety technology module "S2" for safety channel 2 and master communication (SERCOS, PROFIBUS) for safety channel 2 or
- PROFIBUS (or PROFIsafe)

For transition from normal operation / special mode to the safe state, there is one programmable time available for each kind of transition:

- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation

After the respective tolerance time is over, the velocity monitoring and the monitoring of the increment are activated (dual-channel monitoring).

Monitoring function

In the case of the safety function "Safely-limited increment", dual-channel monitoring makes sure that the drive ...

- ...does not exceed the preset velocity limit values (P-0-3244, P-0-3254, P-0-3264, P-0-3274) within the maximum increment, otherwise the drive generates the error "F7013 Safely-limited speed exceeded".
- ...only moves within the maximum increment (cf. P-0-3243, P-0-3253, P-0-3263, P-0-3273), otherwise the drive generates the error "F7010 Safely-limited increment exceeded".

☞ The velocity limit values P-0-3244, P-0-3254, P-0-3264 and P-0-3274, as well as the maximum allowed increments (P-0-3243, P-0-3253, P-0-3263 and P-0-3273), are write-protected with "P-0-3206, Safety technology password" after the safety technology has been activated and cannot be changed by unauthorized persons.

The status of the safety technology password can be seen in "P-0-3207, Safety technology password level".

The special mode "Safe motion" with the safety function "Safely-limited increment" is selected by actuating an enabling control and the mode selector. The activation time of the enabling control ("P-0-3222, Max. activation time of enabling control") can be parameterized and is cyclically monitored. If this time is exceeded, the error message "F3142 Activation time of enabling control exceeded" is generated.

Individual activation times of enabling control are possible for the special modes "Safe motion". For commissioning, it is possible to select in "P-0-3239, Configuration of global safety technology functions" whether a common maximum activation time of enabling control (P-0-3222) is active for all special modes "Safe motion", or whether an individual activation time of enabling control (P-0-3246, P-0-3256, P-0-3266, P-0-3276) is active for each special mode "Safe motion 1..4".

⚠ WARNING

Dangerous movements!

Danger to life, risk of injury, serious injury or property damage by switching off the monitoring of activation time!

You can do without the monitoring of the activation time, if it is not common practice to use an enabling control in your industrial sector and if constant motion does not represent any danger.

The machine manufacturer is responsible for the monitoring of the activation time and his risk analysis has to show his responsibility.

"P-0-3222, Max. activation time of enabling control"="0" deactivates the time monitoring of the special mode "safe motion"; this also applies to the individual activation times of enabling control P-0-3246, P-0-3256, P-0-3266 and P-0-3276.

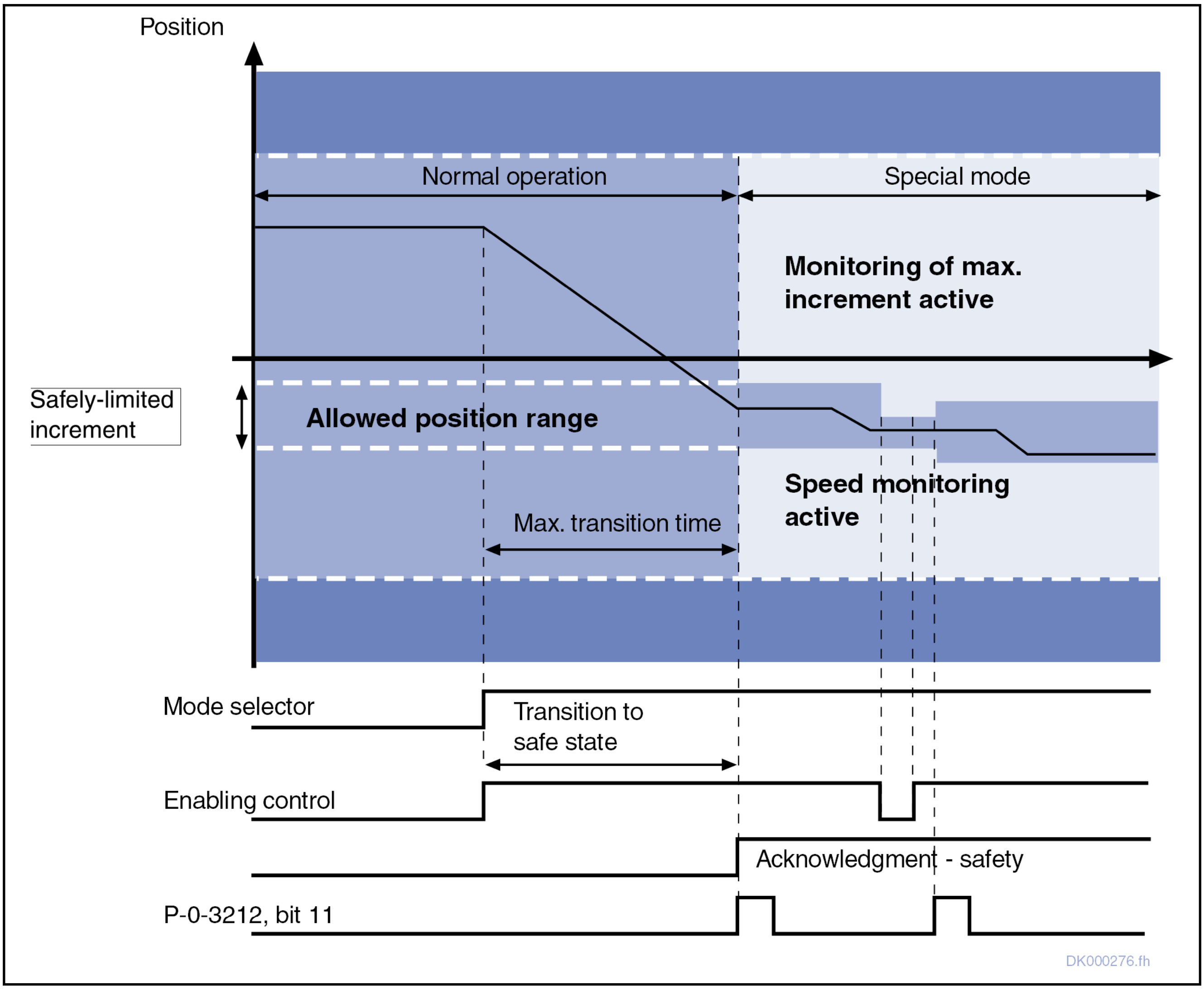


Fig. 6-22: Safely-limited increment (NC-controlled transition to the Safe motion from normal operation)

Selecting the effective limit value

By means of two additional safety switches (S1, S2), the four different "Safe motions" (SMM) can be selected with the corresponding velocity limit values and increments:

- S2="0", S1="0": SMM1 ("P-0-3243, Safely-limited increment 1" and "P-0-3244, Safely-limited speed 1" take effect)
- S2="0", S1="1": SMM2 ("P-0-3253, Safely-limited increment 2" and "P-0-3254, Safely-limited speed 2" take effect)
- S2="1", S1="0": SMM3 ("P-0-3263, Safely-limited increment 3" and "P-0-3264, Safely-limited speed 3" take effect)
- S2="1", S1="1": SMM4 ("P-0-3273, Safely-limited increment 4" and "P-0-3274, Safely-limited speed 4" take effect)

6.4.4 Safely-monitored position (SMP)

Brief description

In the case of the safety function "Safely-monitored position", the dual-channel monitoring detects that the drive moves beyond preset position limit values (+/-). In addition, monitoring with regard to safely-limited speed is always active.

☞ Using the safety function "Safely-monitored position" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

By means of an additional safety switch (S1), two parameter sets for the special mode "Safe motion" can be selected.

☞ Before the safety function "Safely-monitored position" is selected, the "Safe homing procedure" has to be carried out (C4000).

Features

The safety function "Safely-monitored position" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- The position limit values (P-0-3241, P-0-3242, P-0-3251, P-0-3252) are monitored.
- The safety function "Safely-monitored position" is active when the special mode "Safe motion" is selected, if it has been parameterized for this mode.
- For the safety function "Safely-monitored position", the drive must have been safely homed.
- The limit values monitored by the safety function "Safely-monitored position" always refer to the actual position value of P-0-3280. This value might possibly deviate from the actual position value in S-0-0051 or S-0-0053 (e.g., when encoder corrections or the command C3300/C3400 are used).
- The safety function "Safely-monitored position" can be combined with the other safety functions of the special mode "Safe motion".
- The special mode "Safe motion" with the safety function "Safely-monitored position" is selected by actuating an enabling control and the mode selector.

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safely-monitored position":

- P-0-3210, Safety technology configuration
- P-0-3220, Tolerance time transition from normal operation
- P-0-3222, Max. Activation time of enabling control
- P-0-3225, Tolerance time transition from safe operation
- P-0-3239, Configuration of global safety technology functions
- P-0-3240, Configuration of safe motion 1
- P-0-3241, Safely-monitored position 1, positive
- P-0-3242, Safely-monitored position 1, negative
- P-0-3244, Safely-limited speed 1
- P-0-3246, Max. activation time of enabling control 1
- P-0-3250, Configuration of safe motion 2
- P-0-3251, Safely-monitored position 2, positive
- P-0-3252, Safely-monitored position 2, negative
- P-0-3254, Safely-limited speed 2
- P-0-3256, Max. activation time of enabling control 2

- P-0-3280, Actual position value, channel 2

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safely-monitored position":

- F3112 Safe reference missing
- F7011 Safely-monitored position, exceeded in pos. direction
- F7012 Safely-monitored position, exceeded in neg. direction
- F3142 Activation time of enabling control exceeded
- F7013 Safely-limited speed exceeded
- With the safety function "Safely-monitored position" activated, the display of the IndraDrive control panel shows "SMP".

Safety function

Selecting the function

The safety function "Safely-monitored position" becomes active by selecting the special mode "Safe motion".

Safe motion can be selected via

- Digital inputs/outputs for both safety channels
- Digital inputs/outputs of the optional safety technology module "S2" for safety channel 2 and master communication (SERCOS, PROFIBUS) for safety channel 2 or
- PROFIBUS (or PROFIsafe)

For transition from normal operation / special mode to the safe state, there is one programmable time available for each kind of transition:

- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation

After the respective tolerance time is over, velocity monitoring is activated.

Within the selected position range (=travel range which is defined by an upper and lower position limit value), it is possible to move the drive in both directions with a speed below the allowed limited speed (cf. "P-0-3244, Safely-limited speed 1"; "P-0-3254, Safely-limited speed 2").

☞ Before the safety function "Safely-monitored position" is selected, the "Safe homing procedure" has to be carried out (C4000).

Monitoring functions

In the case of the safety function "Safely-monitored position", dual-channel monitoring makes sure that the drive ...

- ...does not exceed the preset velocity limit values (P-0-3244, P-0-3254) within the allowed position ranges, otherwise the drive generates the error "F7013 Safely-limited speed exceeded".
- ...only moves within the allowed position ranges (cf. P-0-3241, P-0-3242, P-0-3251, P-0-3252), otherwise the drive generates the error "F7011 Safely-monitored position, exceeded in pos. direction" or "F7012 Safely-monitored position, exceeded in neg. direction".

☞ The end positions set in P-0-3241, P-0-3242, P-0-3251 and P-0-3252 relate to the actual position value in P-0-3280. This value might possibly deviate from the actual position value in S-0-0051 or S-0-0053 (e.g., when encoder corrections or the command C3300/C3400 are used).

☞ After the safety technology has been activated, the velocity limit values P-0-3244 and P-0-3254, as well as the allowed position ranges (P-0-3241, P-0-3251, P-0-3242, P-0-3252) are write-protected with "P-0-3206, Safety technology password" and cannot be changed by unauthorized persons.

The status of the safety technology password can be seen in "P-0-3207, Safety technology password level".

The special mode "Safe motion" with the safety function "Safely-monitored position" is selected by actuating an enabling control and the mode selector. The activation time of the enabling control (P-0-3222, Max. activation time of enabling control) can be parameterized and is cyclically monitored. If this time is exceeded, the error message "F3142 Activation time of enabling control exceeded" is generated.

Individual activation times of enabling control are possible for the special modes "Safe motion". For commissioning, it is possible to select in "P-0-3239, Configuration of global safety technology functions" whether a common maximum activation time of enabling control (P-0-3222) is active for all special modes "Safe motion", or whether an individual activation time of enabling control (P-0-3246, P-0-3256, P-0-3266, P-0-3276) is active for each special mode "Safe motion 1..4".

⚠ WARNING

Dangerous movements!

Danger to life, risk of injury, serious injury or property damage by switching off the monitoring of activation time!

You can do without the monitoring of the activation time, if it is not common practice to use an enabling control in your industrial sector and if constant motion does not represent any danger.

The machine manufacturer is responsible for the monitoring of the activation time and his risk analysis has to show his responsibility.

"P-0-3222, Max. activation time of enabling control"="0" deactivates the time monitoring of the special mode "safe motion"; this also applies to the individual activation times of enabling control P-0-3246, P-0-3256, P-0-3266 and P-0-3276.

Selecting the effective limit values

By means of an additional safety switch (S1), the two different "Safe motions" (SMM) can be selected with the corresponding velocity limit values and position ranges.

- S2="0", S1="0": SMM1 ("P-0-3241, Safely-monitored position 1, positive", "P-0-3242, Safely-monitored position 1, negative" and "P-0-3244, Safely-limited speed 1" take effect)
- S2="0", S1="1": SMM2 ("P-0-3251, Safely-monitored position 2, positive", "P-0-3252, Safely-monitored position 2, negative" and "P-0-3254, Safely-limited speed 2" take effect)

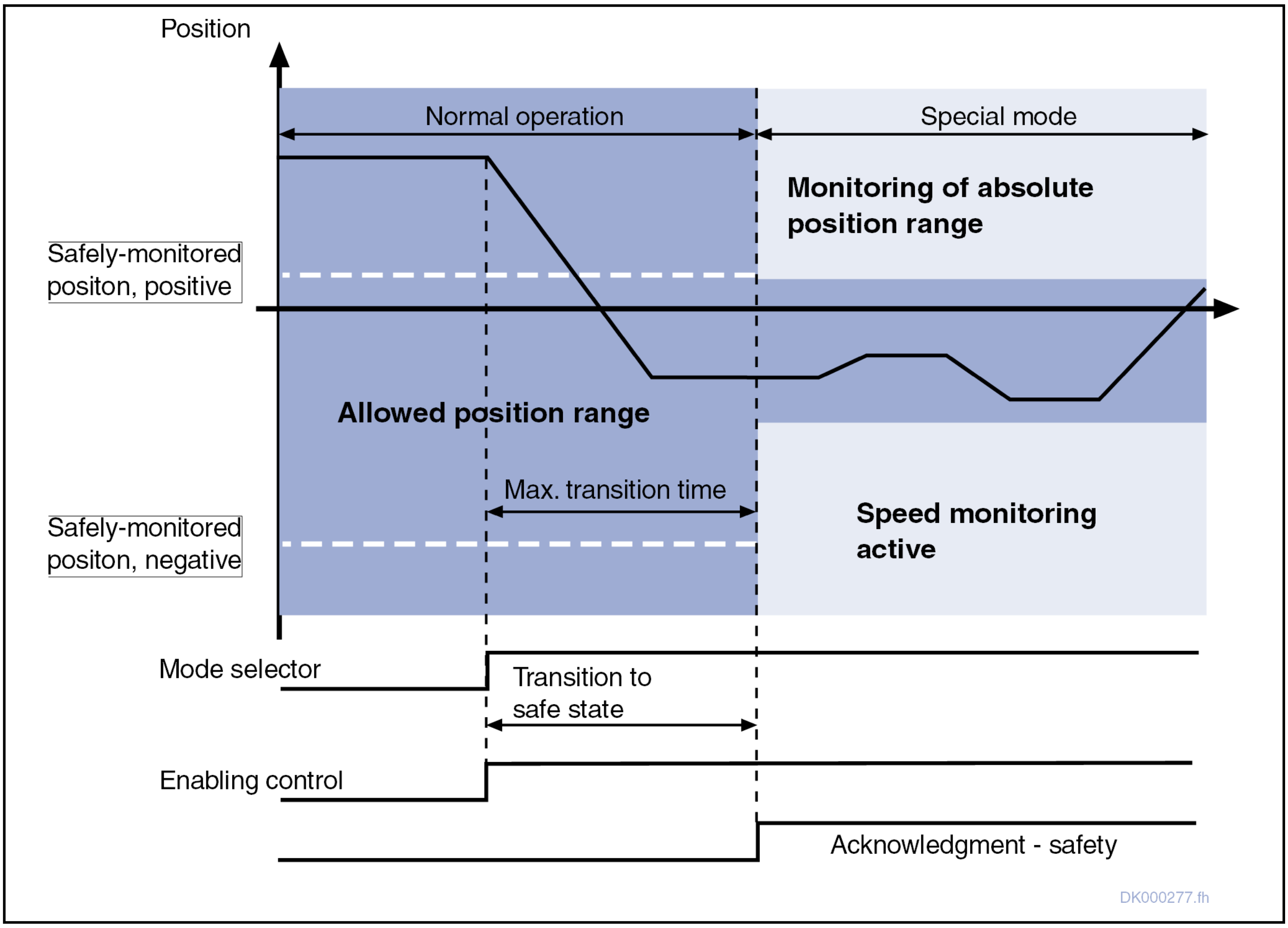


Fig. 6-23: Safely-monitored position (NC-controlled transition to Safe motion from normal operation)

Notes on commissioning

☞ The safely-monitored position limit values have to be set in the following minimum distances to the non-safe position limit values of the axis:

- Modulo scaling: S-0-0103 - "Safely-monitored position x, positive" + "Safely-monitored position x, negative" > "Safely-limited speed x" * 4ms
- Absolute scaling: (2 * S-0-0278) - "Safely-monitored position x, positive" + "Safely-monitored position x, negative" > "Safely-limited speed x" * 4ms

If these distandes are not complied with, the safely-monitored position limit values might possibly be passed without an error being generated!

6.5 Additional or auxiliary functions

6.5.1 Safely-monitored stopping process

Brief description

☞ Using the safety function "Safely-monitored stopping process" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

The integrated safety technology makes available the following variants of the monitoring/safety function "Safely-monitored stopping process":

- Safely-monitored stopping process with safely-monitored deceleration time and braking ramp
  - Monitoring function 1: Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp (to standstill)
  - Monitoring function 2: Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp [to special mode Safe motion (SMM)]
- Monitoring function 3: Safely-monitored stopping process on basis of actual velocity
- Monitoring function 5: Safely-monitored stopping process with Safely-monitored deceleration time

Features

The monitoring/safety function "Safely-monitored stopping process" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- In the case of error, the drive independently activates the monitoring functions according to the settings in the parameters "P-0-0119, Best possible deceleration" and "P-0-0117, Activation of NC reaction on error".
- The deceleration time (P-0-3220, P-0-3225) is monitored.
- Optional monitoring of the deceleration ramp (P-0-3282)
- Optional monitoring of the deceleration ramp (P-0-3282) after the delay is over (P-0-3226)

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safely-monitored stopping process":

- P-0-0117, Activation of NC reaction on error
- P-0-0119, Best possible deceleration
- P-0-3210, Safety technology configuration
- P-0-3220, Tolerance time transition from normal operation
- P-0-3225, Tolerance time transition from safe operation
- P-0-3226, Delay Safely-monitored deceleration
- P-0-3233, Velocity threshold for safe standstill
- P-0-3282, Safely-monitored deceleration
- P-0-3283, Safely-monitored deceleration, veloc. envelope curve

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safely-monitored stopping process":

- E3108 Safely-monitored deceleration exceeded
- F7050 Time for stopping process exceeded
- F7051 Safely-monitored deceleration exceeded
- F8135 SMD: Velocity exceeded

Safety function

Selecting the function

The safety function "Safely-monitored stopping process" is active during every transition to a special mode. With the parameters P-0-3210 and P-0-3226, it is possible to select the type/variant of stopping process monitoring.

☞ Delay monitoring is always active during the stopping process [except for drive-controlled operation mode transitions with return motion (P-0-0119)]; it is therefore definitely necessary to parameterize an effective braking ramp in P-0-3282.

Overview

The active monitoring functions depend on the parameterization of the axis, as well as on the selected special mode. The tables below show when the different types of monitoring are active and which error is generated when the monitoring function triggers.

Transitions	Parameterization	Reaction	
	Delay Safely-monitored deceleration (P-0-3226)	Monitoring	Error message when monitoring function is violated
NO, SMMx → SS1ES, SS1, SS2	0	1	F7051
	>0	3	F7051
NO, SMMx → SMMx	x	2	F7051

Monitoring 1 "Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp" (to standstill)

Monitoring 2 "Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp" (to special mode "Safe motion (SMM)")

Monitoring 3 "Safely-monitored stopping process on basis of actual velocity"

Tab. 6-7: Monitoring functions during NC-controlled safety technology operation mode transitions

Transitions	Parameterization		Reaction		
	F7 deceleration (P-0-0119)	F3 deceleration (P-0-0119)	Current deceleration	Monitoring	Error message when monitoring function is violated
NO, SMMx → SS1ES, SS1	X	0	Emergency stop	3	F8135
	X	1*	Torque disable	Output stage switched off	F8135
	X	2	Drive Halt acc. to S-0-0372	3	F7051
	X	3*	Return motion	5	F7050 (P-0-3220/ P-0-3225)
	0	4	Emergency stop with ramp and filter (S-0-0429, S-0-0349)	3	F7051
	4	4	Emergency stop with ramp and filter (S-0-0429, S-0-0349)	3	F8135
NO, SMMx → SS2	X	X	Drive Halt acc. to S-0-0372	3	F7051
SMMx → SMMx	X	X	-	5	F7013

* Cannot be parameterized in conjunction with the safe braking and holding system

Monitoring 3 "Safely-monitored stopping process on basis of actual velocity"

Monitoring 5 "Safely-monitored stopping process with Safely-monitored deceleration time"

Tab. 6-8: Monitoring functions during drive-controlled operation mode transitions

Parameterization			Reaction		
NC error reaction (P-0-0117)	F7 deceleration (P-0-0119)	F3 deceleration (P-0-0119)	Current deceleration	Monitoring	Error message when monitoring function is violated
0	X	0	Emergency stop	3	F8135
1*	X	0	NC-controlled	5	F7050 (P-0-3220/P-0-3225)
X	X	1*	Torque disable	Output stage switched off	F8135
0	X	2	Drive Halt acc. to S-0-0372	3	F7051
1*	X	2	NC-controlled	5	F7050 (P-0-3220/P-0-3225)
0	X	3*	Return motion	5	F7050 (P-0-3220/P-0-3225)
1*	X	3*	NC-controlled	5	F7050 (P-0-3220/P-0-3225)

Parameterization			Reaction		
NC error reaction (P-0-0117)	F7 deceleration (P-0-0119)	F3 deceleration (P-0-0119)	Current deceleration	Monitoring	Error message when monitoring function is violated
0	0	4	Emergency stop with ramp and filter (S-0-0429, S-0-0349)	3	F7051
0	4	4	Emergency stop with ramp and filter (S-0-0429, S-0-0349)	3	F8135
1*	X	4	NC-controlled	5	F7050 (P-0-3220/P-0-3225)

***** Cannot be parameterized in conjunction with the safe braking and holding system

Monitoring 3 "Safely-monitored stopping process on basis of actual velocity"

Monitoring 5 "Safely-monitored stopping process with Safely-monitored deceleration time"

Tab. 6-9: Monitoring functions in the case of F3xxx errors (non-fatal safety technology errors)

Parameterization		Reaction		
F7 safety technology reaction (P-0-3210)	F7 deceleration (P-0-0119)	Current deceleration	Monitoring	Error message when monitoring function is violated
0	0	Emergency stop	3	F8135
1*	1*	Torque disable	Output stage switched off	F8135
0	4	Emergency stop at acceleration limit S-0-0138	3	F8135

***** Cannot be parameterized in conjunction with the safe braking and holding system

Monitoring 3 "Safely-monitored stopping process on basis of actual velocity"

Tab. 6-10: Monitoring functions in the case of F7xxx errors

Function

Monitoring function 1: "Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp" (to standstill)

The monitoring function 1 "Safely-monitored stopping process with safely-monitored deceleration time and braking ramp" (to standstill) is active during NC-controlled transition from motion (normal operation or special mode "Safe motion") to the special mode "Safe standstill" and "Safe stop 1 (Emergency stop)". As a prerequisite, the delay (P-0-3226) has to contain the value "0". If a delay unequal "0" has been parameterized, the safety function "Safely-monitored stopping process on basis of actual velocity after delay is over" is carried out.

Monitoring via two channels takes place to find out whether the actual velocity is within the velocity envelope curve (P-0-3283). Using the braking ramp (P-0-3282, Safely-monitored deceleration), the drive calculates the velocity envelope curve in such a way that it is at any time able to reach standstill (P-0-3233) - within the scope of the possible deceleration - before the transition/tolerance time (P-0-3220 or P-0-3225) is over. If this is no longer possible, the error "F7051 Safely-monitored deceleration exceeded" is generated and the drive is shut down accordingly. Energy supply is safely (i.e. via two channels) interrupted.

The drive is shut down according to the setting in "P-0-0119, Best possible deceleration".

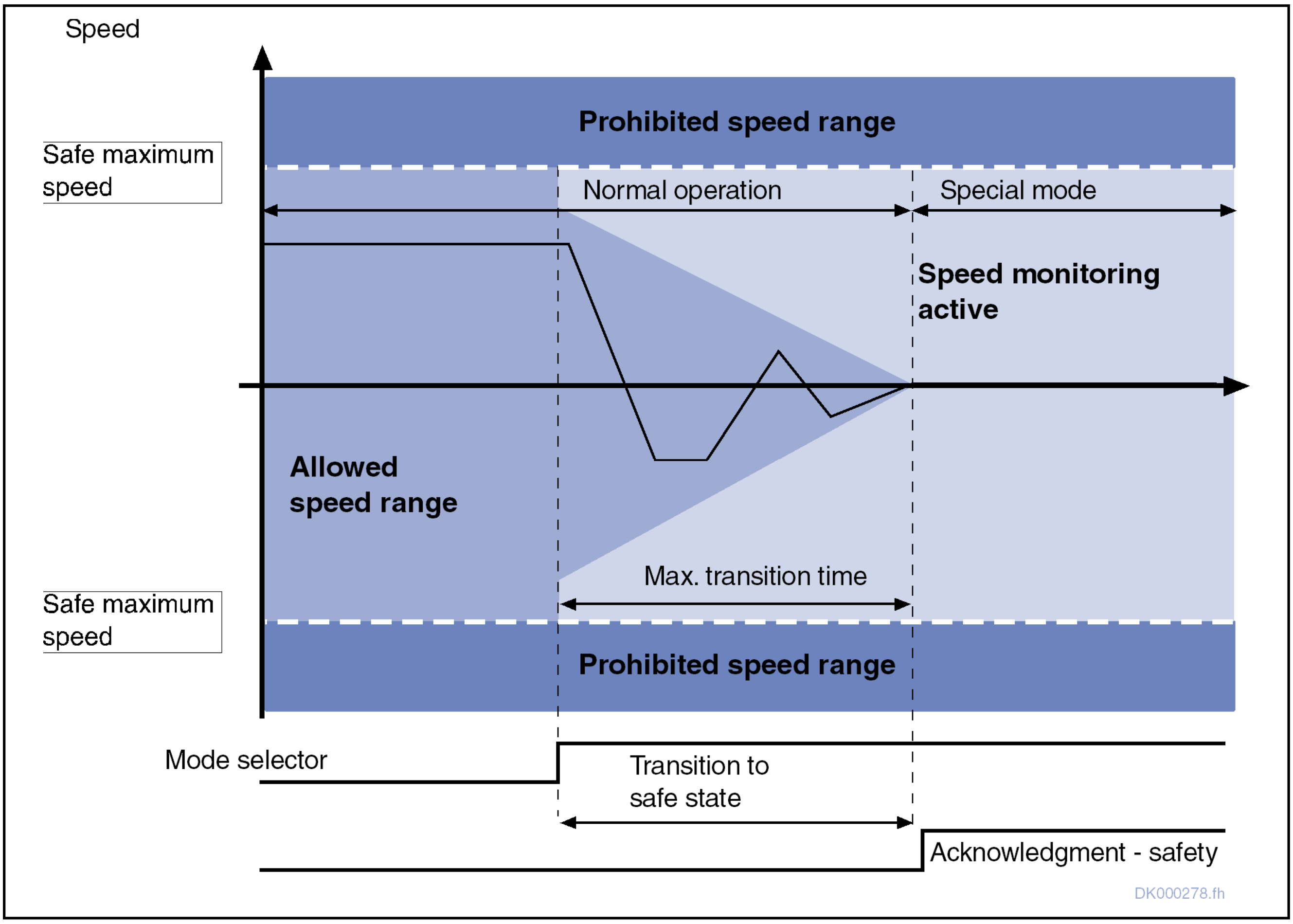


Fig. 6-24: Safely-monitored stopping process with monitored deceleration time and braking ramp from normal operation (to standstill) (NC-controlled transition)

Monitoring function 2: "Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp" [to special mode "Safe motion" (SMM)]

The monitoring function 2 "Safely-monitored stopping process with safely-monitored deceleration time and braking ramp" [to special mode "Safe motion" (SMM)] is active during NC-controlled transition from motion (normal operation or special mode "Safe motion") to the special mode "Safe motion" (SMM).

Monitoring via two channels takes place to make sure that the actual velocity is within the velocity envelope curve (P-0-3283). Using the braking ramp (P-0-3282, Safely-monitored deceleration), the drive calculates the velocity envelope curve in such a way that the parameterized velocity window of the selected special mode "Safe motion" ("P-0-3244, Safely-limited speed 1", "P-0-3254, Safely-limited speed 2", "P-0-3264, Safely-limited speed 3" or "P-0-3274, Safely-limited speed 4") is reached until the end of the transition/tolerance time (P-0-3220 or P-0-3225). When the values leave the velocity envelope curve, the drive generates the error message "F7051 Safely-monitored deceleration exceeded".

The drive is shut down according to the setting in "P-0-0119, Best possible deceleration".

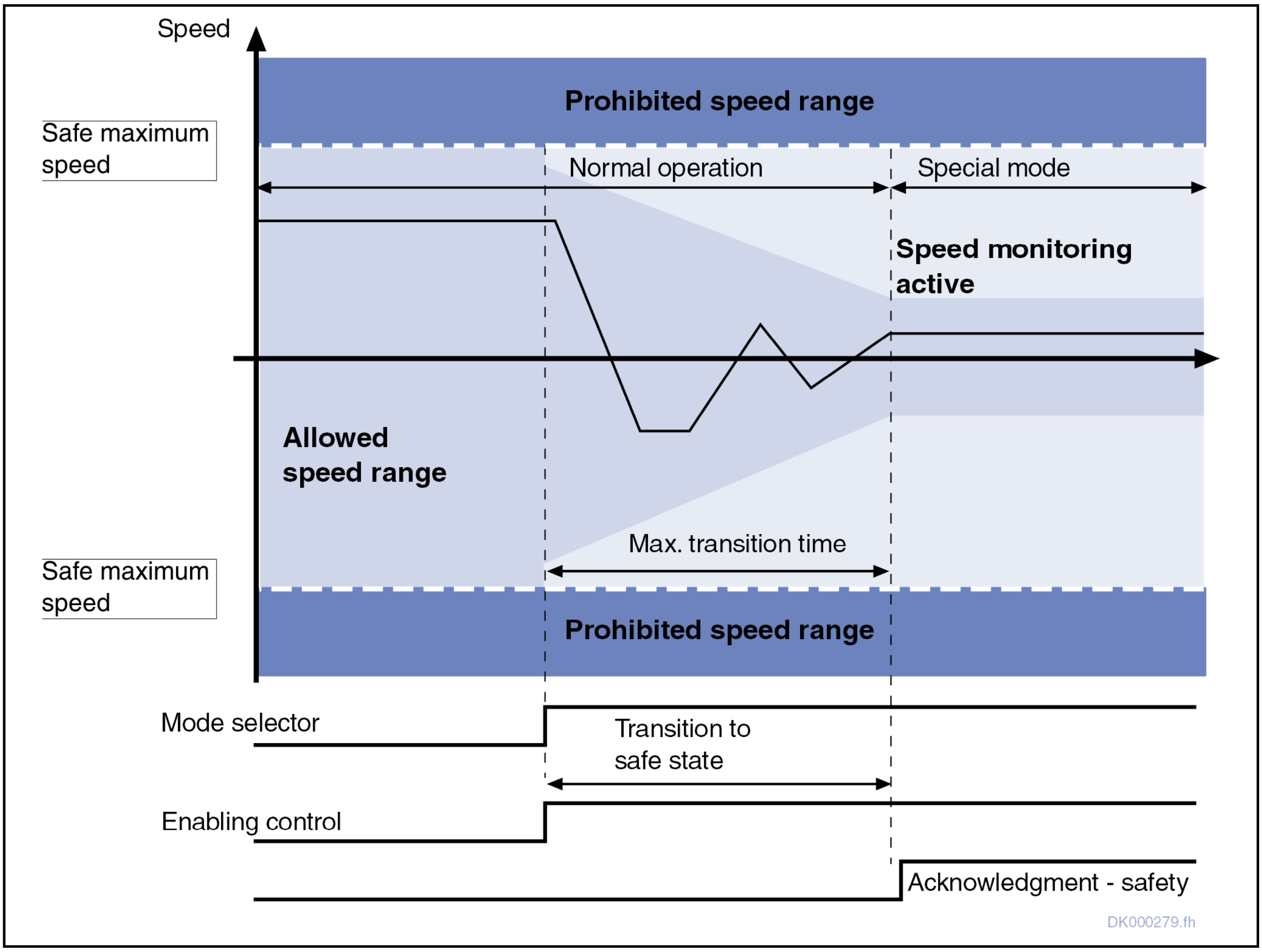


Fig. 6-25: "Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp" [to special mode "Safe motion" (SMM)]

Monitoring function 3: "Safely-monitored stopping process on basis of actual velocity"

The monitoring function "Safely-monitored stopping process on basis of actual velocity" is active

- in conjunction with the safe braking and holding system in the case of "Drive Halt" and "drive off",
- in the case of reactions to safety technology errors and
- in the case of the following transitions:
  - Drive-controlled transitions from motion (normal operation or special mode "Safe motion") to the special mode "Safe standstill" and the safety function "Safe stop 1 (Emergency stop)"
  - NC-controlled operation mode transitions (see P-0-3210) with a **delay (P-0-3226) unequal "0"**

    ⇒In the case of NC-controlled operation mode transitions and **P-0-3226="0"** , the **safety function "Safely-monitored stopping process with Safely-monitored deceleration time and braking ramp"** is carried out instead of the safety function "Safely-monitored stopping process on basis of actual velocity"!

Monitoring via two channels takes place to make sure that the actual velocity is within the velocity envelope curve (P-0-3283). When the threshold is exceeded, the differences of the actual values and threshold values are added, this corresponds to an incorrect distance and a warning is generated. If the incorrect distance is greater than the monitoring window (P-0-3230), an error message is generated.

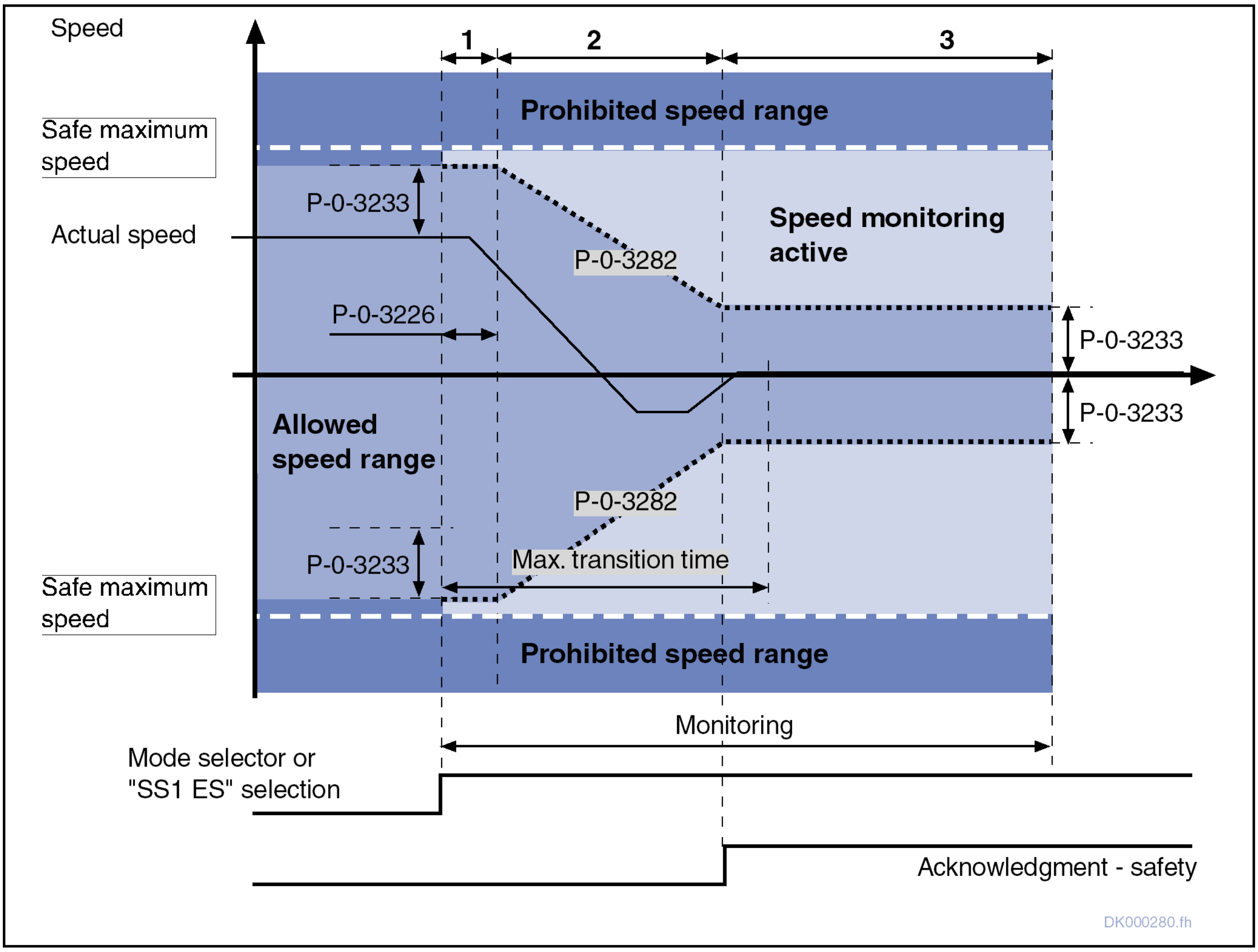


Fig. 6-26: Safely-monitored stopping process on basis of actual velocity with active monitoring at selection

The monitoring curve consists of three sections and is generated as follows:

1. "Reaction time to change in selection" (drive-side or NC-side) for the duration of P-0-3226:

For the duration of P-0-3226, the safety technology gives the system (control unit and drive) the time to adjust the command value input for the transition process. For this time, the active monitoring can be configured via P-0-3210. The following monitoring functions can be selected:

- "Monitoring active immediately after selection"

  For the duration of P-0-3226, monitoring makes sure that the actual velocity is smaller than the actual velocity at selection plus the tolerance (P-0-3233) (see figure above, section 1). When the monitoring limit is exceeded, the error "F7051 Safely-monitored deceleration exceeded" is generated.

- "Monitoring active after P-0-3226 is over" (with MPx07V10 and above)

  For the duration of P-0-3226, there is no monitoring within the scope of the safely-monitored stopping process. Only the configured monitoring functions for "normal operation and special mode" are active (see chapter "Safety functions in normal operation and in special mode"). After P-0-3226 is over, the start value for the deceleration ramp is determined in section 2 from the current actual velocity plus the tolerance (P-0-3233).

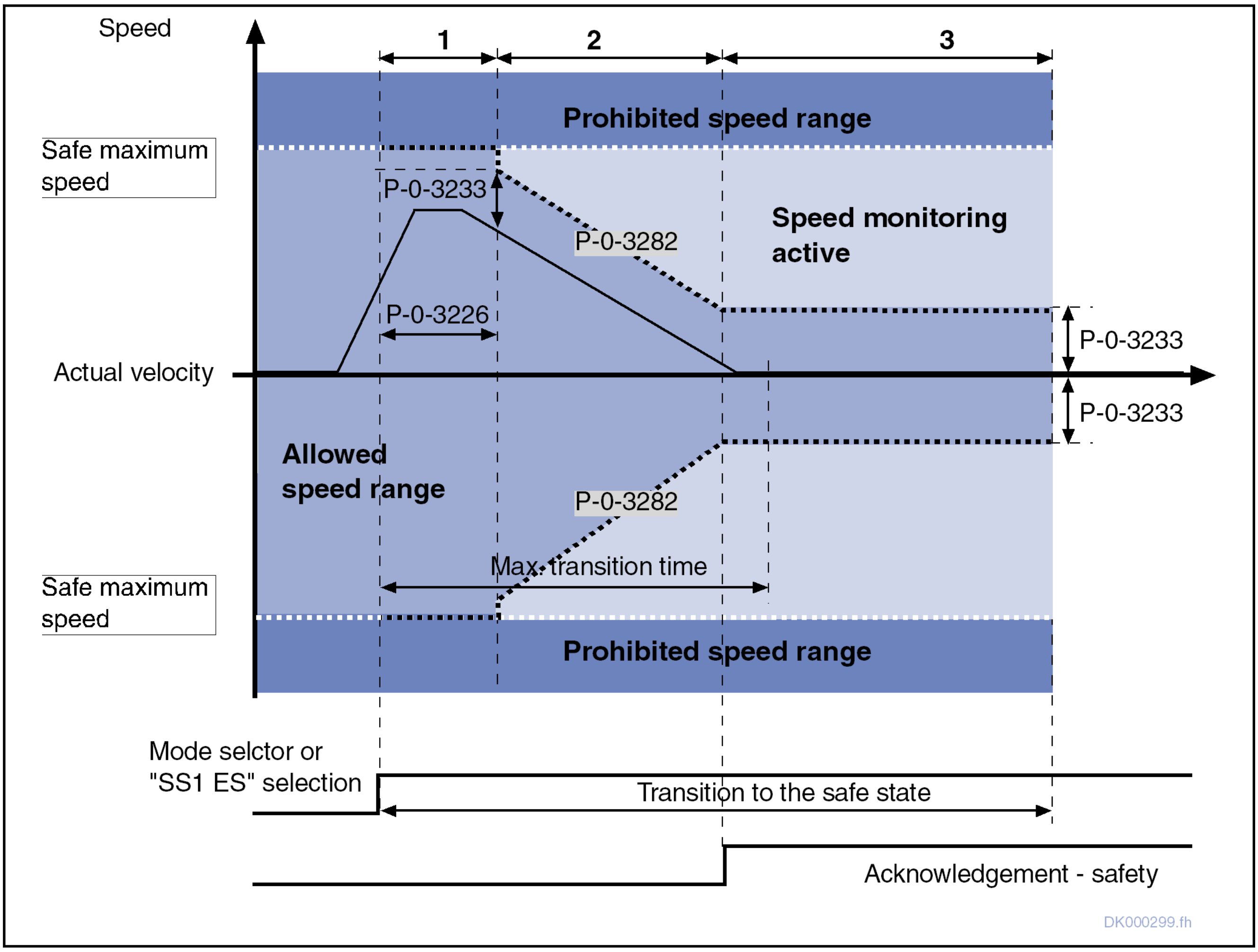


Fig. 6-27: Safely-monitored stopping process on basis of actual velocity with active monitoring after P-0-3226 is over

☞ When the safe maximum speed has been deactivated in P-0-3239, "0" is displayed in P-0-3283 for this part of the safely-monitored stopping process.

2. "Monitoring of the transition to the selected special mode" using **deceleration ramp (P-0-3282)** until the standstill window has been reached (P-0-3233):

In section 2, monitoring via two channels takes place to find out whether the actual velocity is within the velocity envelope curve (P-0-3283). With the start value determined in section 1, the drive generates the velocity envelope curve by means of the deceleration ramp (P-0-3282, Safely-monitored deceleration) and the transition time that has passed (less P-0-3226).

3. "Monitoring of the **standstill window (P-0-3233)**" until the end of the safely-monitored stopping process:

After the velocity envelope curve (P-0-3283) has reached the standstill window (P-0-3233), monitoring makes sure that the actual velocity is smaller than the standstill window until switching to the selected special mode takes place.

By means of the pertinent parameters, it is possible to adjust the monitoring function to many applications. This can be achieved mainly by P-0-3226 and P-0-3282.

If the incorrect distance is greater than the position standstill window P-0-3230, the error "F7051 Safely-monitored deceleration exceeded" is always generated in the case of NC-controlled transitions (see P-0-3210). In the case of drive-controlled transitions and depending on the setting in P-0-0119, the errors

- "F7051 Safely-monitored deceleration exceeded" or
- "F8135 SMD: Velocity exceeded"

are generated. The drive is shut down accordingly and the energy supply is safely interrupted via two channels.

While the incorrect distance is determined (integration of the velocity differences), the warning E3108 is generated to show that the tolerance has come to its limit.

Monitoring function 5: "Safely-monitored stopping process with Safely-monitored deceleration time"

The monitoring function "Safely-monitored stopping process with safely-monitored deceleration time" is active during all transitions between safety technology operating states (P-0-3213, bit0 to bit6) due to changes in selection or in the case of reactions to safety technology errors.

Monitoring via two channels takes place to find out whether the drive has come to a standstill after the transition time (P-0-3220 or P-0-3225) is over.

Time monitoring is started when the selection is changed or when a safety technology error occurs. Time monitoring ends when the new safety technology operating status has been reached, but at the latest after the deceleration/tolerance time is over (the **deceleration/tolerance time** for transition from **normal operation to the special mode "Safe standstill"** has to be set in "P-0-3220, Tolerance time transition from normal operation"; the **deceleration/tolerance time** for transition from the **special mode "Safe motion" to the special mode "Safe standstill"** has to be set in "P-0-3225, Tolerance time transition from safe operation").

If the actual velocity is greater than P-0-3233 after the corresponding tolerance time is over (end of operation mode transition), the error "F7050 Time for stopping process exceeded" is generated. In the case of transition from **normal operation to the special mode "safe standstill"**, the drive is shut down accordingly and energy supply is safely (i.e. via two channels) interrupted. **Special case:** In the case of transitions to the **special mode "Safe motion" (SMM)**, the transition time is monitored, too, but in this case switching to the selected special mode "Safe motion" (SMM) takes place after the corresponding tolerance time is over. The motion monitoring functions configured in the special mode then are immediately active and trigger, if necessary.

☞ Before the corresponding tolerance time is over, the following error messages can have been generated by other monitoring functions of the safety technology function "Safely-monitored stopping process" which were carried out in parallel:

- "F7051 Safely-monitored deceleration exceeded" or
- "F8135 SMD: Velocity exceeded"

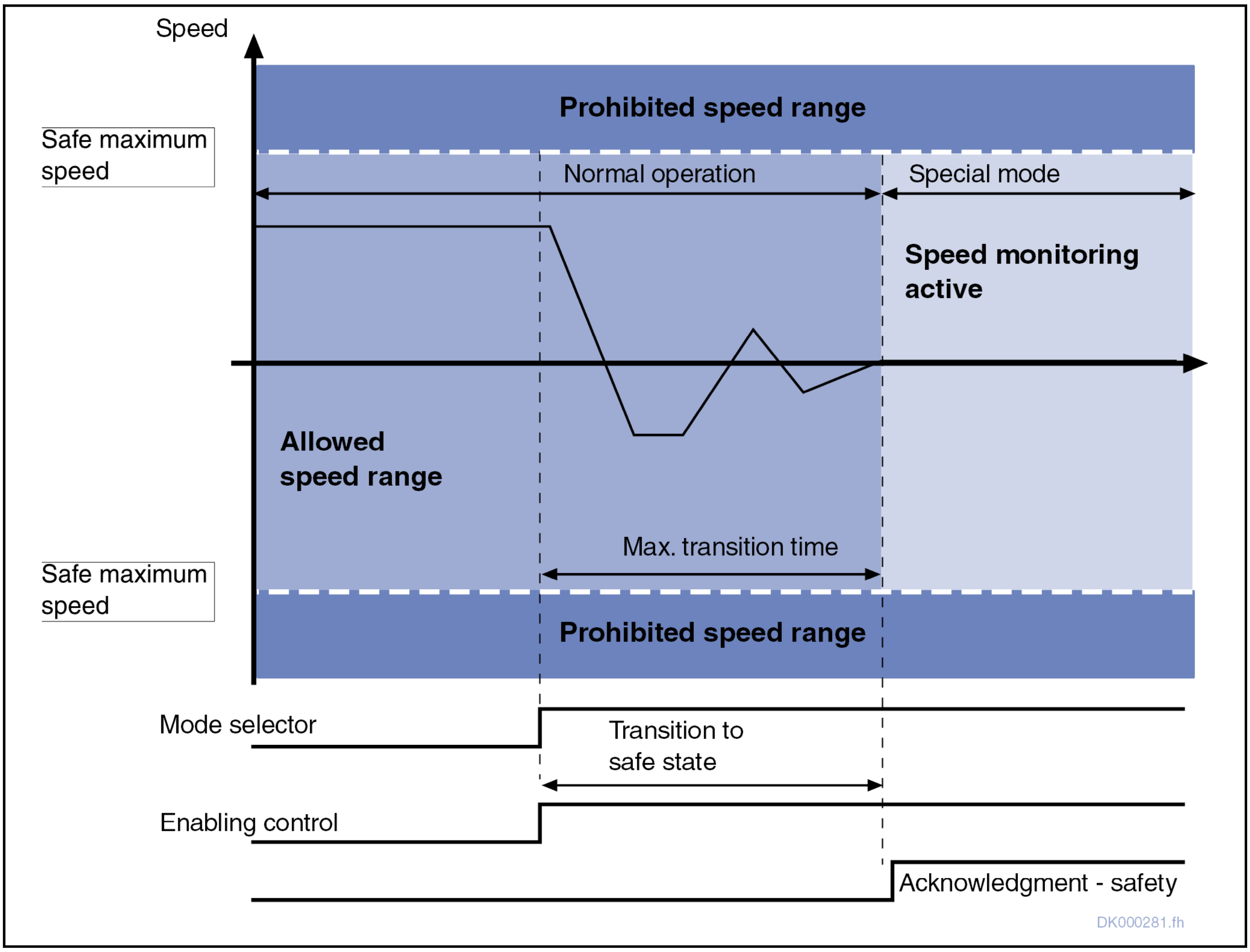


Fig. 6-28: Safely-monitored stopping process with Safely-monitored deceleration time

6.5.2 Safe homing procedure

Brief description

☞ The safe homing procedure by itself is not an independent safety function, but the basis of all safety functions with safely-monitored position!

The auxiliary safety technology function "Safe homing procedure" has to be carried out before selecting the safety function "Safely-monitored position". The safe homing procedure is a homing procedure during normal operation with additional home switch for safe determination of the reference position.

☞ Using the function "Safe homing procedure" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

☞ For absolute measuring systems, the safe homing procedure has to be carried out, too, but only the homing of channel 2 is required in this case.

Features

The auxiliary safety technology function "Safe homing procedure" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- Individual additional homing command for channel 2 (P-0-3228); there are two options for starting the homing procedure of channel 2.
- According to application requirements, the position data reference for channel 2 can be realized by a static or dynamic reference signal.
- Only single-channel design of the home switch required (wiring at channel 2/X41).
- No dynamization of home switch.
- The position difference between channel 1 and channel 2 (P-0-3229) is monitored.
- The safe reference gets lost when leaving phase 4.
- The auxiliary safety technology function "Safe homing procedure" is the prerequisite of the safety functions "Safely-monitored position" and "Safely-limited position".

Pertinent parameters

The following parameters are used in conjunction with the auxiliary safety technology function "Safe homing procedure":

- P-0-3210, Safety technology configuration
- P-0-3211, Safety technology I/O configuration list, channel 2
- P-0-3213, Safety technology operating status
- P-0-3228, C4000 Homing procedure command channel 2
- P-0-3229, Tolerance window for safe homing procedure
- P-0-3231, Reference position for safe reference
- P-0-3280, Actual position value, channel 2
- P-0-3240, Configuration of safe motion 1
- P-0-3250, Configuration of safe motion 2
- S-0-0147, Homing parameter
- S-0-0148, C0600 Drive-controlled homing procedure command
- S-0-0052, Reference distance 1
- S-0-0051, Position feedback value 1
- S-0-0053, Position feedback value 2
- S-0-0054, Reference distance 2
- S-0-0150, Reference offset 1
- S-0-0151, Reference offset 2

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the auxiliary safety technology function "Safe homing procedure":

- C4001 Error during safe homing procedure
- C4002 Incorrect distance of dedicated point channel 1- 2
- E3102 Actual position values validation error
- F3112 Safe reference missing
- F3117 Actual position values validation error

Functional description - Safe homing procedure

Basic function

In order to realize diversitary position monitoring, i.e. separate dual-channel position monitoring, the individual channels have to home their actual position value systems in diversitary form, too. This requires another homing command which is available in addition to the drive-controlled homing procedure command.

In order to get the safe reference, it is first necessary to home channel 1 by means of the known mechanisms (see Functional Description of firmware "Establishing the position data reference"). Then it is necessary to additionally home channel 2.

The drive only remains homed in a safe way as long as it is in phase 4. After restart or phase switch, the safe homing procedure has to be carried out again.

Selecting the reference signal for channel 2

According to application requirements, the position data reference for channel 2 can be realized by a static or dynamic reference signal. The setting is made in "P-0-3210, Safety technology configuration".

- "Static evaluation" means that in standstill a high level is expected at the input of the home switch in "P-0-3231, Reference position for safe reference" in order to establish the position data reference. Evaluation of a static reference signal should be used, when
  - the start position of channel 1 for moving to the reference position is not unequivocally before or behind the reference distance position of channel 2 and it is therefore only possible to position the drive unequivocally at this position, or
  - the safe reference is to be manually confirmed.
- "Dynamic evaluation" means that during a movement a defined edge is expected at the input of the home switch in "P-0-3231, Reference position for safe reference" in order to establish the position data reference. The evaluation of a dynamic reference signal should be used when it is possible to ensure, by moving to the reference mark in channel 1, that the reference position of channel 2 is passed with defined edge.

☞ As these methods have a velocity and switch tolerance, the position data reference is adjusted to the actual position value of channel 1. During the adjustment a check is run to find out whether the difference of the actual position values of channel 1 and channel 2 is within the value parameterized in "P-0-3229, Tolerance window for safe homing procedure".

Establishing the position data reference for channel 2

There are two options for establishing the position data reference for channel 2:

- Via digital input or parameter, start the independent command "P-0-3228, C4000 Homing procedure command channel 2" and observe the points listed below:
  - Channel 1 already must have been homed (e.g. absolute encoder).

  - NC-controlled motion has to be carried out so that the selected dedicated point is "passed" (detected), as the drive does not carry out any independent motion during the execution of the command "P-0-3228, C4000 Homing procedure command channel 2".
- Start "S-0-0148, C0600 Drive-controlled homing procedure command" and observe points listed below:
  - The command "S-0-0148, C0600 Drive-controlled homing procedure command" at the beginning internally also starts the command "P-0-3228, C4000 Homing procedure command channel 2" automatically, if the safety function "Safely-monitored position" has been parameterized.
  - The home switch of channel 2 has to be mechanically mounted in such a way that it is actuated with the travel motion to be expected or during the concluding positioning; if this is not the case, the home switch has to be actuated by an NC-controlled motion.

☞ Using "P-0-3213, Safety technology operating status", it is possible check whether the drive has been safely homed.

Notes on commissioning

The paragraphs below describe typical commissioning sequences for different measuring systems. According to the mounting position of the home switches and the control unit used, there are up to three different commissioning sequences for each encoder type:

- Option 1: "drive-controlled"
  - The home switches are mounted in such a way that by carrying out drive-controlled homing for channel 1 it can be ensured that the home switch for channel 2 is passed from the correct side (dynamic evaluation) or the drive is positioned at it (static evaluation).
  - The control unit knows the command "S-0-0148, C0600 Drive-controlled homing procedure command".
- Option 2: "drive-/NC-controlled"
  - The home switches are mounted in such a way that by carrying out drive-controlled homing for channel 1 it **cannot** be ensured that the home switch for channel 2 is passed from the correct side (dynamic evaluation) or the drive is positioned at it (static evaluation).
  - The homing command of the control unit is extended by NC-controlled actuation of the home switch for channel 2.
- Option 3: "NC-controlled"
  - The homing of channel 1 is completely carried out by the control unit (the travel motions, too); the homed system is transmitted to the drive.
  - The homing command of the control unit is extended by NC-controlled actuation of the home switch for channel 2.

The commissioning example applying to the application is selected using the diagram below:

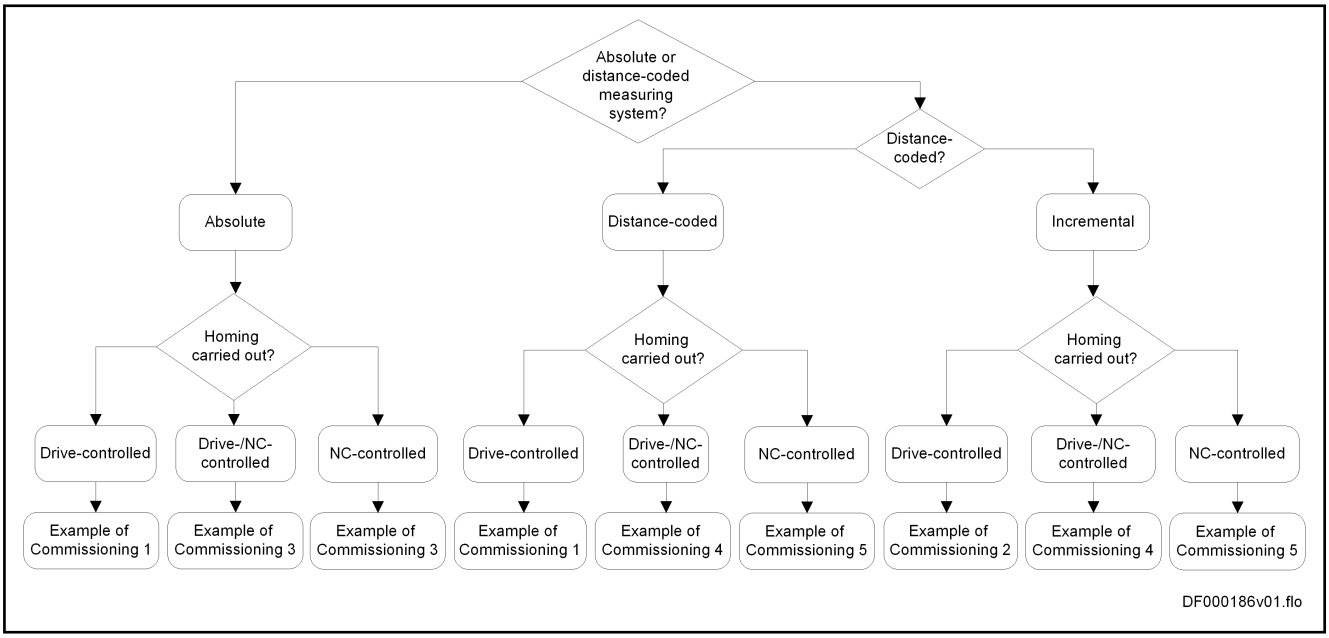

Absolute or distance-coded measuring system?
Distance-coded?
Absolute
Distance-coded
Incremental
Homing carried out?
Homing carried out?
Homing carried out?
Drive-controlled
Drive-/NC-controlled
NC-controlled
Drive-controlled
Drive-/NC-controlled
NC-controlled
Drive-controlled
Drive-/NC-controlled
NC-controlled
Example of Commissioning 1
Example of Commissioning 3
Example of Commissioning 3
Example of Commissioning 1
Example of Commissioning 4
Example of Commissioning 5
Example of Commissioning 2
Example of Commissioning 4
Example of Commissioning 5
DF000186v01.flo

Fig. 6-29: Selection diagram for commissioning examples of Safe homing procedure

In the descriptions below, channel 1 always refers to the motor encoder. If an external encoder has been plugged in instead of the motor encoder at optional slot 1, it is only necessary to replace the following parameters, the function remains as described:

- S-0-0051 replaced by S-0-0053
- S-0-0052 replaced by S-0-0054
- S-0-0150 replaced by S-0-0151

Commissioning example 1

Requirements

The following requirements must have been fulfilled so that safe reference can be established via the command "S-0-0148, C0600 Drive-controlled homing procedure command":

- Use absolute or distance-coded measuring system.
- Establish the position data reference for channel 1 using drive-controlled homing (S-0-0148).
- Static evaluation or manual actuation of home switch for channel 2.

Presetting

The following parameter setting has to be made in the drive:

- "P-0-3210, Safety technology configuration": "Evaluate home switch as static switch"
- "P-0-3229, Tolerance window for safe homing procedure": "Positioning accuracy at home switch +10%"
- "S-0-0052, Reference distance 1" (or "S-0-0054, Reference distance 2") = P-0-3231
- "S-0-0147, Homing parameter", position drive at reference point at the end of homing (S-0-0052 or S-0-0054)

How to carry out Safe homing (chronological sequence)

Carry out the safe homing procedure in the following order:

1. Start command "C0600 Drive-controlled homing procedure command"; drive establishes reference for channel 1 and positions at reference distance [S-0-0052 (or S-0-0054)=P-0-3231].
2. In reference position for channel 2, reference signal either has to be triggered automatically by means of mounted switch or by manual actuation.
3. Complete command "C0600 Drive-controlled homing procedure command".

When the safe homing procedure was successful, this is signaled in "P-0-3213, Safety technology operating status" and the safety function "Safely-monitored position" can be used.

Commissioning example 2

Requirements

The following requirements must have been fulfilled so that safe reference can be established via the command "S-0-0148, C0600 Drive-controlled homing procedure command":

- Use an incremental measuring system.
- Establish the position data reference for channel 1 using drive-controlled homing (S-0-0148).
- Dynamic evaluation of the home switch for channel 2 without reference mark.
- Home switch for channel 2 has to be situated on the way to reference point for channel 1.
- The distance between the reference point for channel 1 (Reference point$_{\text{channel 1}}$) and channel 2 (Reference point$_{\text{channel 2}}$) has to be greater than the tolerance window ("P-0-3229, Tolerance window for safe homing procedure" + 10%):

$$|\text{Reference point}_{\text{channel 2}} - \text{Reference point}_{\text{channel 1}}| < \text{P-0-3229} + 10\ \%$$

Presetting

The following parameter setting has to be made in the drive:

- "P-0-3210, Safety technology configuration": Evaluate home switch as dynamic reference signal and select corresponding edge evaluation
- Adjust "P-0-3229, Tolerance window for safe homing procedure" (value depends on delay of signals, as well as on homing velocity). The minimum value for "P-0-3229, Tolerance window for safe homing procedure" (P-0-3229$_{\text{min}}$) can be calculated from the homing velocity (v$_{\text{homing}}$) as follows:

$$\text{P-0-3229}_{\text{min}} = 2 \times v_{\text{homing}} \times 1\ \text{ms}$$

- "P-0-3231, Reference position for safe reference": Enter position of home switch edge channel 2

$$\text{Reference distance} = \text{Reference point}_{\text{channel 2}} - \text{Reference point}_{\text{channel 1}}$$

$$\text{P-0-3231} = \text{S-0-0052} - \text{S-0-0150} - \text{reference distance} \quad \text{or}$$

$$\text{P-0-3231} = \text{S-0-0054} - \text{S-0-0151} - \text{reference distance}$$

P-0-3231	Reference position for safe reference
S-0-0052	Reference distance 1 (or S-0-0054)
S-0-0150	Reference offset 1 (or S-0-0151)

- "S-0-0147, Homing parameter": Activate "Evaluation of home switch"

How to carry out Safe homing (chronological sequence)

Carry out the safe homing procedure in the following order:

1. Start command "C0600 Drive-controlled homing procedure command"; drive establishes reference for channel 1.
2. During homing procedure for channel 1, channel 2 detects edge of home switch for channel 2 and changes its actual position value to "P-0-3231, Reference position for safe reference".
3. Drive checks whether actual position value difference between channel 1 and channel 2 is smaller than "P-0-3229, Tolerance window for safe homing procedure".
4. Complete command "C0600 Drive-controlled homing procedure command".

When the safe homing procedure was successful, this is signaled in "P-0-3213, Safety technology operating status" and the safety function "Safely-monitored position" can be used.

☞ Any position errors in channel 1 of the size of the tolerance window (P-0-3229) will not be detected!

Commissioning example 3

Requirements

The following requirements must have been fulfilled so that safe reference can be established via the command "P-0-3228, C4000 Homing procedure command channel 2":

- Use an absolute measuring system (absolute position must have been set)
- For establishing reference, travel motion by the control unit has to be possible.
- Home switch for channel 2 can be evaluated either dynamically or statically.

Presetting

The following parameter setting has to be made in the drive:

- "P-0-3210, Safety technology configuration": Evaluate home switch dynamically or statically and select corresponding edge evaluation in the case of dynamic evaluation
- "P-0-3229, Tolerance window for safe homing procedure": Content depends on home switch evaluation type:
  - – Dynamic evaluation of the home switch: Adjust "P-0-3229, Tolerance window for safe homing procedure" (value depends on delay of signals, as well as on homing velocity)

$$\boxed{\text{P-0-3229}_{min} = 2 \times v_{homing} \times 1\ \text{ms}}$$

- Static evaluation of the home switch: Enter positioning accuracy at home switch +10%
- "P-0-3231, Reference position for safe reference": Enter position of home switch channel 2

How to carry out Safe homing (chronological sequence)

Carry out the Safe homing procedure in the following order:

1. Start command "C4000 Homing procedure command channel 2".

   Control unit moves drive to (static home switch evaluation) or over (dynamic home switch evaluation) reference position for safe reference (P-0-3231).
2. In the case of manual actuation of home switch for channel 2, reference signal has to be triggered when drive is at reference position for channel 2.

3. Complete command "C4000 Homing procedure command channel 2".

When the safe homing procedure was successful, this is signaled in "P-0-3213, Safety technology operating status" and the safety function "Safely-monitored position" can be used.

Commissioning example 4

Requirements

The following requirements must have been fulfilled so that the safe reference can be established in a drive-/NC-controlled way:

- Use an incremental or distance-coded measuring system.
- Establish the position data reference for channel 1 using drive-controlled homing (S-0-0148).
- For establishing reference, travel motion by the control unit has to be possible.
- Home switch for channel 2 can be evaluated either dynamically or statically.
- When an incremental measuring system is used, the distance between the reference point for channel 1 and channel 2 has to be greater than the tolerance window ("P-0-3229, Tolerance window for safe homing procedure" + 10%).

$$|\text{Reference point}_{\text{channel 2}} - \text{Reference point}_{\text{channel 1}}| < \text{P-0-3229} + 10\ \%$$

Presetting

The following parameter setting has to be made in the drive:

- "P-0-3210, Safety technology configuration": Evaluate home switch dynamically or statically and select corresponding edge evaluation in the case of dynamic evaluation
- "P-0-3229, Tolerance window for safe homing procedure": Content depends on whether home switch is to be evaluated statically or dynamically:
  - **Static evaluation** of the home switch: Enter positioning accuracy at home switch +10%
  - **Dynamic evaluation** of the home switch: Adjust according to formula below (value depends on delay of signals, as well as on homing velocity)

$$\text{P-0-3229}_{\text{min}} = 2 \times v_{\text{homing}} \times 1\ \text{ms}$$

- "P-0-3231, Reference position for safe reference": Enter position of home switch edge channel 2. When using an incremental encoder, calculate the position as follows:

$$\text{Reference distance} = \text{Reference point}_{\text{channel 2}} - \text{Reference point}_{\text{channel 1}}$$

$$\text{P-0-3231} = \text{S-0-0052} - \text{S-0-0150} - \text{reference distance} \quad \text{or}$$

$$\text{P-0-3231} = \text{S-0-0054} - \text{S-0-0151} - \text{reference distance}$$

P-0-3231	Reference position for safe reference
S-0-0052	Reference distance 1 (or S-0-0054)
S-0-0150	Reference offset 1 (or S-0-0151)

How to carry out Safe homing (chronological sequence)

Carry out the safe homing procedure in the following order:

1. Start command "C0600 Drive-controlled homing procedure command".

   Drive carries out homing on channel 1.

2. Complete command "C0600 Drive-controlled homing procedure command".

   Control unit moves drive to (static home switch evaluation) or over (dynamic home switch evaluation) reference position for safe reference (P-0-3231).
3. In the case of manual actuation of home switch for channel 2, reference signal has to be triggered when drive is at reference position for channel 2.
4. Drive checks whether actual position value difference between channel 1 and channel 2 is smaller than "P-0-3229, Tolerance window for safe homing procedure".

When the safe homing procedure was successful, this is signaled in "P-0-3213, Safety technology operating status" and the safety function "Safely-monitored position" can be used.

☞ Any position errors in channel 1 of the size of the tolerance window (P-0-3229) will not be detected!

Commissioning example 5

Requirements

The following requirements must have been fulfilled so that the safe reference can be established in an NC-controlled way:

- Use incremental or distance-coded measuring system.
- Establish position data reference for channel 1 using NC-controlled homing.
- For establishing reference for channel 2, additional travel motion by the control unit has to be possible.
- Home switch for channel 2 can be evaluated either dynamically or statically.
- When an incremental measuring system is used, the distance between the reference point for channel 1 and channel 2 has to be greater than the tolerance window ("P-0-3229, Tolerance window for safe homing procedure" + 10%).

$$|\text{Reference point}_{\text{channel 2}} - \text{Reference point}_{\text{channel 1}}| < \text{P-0-3229} + 10\ \%$$

Presetting

The following parameter setting has to be made in the drive:

- "P-0-3210, Safety technology configuration": Evaluate home switch dynamically or statically and select corresponding edge evaluation in the case of dynamic evaluation
- "P-0-3229, Tolerance window for safe homing procedure": Content depends on whether home switch is to be evaluated statically or dynamically:
  - **Static evaluation** of the home switch: Enter positioning accuracy at home switch +10%
  - **Dynamic evaluation** of the home switch: Adjust according to formula below (value depends on delay of signals, as well as on homing velocity)

$$\text{P-0-3229}_{\text{min}} = 2 \times v_{\text{homing}} \times 1\ \text{ms}$$

- P-0-3231: Enter position of home switch edge channel 2. When using an incremental encoder, calculate the position as follows:

Reference distance=Reference point$_{\text{channel 2}}$ - Reference point$_{\text{channel 1}}$
P-0-3231 = S-0-0052 - S-0-0150 - reference distance or
P-0-3231 = S-0-0054 - S-0-0151 - reference distance

P-0-3231	Reference position for safe reference
S-0-0052	Reference distance 1 (or S-0-0054)
S-0-0150	Reference offset 1 (or S-0-0151)

How to carry out Safe homing (chronological sequence)

Carry out the safe homing procedure in the following order:

1. Establish reference for channel 1 in NC-controlled way.
2. Start command "C4000 Homing procedure command channel 2".

   Control unit moves drive to (static home switch evaluation) or over (dynamic home switch evaluation) reference position for safe reference (P-0-3231).
3. In the case of manual actuation of home switch for channel 2, reference signal has to be triggered when drive is at reference position for channel 2.
4. Drive checks whether actual position value difference between channel 1 and channel 2 is smaller than "P-0-3229, Tolerance window for safe homing procedure".
5. Complete command "C4000 Homing procedure command channel 2".

When the safe homing procedure was successful, this is signaled in "P-0-3213, Safety technology operating status" and the safety function "Safely-monitored position" can be used.

☞ Any position errors in channel 1 of the size of the tolerance window (P-0-3229) will not be detected!

6.5.3 Safe parking axis

Brief description

The drive function "parking axis" can be used in conjunction with integrated safety technology, too. When this is done, it is possible to acknowledge the safety state at the diagnostic output.

For a detailed description of the drive function "parking axis", see the Functional Description of the firmware.

☞ Using the safety function "Safe parking axis" requires the optional safety technology module "S2" which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

Features

The safety function "Safe parking axis" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- The output stage is locked via two channels for the duration of the parking axis.
- For the safety function "Safe parking axis" there isn't any encoder monitoring function active. This means that the monitoring functions for speed, acceleration and position are deactivated.
- Acknowledgment of safety with the corresponding result of the risk analysis.

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safe parking axis":

- P-0-3210, Safety technology configuration
- P-0-3213, Safety technology operating status
- P-0-3215, Selected safety technology operating status

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the safety function "Safe parking axis":

- F3131 Error when checking acknowledgement signal
- F3140 Safety parameters validation error
- F7040 Validation error parameterized - effective threshold
- F7042 Validation error of safe operation mode
- F7043 Error of output stage interlock
- F8129 Incorrect optional module firmware
- With safe parking axis activated, the display of the IndraDrive control panel shows "PA".

Safety function

Selecting the function

The safety function "Safe parking axis" is active after safety technology has been activated and the drive function "parking axis" has been selected. For how to proceed to activate the drive function "parking axis", see the Functional Description of the firmware.

Monitoring functions

With the safety function "Safe parking axis", the following monitoring functions are **deactivated**:

- Monitoring functions of the measuring systems
- Monitoring functions regarding speed, acceleration and position

☞ The missing speed information can be replaced via the control bit "defined safety with parked axis" in "P-0-3210, Safety technology configuration".

The control bit signals safety which has to result from the risk analysis of the installation. Using the function for axes with long coasting times (grinding wheels, spindles, rolls, ...) must be excluded.

☞ It is possible to use either the safety function Safe braking and holding system **or** the function "defined safety with parked axis". A combination of both functions cannot be parameterized.

Acknowledging safety

When the control bit "defined safety with parked axis" has been set in "P-0-3210, Safety technology configuration", the following axes will acknowledge safety with the safety function "Safe parking axis" having been activated:

- Axes with single acknowledgment at the diagnostic outputs O10 and IO10n
- Diagnostic slave axes at the diagnostic outputs O10 and IO10n, as well as via the I/O20 bus to the diagnostic master
- Diagnostic master axes with feedback to a PLC at the diagnostic outputs O10 and IO10n, when the diagnostic slaves signal safety

- Diagnostic master axes with control of a safety door at the diagnostic outputs O10 and IO10n, when the diagnostic slaves signal safety and dual-channel selection has been made via the mode selector

6.5.4 Safe brake check

Brief description

☞ The safe brake check is not an independent safety function, but the basis of the "Safe braking and holding system".

To achieve safety according to EN ISO 13849-1 Category 3 PL d and IEC EN 62061 SIL 2 for the "Safe braking and holding system", it is necessary to check the function and the holding torque of the two holding brakes in regular intervals. The check is run within the scope of the command "C2100 Command Holding system check". The regular check is normally ensured by dual-channel, parameterizable time monitoring, unless the function made available with MPx08 and above has been configured as a special case: "Brake check only upon access request".

Special case: "Brake check only upon access request"

To avoid interrupting the automatic operation at a "random" point, it is possible with MPx08 and above to configure P-0-3300 in such a way that the error F3115 or the prewarning E3115 will not be generated at the end of "time interval brake check".

⚠ WARNING **Dangerous movements! Danger to life, risk of injury, serious injury or property damage!**

Configuring the special case "brake check only upon access request" is only allowed if it has been ensured by appropriate measures that the user cannot access the danger zone of a gravity-loaded axis until a valid brake check status exists. The machine manufacturer must carry out a risk analysis.

As the brake check request is missing in normal operation, the holding system check risks not being carried out over longer operating times or downtimes. The user is responsible for carrying out a brake check in regular intervals by means of the command "C2100 Command Holding system check", because only this procedure guarantees that the holding torques of motor brake and/or redundant holding brake are sufficient!

Features

The auxiliary safety technology function "Safe brake check" has the following features:

- Is suited for safety-relevant applications up to Category 3 PL d according to EN ISO 13849-1 or up to SIL 2 according to IEC EN 62061.
- Parameterizable time interval in which the safe brake check must be repeated.
- MPx08 and above: The special case "brake check only upon access request" can be configured.
- When control voltage is switched off, the brake status of the two brakes is set to "not successful".
- Holding torque of the two holding brakes can be checked in positive, negative or in both directions.
- The command "C2100 Command Holding system check" is executed with the encoder set in S-0-0520, bit 0. The safety technology always monitors the check with the encoder connected to X4.

- MPx08 and above: Different test torques are possible for the motor holding brake and the redundant holding brake.
- Check for releasing the two holding brakes.
- Monitoring of the actual load torque of the holding system.
- The auxiliary safety technology function "Safe brake check" is the prerequisite for using the safe braking and holding system.
- MPx08V04 and above: Activating the command "S-0-0139, C1600 Parking axis procedure command" sets the brake status to "not successful"

Pertinent parameters

The following parameters are used in conjunction with the auxiliary safety technology function "Safe brake check":

- S-0-0520, Control word of axis controller
- P-0-0525, Holding brake control word
- P-0-0539, Holding brake status word
- P-0-0540, Torque of motor holding brake
- P-0-0541, C2100 Holding system check command
- P-0-0542, C2000 Command Release motor holding brake
- P-0-0543, C3800 Command Apply motor holding brake
- P-0-0545, Test torque for releasing holding system
- P-0-0546, Starting torque for releasing holding system
- P-0-0547, Nominal load of holding system
- P-0-0549, Oper. hours control section at last successful brake check
- P-0-0550, Time interval brake check
- P-0-0551, Current load torque
- P-0-3300, Redundant holding brake: Configuration
- P-0-3301, Redundant holding brake: Status word
- P-0-3302, SBS: Time interval brake check
- P-0-3303, SBS: Nominal load
- P-0-3304, SBS: Torque/force constant
- P-0-3306, SBS: Delay time motor holding brake
- P-0-3307, SBS: Safety technology - drive off delay time
- P-0-3310, SBS: Travel range brake check
- P-0-3311, SBS: Duration test torque injection brake check

Additionally in MPx08 and above:

- P-0-3305, SBS: Safety technology drive On delay time
- P-0-3316, SBS: Test torque factor motor holding brake
- P-0-3317, SBS: Test torque factor redundant holding brake

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the auxiliary safety technology function "Safe brake check":

- E3115 Prewarning, end of brake check time interval
- F3115 Brake check time interval exceeded
- E3116 Nominal load torque of holding system reached
- F3116 Nominal load torque of holding system exceeded
- F3122 SBS: System error

- F3123 SBS: Brake check missing
- F3147 System error channel 1
- F7051 Safely-monitored deceleration exceeded
- F8134 SBS: Fatal error
- C2100 Command Holding system check
- C2101 Holding system check only possible with drive enable
- C2103 Motor holding brake: Torque too low
- C2104 Command execution impossible
- C2105 Load of holding system greater than test torque
- C2106 Test torque of holding system not reached
- C2107 Redundant holding brake: Torque too low
- C2108 Error when releasing the holding system
- C2109 SBS: Test torque invalid

Functional description

With the brake check, the function of the two holding brakes is checked. The objective is to detect sleeping errors, soiling (fouling of the brake by oil, film rust on the friction surfaces of the brake) and wear.

The "Safe brake check" is started via the command "C2100 Command Holding system check" (P-0-0541).

☞ With MPx08, the parameter "P-0-3305, SBS: Safety technology drive On delay time" was implemented. With the appropriate parameterization, the time for releasing the brakes (motor brake and redundant holding brake) and the delay in the control of the redundant holding brake by the "HAT" control module can be taken into account.

Monitoring functions

The following aspects are checked:

- Releasing the "Safe braking and holding system": A check is run to find out whether the two holding brakes can be released. For this purpose, there is an attempt to move the axis by a distance greater than P-0-3310 and smaller than 2 * P-0-3310. If this is impossible, the command error "C2108 Error when releasing the holding system" is generated if the distance of axis motion is too small and the error "F3147 System error channel 1" is generated if the distance of axis motion is too big.
- The **holding torque of motor holding brake** in positive and negative direction is checked with the motor holding brake applied and the redundant holding brake released:
  - MPx07 and below: with the 1.3-fold torque of P-0-3303
  - MPx08 and above: with the torque parameterized in P-0-3303, multiplied with the factor parameterized in P-0-3316

  When this is done, the axis may not move, within the parameterized check time (P-0-3311), by more than the distance parameterized in P-0-3310; otherwise, the command error "C2103 Motor holding brake: Torque too low" is generated.
- The **holding torque of redundant holding brake** in positive and negative direction is checked with the motor holding brake released and the redundant holding brake applied:

– MPx07 and below: with the 1.3-fold torque of P-0-3303

– MPx08 and above: with the torque parameterized in P-0-3303, multiplied with the factor parameterized in P-0-3317

When this is done, the axis may not move, within the parameterized check time P-0-3311, by more than the distance parameterized in P-0-3310; otherwise, the command error "C2107 Redundant holding brake: Torque too low" is generated.

☞ To check the holding torque of the brakes, the value parameterized in P-0-0547, multiplied with P-0-3317, is used as test torque (MPx07 and below: fixed to 1.3). During the check, the safety technology monitors that the test torque reaches at least the value of P-0-3303, multiplied with P-0-3317 (MPx07 and below: fixed to 1.3).

☞ If brakes are used which generate the holding torque in one direction only or if the brake check is only possible in one direction due to the axis mechanics, the brake check can be carried out in direction-dependent form (P-0-3300).

☞ The brake check is carried out with the encoder parameterized in "S-0-0520, Control word of axis controller", bit 0. The safety technology always monitors the brake check with the encoder connected to X4.

To eliminate the risk of backlash between the two measuring systems causing one or both brakes to be checked as faulty, it is recommended to select the encoder connected to X4 in S-0-0520, bit 0, for the duration of the brake check.

The user-side performance of the "Safe brake check" is monitored, too. Depending on the status of the safe brake check and the selected operating status (normal operation/special mode), the following diagnostic messages are possible:

Status "Safe brake check" (P-0-0539, P-0-3301)	Selection normal operation/special mode	Drive enable < 10s	Drive enable	Drive enable and special case "brake check only upon access request"
Not successful	Normal operation	No warning, no error	0-5 min. after end of "Safe brake check" status → No warning / no error	No warning, no error
			5-15 min. after end of "Safe brake check" status → E3115	
			> 15 min. after end of "Safe brake check" status → F3115	
	Special mode	→ F3123	→ F3123	→ F3123

Status "Safe brake check" (P-0-0539, P-0-3301)	Selection normal operation/special mode	Drive enable < 10s	Drive enable	Drive enable and special case "brake check only upon access request"
Successful	Normal operation	No warning, no error	15-0 min. before end of "Safe brake check" status → E3115	No warning, no error
			> 15 min after end of "Safe brake check" status → F3115	
	Special mode	No warning, no error	15-0 min. before end of "Safe brake check" status → E3115	
			> 15 min. after end of "Safe brake check" status → F3115	

Tab. 6-11: Drive reaction depending on "Safe brake check" status (P-0-0539 and P-0-3301)

After control voltage was switched on, the status of the motor holding brake in P-0-0539 and the status of the redundant holding brake in P-0-3301 are set to "not successful".

After successful safe brake check, the status "Safe brake check" is set to "successful" for the time parameterized in P-0-3302 and reset to "not successful" after this time is over. The time interval for the brake check is monitored on the basis of the operating hours of the control section; i.e. the brake status "successful" is set to "not successful" again after the parameterized time is over, independent of whether the drive is in control or not.

Commissioning

The command "C2100 Command Holding system check" can only be started in normal operation and under drive enable.

☞ If such states can occur at the installation in which the axis must be moved in special mode before the brake check, the axis can be moved under defined conditions via the command "C6200 Command Enabling SM without valid brake status" (see "Enabling the Special Mode Without Valid Brake Status") .

☞ The brake check is carried out with the encoder parameterized in "S-0-0520, Control word of axis controller", bit 0. The safety technology always monitors the brake check with the encoder connected to X4.

To eliminate the risk of backlash between the two measuring systems causing one or both brakes to be checked as faulty, it is recommended to select the encoder connected to X4 in S-0-0520, bit 0, for the duration of the brake check.

NOTICE **Property damage caused by collisions with other axes when carrying out the brake check!**

⇒ On user-side and control-unit-side, make sure that collisions with other axes are avoided when the brake check is carried out.

After control voltage was switched on, the status of the motor holding brake in P-0-0539 and the status of the redundant holding brake in P-0-3301 are always set to "not successful". Therefore, a brake check has to be carried out in order to use the Safe braking and holding system.

Standard case

To allow the command C2100 to be carried out in a position defined by the user or the control unit, there is no warning or error displayed at first. Activating drive enable starts the "rest time" of 5 minutes, before the warning E3115 appears for another 10 minutes. After 15 minutes under drive enable, the error message F3115 is generated if the command C2100 has not been carried out successfully.

The error F3115 can be cleared. Then the procedure described in the preceding paragraph is started again.

MPx08 and above: Special case "brake check only upon access request"

In **normal operation**, the warning E3115 and the error message F3115 are not generated. The user is responsible for regularly carrying out the command "C2100 Command Holding system check".

With command C2100 carried out successfully, the status "Safe brake check" is set to "successful". The time monitoring P-0-3302 is started again. 15 minutes before the end of the time interval, the warning E3115 is displayed again.

☞ When guards are used, a brake check should be carried out before the safety door is opened; this gives the user the maximum time (and safety) with safe feedback.

6.5.5 Enabling the special mode without valid brake status

Brief description

With the command "C6200 Command Enabling SM without valid brake status", it is possible to cause the enabling of the special mode under defined conditions, as a one-time event for the duration of a maximum of 15 minutes, although the brake status (status of holding brake check P-0-0539/P-0-3301) is invalid. This allows the axis to be moved manually in the special mode (after an error or E-Stop, for example) to an appropriate position for the brake check. The brake check itself can only be carried out after the command C6200 has been completed and only in normal operation.

⚠ WARNING

Possible personal injury and property damage, since the holding torques of motor brake and/or redundant holding brake are not sufficient!

If the point of time of the last brake check "C2100 Command Holding system check" has passed for a long operating time or downtime, the holding torques of motor brake and/or redundant holding brake might no longer be sufficient; an error in the safe braking and holding system cannot be excluded any longer! This can only be clarified in a brake check.

The command C6200 must have been enabled during commissioning. The command should only be enabled and used after a risk assessment.

Features

The command C6200 has the following features:

- The command C6200 must have been enabled during commissioning.
- The command C6200 can only be executed, if

  - it had not yet been executed (only allowed once per control voltage ON),
  - the safety function "Safe braking and holding system" is active,
  - the brake status of motor brake and/or redundant holding brake is invalid ("status of holding brake check"="carried out without success"),
  - the operating mode is active and
  - the command C2100 is not active at the same time.
- The special mode is only enabled for a maximum of 15 minutes, by
  - setting the status of holding brake check of the motor brake and the status of the redundant holding brake to "successful" and
  - setting the remaining time of the brake check interval to 15 minutes.
- The command C6200 has to be reset before the command C2100 is executed.

Pertinent parameters

The following parameters are used in conjunction with the command C6200:

- P-0-3315, C6200 Comm. Enabling SM without valid brake status
- P-0-3300, Redundant holding brake: Configuration
- P-0-3301, Redundant holding brake: Status word
- P-0-3302, SBS: Time interval brake check
- P-0-0539, Holding brake status word
- P-0-0541, C2100 Holding system check command

Pertinent diagnostic messages

The following diagnostic messages can be generated in conjunction with the command C62:

- C6200 Comm. Enabling SM without valid brake status
- C6201 Command execution impossible
- F3123 SBS: Brake check missing
- F3115 Brake check time interval exceeded
- C2100 Command Holding system check

Functional description

With the command "C6200 Command Enabling SM without valid brake status", the machine operator can - under defined conditions - move an axis with Safe braking and holding system in the special mode without valid brake status (P-0-0539 and P-0-3301).

⚠ WARNING

Dangerous movements! Danger to life, risk of injury, serious injury or property damage, as the holding torques of motor brake and/or redundant holding brake are not sufficient!

The command "C6200 Command Enabling SM without valid brake status" may only be used, when the use of the command was taken into account in the risk analysis of the installation ("danger to persons in the safety area due to brake defect").

If the point of time of the last brake check "C2100 Command Holding system check" has passed for a long operating time or downtime, the holding torques of motor brake and/or redundant holding brake might no longer be sufficient! Only the brake check can give information about the holding torques.

Moving the axis in special mode without the brakes having been checked causes additional dangers for the operator! This requires the following measures:

- The machine manual must contain explicit information on the additional danger caused when the axis is moved in special mode without the brakes having been checked.
- The operator must be informed (e.g., within the scope of a training course) on the additional danger caused when the axis is moved in special mode without the brakes having been checked.
- It may only be possible to start the command C62 at the machine in the specific safety technology context (key switch, warning on the display, ...).

The command is active for a maximum of 15 minutes and can only be started once per control voltage ON.

The command is destined for special cases in which it is impossible to comply with the standard procedure; such cases are, for example:

- Restart of an axis with automatic, position-dependent selection of the special mode
- Manual release of the axis after E-Stop or error

Starting command C6200

Requirements for starting the command C6200:

- The intention to use the command was defined at commissioning and the use of the command was taken into account in the risk analysis of the machine.
- The safety function "Safe braking and holding system" is active (P-0-3300).
- The brake states of motor brake and/or redundant holding brake are invalid ("status of holding brake check"="carried out without success").
- The command C6200 had not yet been executed (only allowed once per control voltage ON).
- The operating mode is active.
- The command C2100 is not active.

When the requirements have been fulfilled, the following **actions** are carried out by starting the **command C6200**:

- The brake states of motor brake and redundant holding brake are set to valid ("status of holding brake check"="successful").

- The time remaining up to the next brake check (P-0-3302) is set to 15 minutes.
- The warning "E3115 Prewarning, end of brake check time interval" is suppressed in favor of the diagnostic command message "C62".

While the command is active (max. 15 minutes), safety is acknowledged in the special mode. The possibly present error message F3123 can be cleared. The machine operator can now move the axis in the special mode to reach a position in which the brake check is possible. In this position, the brake check can be carried out after the special mode has been deselected and the command C6200 has been terminated.

The enabling of the special mode is removed by errors in the control circuit of the redundant holding brake. After 15 minutes, the enabling of the special mode is deactivated and the error F3115 is signaled.

When the command "C6200 Command Enabling SM without valid brake status" is terminated, the states of holding brake check of motor brake (P-0-0539) and redundant holding brake (P-0-3301) are set to "carried out without success" again.

6.6 Safety functions "Safe feedback"

6.6.1 Safe diagnostic outputs

Via safe diagnostic outputs, "safely detected states" are transmitted from the drive to other system components (e.g., control of safety relays, safety PLC) in order to initiate, from these system components, a reaction to the process.

☞ When PROFIsafe is used, the safe diagnostic message is not output via the safe diagnostic outputs, but the signal is handled as a PLC signal and constantly stored in the F-data to the control unit in the PROFIsafe protocol (see also "PROFIsafe").

6.6.2 Safe door locking

In a drive controller, it is possible to activate a diagnostic master for several axes within a protective zone which recognizes the safe state of these axes and controls the locking device of the safety door.

In the case of the safety function "Safe door locking", the locking device of an interlocking guard is controlled via two channels when all axes of this zone are in the safe state. The position monitor of the locking device is monitored, too.

☞ Position monitoring of the interlocking guard is still required.

☞ When PROFIsafe is used, safe control of the door locking device is not possible.

6.6.3 Safe inputs/outputs

Brief description

If the safe master communication PROFIsafe via PROFIBUS is used, the drive-internal safety functions are controlled via PROFIsafe. The safe 2-channel inputs (a maximum of 4 per axis) and the 2-channel safe output (one per axis) available in the drive can be made available to a higher-level safety PLC.

Sensors such as switches, E-Stop pushbuttons and light barriers can be connected to the safe inputs. Actuators such as contactors, valves and brake can be connected to the safe output.

☞ Using the function "Safe inputs/outputs" requires the optional safety technology module "S2" and the master communication PROFIBUS (PB) which can be selected as configuration for the control sections CSH01.1 or CSH01.3 (ADVANCED) and CDB01.1 (BASIC).

Features

The safety function "Safe inputs/outputs" has the following features:

- Is suited for safety-relevant applications up to PL d according to EN ISO 13849-1 Category 3 or up to SIL 2 according to IEC 62061.
- Safe inputs/outputs can only be used in conjunction with PROFIsafe.
- 3 or 4 safe inputs per axis in N/C-N/O combination. If the safe reference is used, only 3 safe inputs are available.
- 1 safe output per axis, optionally as Plus-Plus-switching output or Plus-Minus-switching output.
- The freely configurable digital inputs/outputs (24 V) for channel 1 can be realized in the following ways:
  - Using digital I/Os at the control section of the single-axis device (e.g. CSH01.1) at terminal connector X31 / 32
  - Using digital I/Os at the control section of the double-axis device (CDB01.1) at terminal connector X31 / X32 / X33 / X34
  - Using digital I/Os at an I/O extension (MD1) at terminal connector X10
- The digital inputs/outputs (24 V) for channel 2 are situated on the optional safety technology module "S2" at terminal connector X41.

Pertinent parameters

The following parameters are used in conjunction with the safety function "Safe inputs/outputs":

- P-0-0300, Digital I/Os, assignment list
- P-0-0301, Digital I/Os, bit numbers
- P-0-0302, Digital I/Os, direction
- P-0-0303, Digital I/Os, status display
- P-0-0304, Digital I/Os, outputs
- P-0-3211, Safety technology I/O configuration list, channel 2
- P-0-3212, Safety technology control word, channel 1
- P-0-3214, Safety technology status word, channel 1
- P-0-3216, Active safety technology signals
- P-0-3221, Max. tolerance time for different channel states
- P-0-3295, Safety technology field bus configuration
- P-0-3296, Safety technology field bus control word
- P-0-3297, Safety technology field bus status word

Configuring the Safe inputs/outputs

The digital inputs/outputs of the drive controller which are used have to be accordingly configured during safety technology commissioning:

- Digital inputs/outputs on the control section or an I/O extension (channel 1) have to be configured (like all other digital inputs/outputs in the drive) via the following parameters:
  - P-0-0300, Digital I/Os, assignment list
  - P-0-0301, Digital I/Os, bit numbers
  - P-0-0302, Digital I/Os, direction

See also Functional Description of firmware "Digital inputs/outputs"

- The digital inputs/outputs situated on the optional safety technology module have to be configured by means of "P-0-3211, Safety technology I/O configuration list, channel 2".

☞ To simplify commissioning, the IndraWorks D commissioning software provides a commissioning wizard.

Integrated safety functions

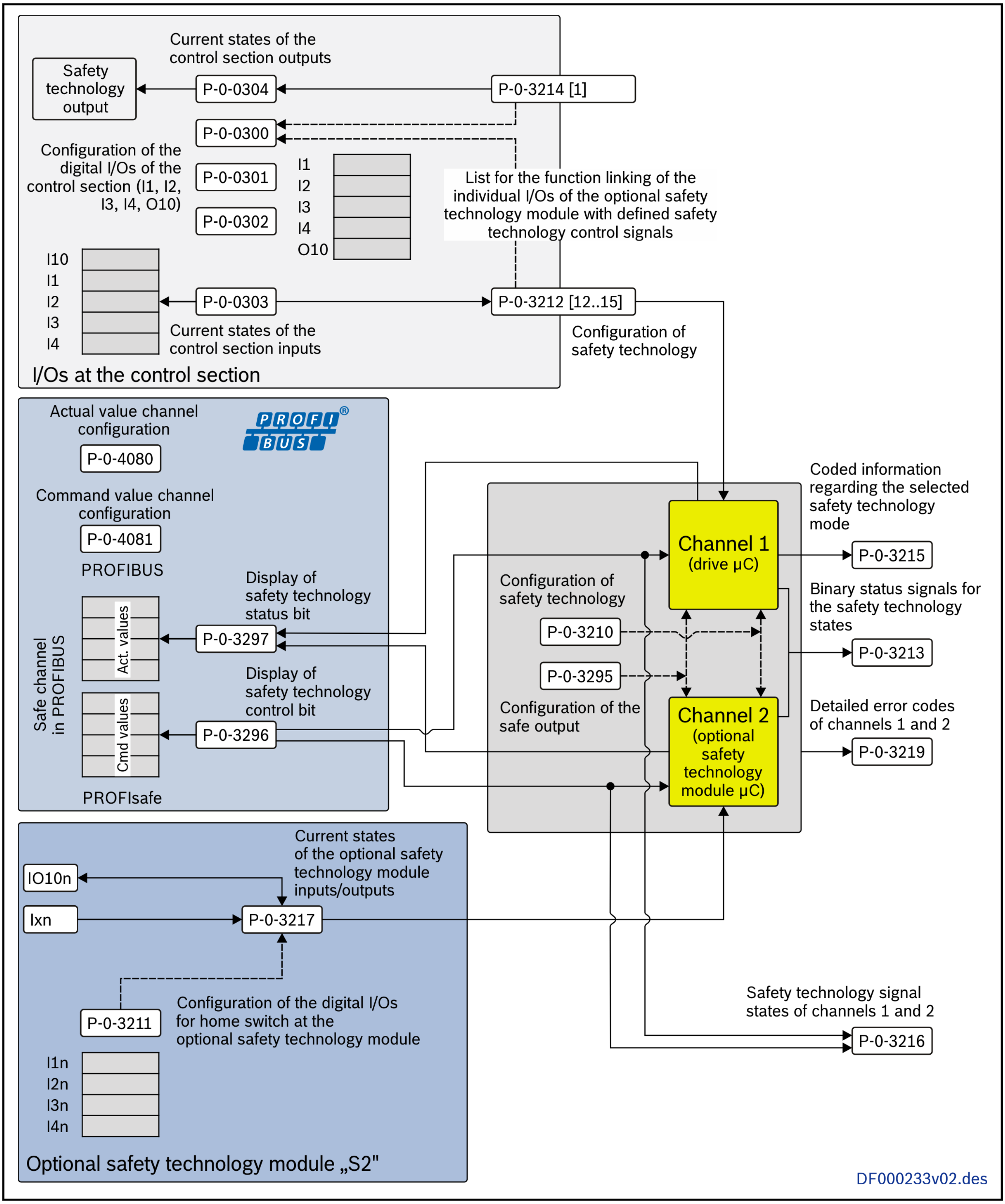

Current states of the control section outputs
Safety technology output
P-0-0304
P-0-3214 [1]
P-0-0300
Configuration of the digital I/Os of the control section (I1, I2, I3, I4, O10)
P-0-0301
P-0-0302
I1
I2
I3
I4
O10
List for the function linking of the individual I/Os of the optional safety technology module with defined safety technology control signals
I10
I1
I2
I3
I4
P-0-0303
P-0-3212 [12..15]
Current states of the control section inputs
Configuration of safety technology
I/Os at the control section
Actual value channel configuration
P-0-4080
PROFIBUS
Command value channel configuration
P-0-4081
PROFIBUS
Display of safety technology status bit
Act. values
P-0-3297
Display of safety technology control bit
Cmd values
P-0-3296
Safe channel in PROFIBUS
PROFIsafe
Coded information regarding the selected safety technology mode
Channel 1 (drive µC)
P-0-3215
Configuration of safety technology
Binary status signals for the safety technology states
P-0-3210
P-0-3213
P-0-3295
Configuration of the safe output
Channel 2 (optional safety technology module µC)
Detailed error codes of channels 1 and 2
P-0-3219
Current states of the optional safety technology module inputs/outputs
IO10n
Ixn
P-0-3217
P-0-3211
Configuration of the digital I/Os for home switch at the optional safety technology module
I1n
I2n
I3n
I4n
Optional safety technology module „S2"
Safety technology signal states of channels 1 and 2
P-0-3216
DF000233v02.des

Fig. 6-30: PROFIsafe communication and Safe inputs/outputs

Functional principle

Safe inputs

It is only possible to connect sensors of the N/C-N/O combination design to the safe inputs. As illustrated in the figure below, the connected sensors are dynamized by a dynamization master (drive or PLC) to detect "sleeping errors" (see "Dynamization").

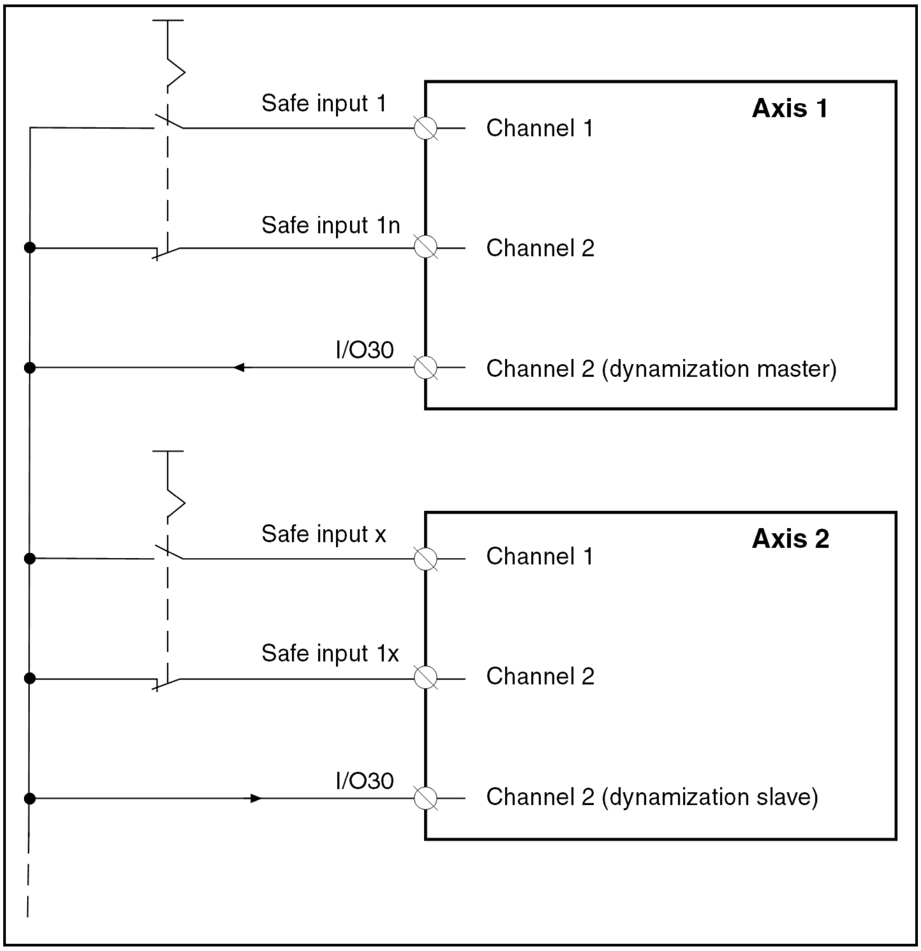


Fig. 6-31: Safe inputs with dynamization by the drive

The results of the signal evaluation of the safe inputs are not directly transmitted to the corresponding data container of the safety bus, as these results are synchronized due to the possibly different signal run times between channel 1 and channel 2. In the parameter "P-0-3221, Max. tolerance time for different channel states", it is possible to set the time within which the safe inputs of channel 1 and channel 2 may have different signal states.

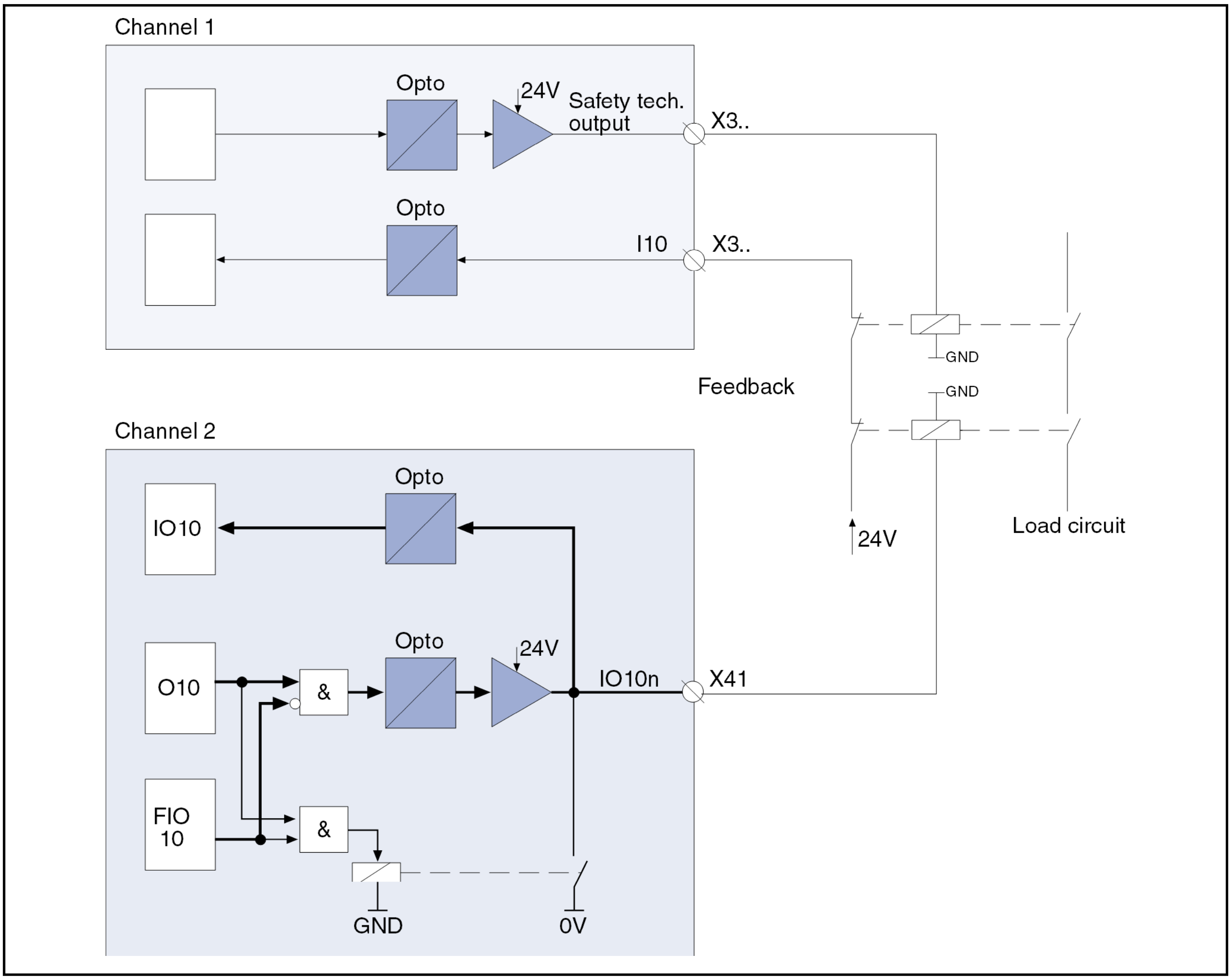
Safe output

The safe output can be designed in two types, as a Plus-Plus-switching output or a Plus-Minus-switching output. The safe output is activated and parameterized in parameter "P-0-3295, Safety technology field bus configuration".

Plus-Plus-switching output

In the Plus-Plus-switching design, the two outputs (channel 1 X3x and channel 2 X41) only switch one load circuit. In their active state, both channels output 24 V. Feedback on the current state of the load circuit takes place via two N/C contacts connected in series which are supplied with 24 V.

With non-activated safe output, the two channels are not controlled (open); the load circuit in this case is in the safe state (corresponds to "Safety Default" state).



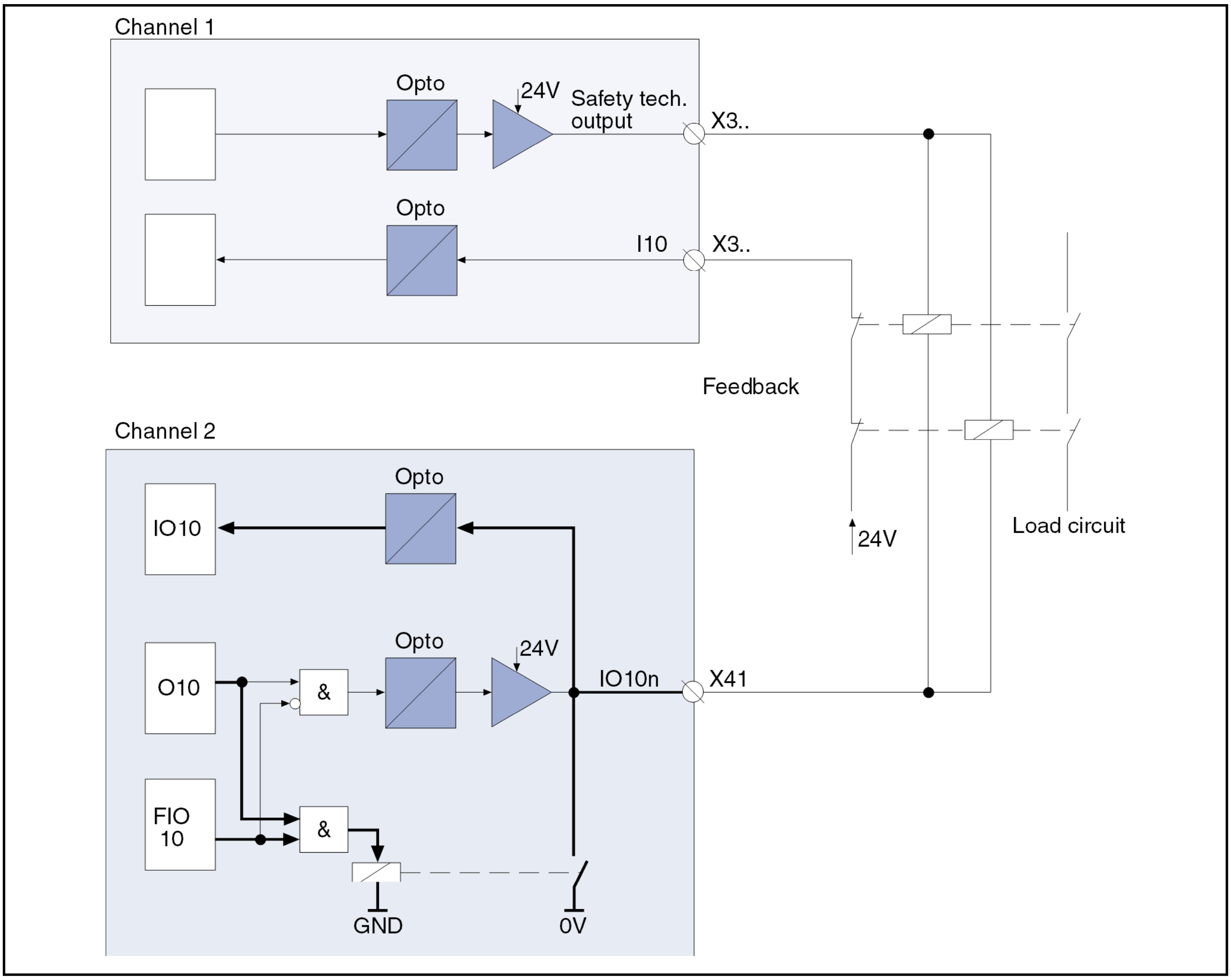
Note The active part in channel 2 has been marked bold.

Fig. 6-32: Plus-Plus-switching output

Plus-minus-switching output

In the Plus-Minus-switching design, channel 1 (X3x) is Plus-switching, i.e. output of 24 V when output active, and channel 2 (X41) is Minus-switching, i.e. output of 0 V when output active. This variant can be used for safe control of a coil (e.g. brake, contactor, ...). With activated safe output, both channels are controlled (channel 1 active => 24 V and channel 2 active => 0 V). Feedback on the current state of the load circuit takes place via an N/C contact which is supplied with 24 V.

With non-activated safe output, the two channels are not controlled (open) and the load circuit in this case is in the safe state (corresponds to "Safety Default" state).



Note The active part in channel 2 has been marked bold.

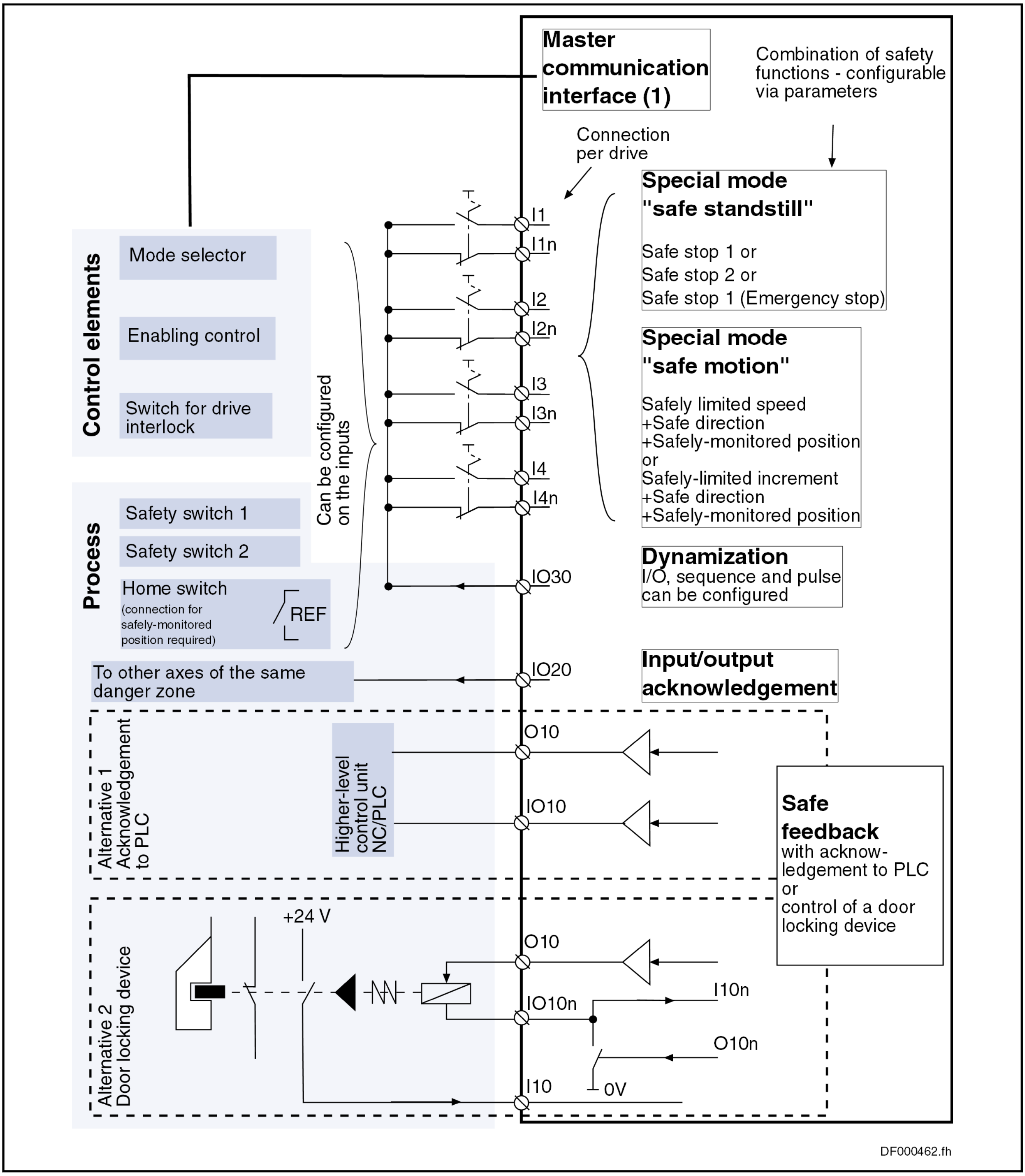
Fig. 6-33: Plus-minus-switching output

7 Examples of application

7.1 Overview

Functionality and connections for integrated safety technology at the IndraDrive controller.

Examples of application


Master communication interface (1)
Combination of safety functions - configurable via parameters
Connection per drive
Special mode "safe standstill"
Safe stop 1 or
Safe stop 2 or
Safe stop 1 (Emergency stop)
Special mode "safe motion"
Safely limited speed
+Safe direction
+Safely-monitored position
or
Safely-limited increment
+Safe direction
+Safely-monitored position
Dynamization
I/O, sequence and pulse can be configured
Input/output acknowledgement
Safe feedback
with acknow-ledgement to PLC
or
control of a door locking device
Control elements
Mode selector
Enabling control
Switch for drive interlock
Process
Safety switch 1
Safety switch 2
Home switch
(connection for safely-monitored position required)
REF
Can be configured on the inputs
To other axes of the same danger zone
Alternative 1 Acknowledgement to PLC
Higher-level control unit NC/PLC
Alternative 2 Door locking device
+24 V
I1
I1n
I2
I2n
I3
I3n
I4
I4n
IO30
IO20
O10
IO10
O10
IO10n
I10n
O10n
I10
0V
DF000462.fh

1	Alternatively, channel 1 can be selected via the master communication.
I1, .. , I4	Channel 1 for selection and reference input
I1n, .. , I4n	Channel 2 for selection inverted and reference input

Fig. 7-1: Overview

☞ A maximum of 4 safety functions can be selected at the inputs. I1 to I4 for channel 1 and I1n to I4n for channel 2. Configuration takes place via parameters.

7.2 Selecting normal operation/special mode with position monitoring of safety door with door locking device

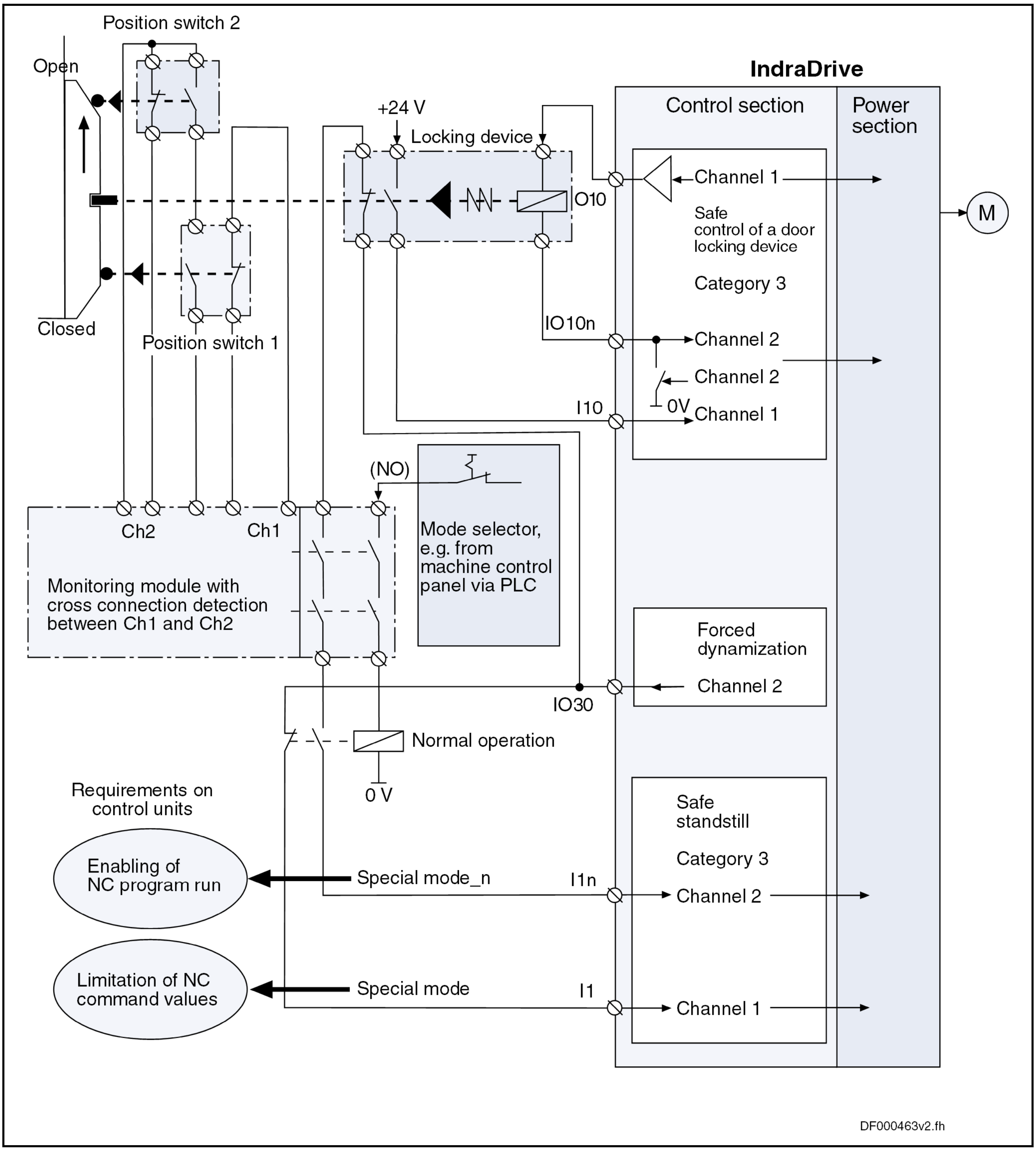


Fig. 7-2: Single-channel mode selector combined with position monitoring of a safety door with door locking device

Examples of application

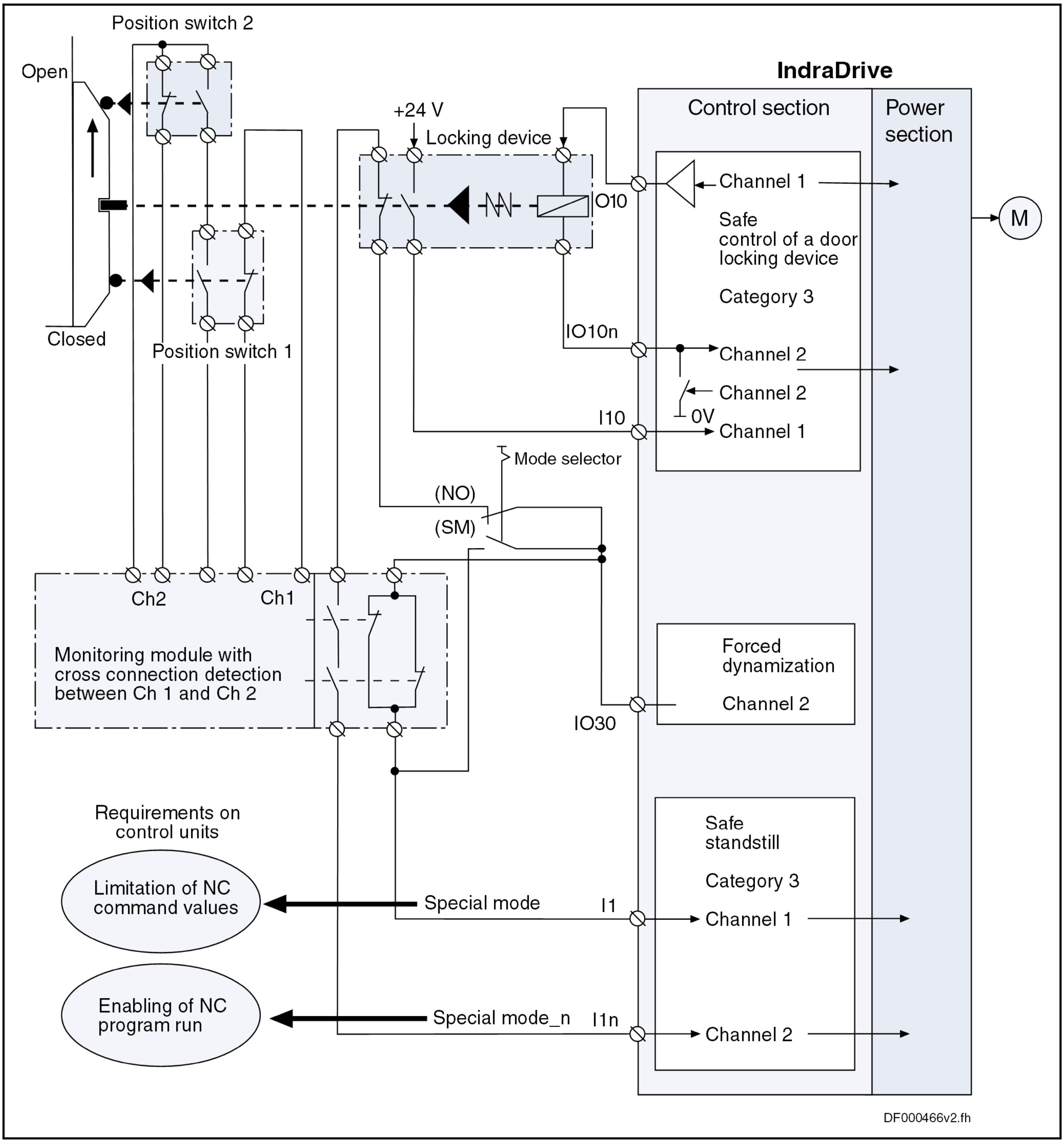


Fig. 7-3: Dual-channel mode selector combined with position monitoring of a safety door with door locking device

7.3 Enabling control with three positions

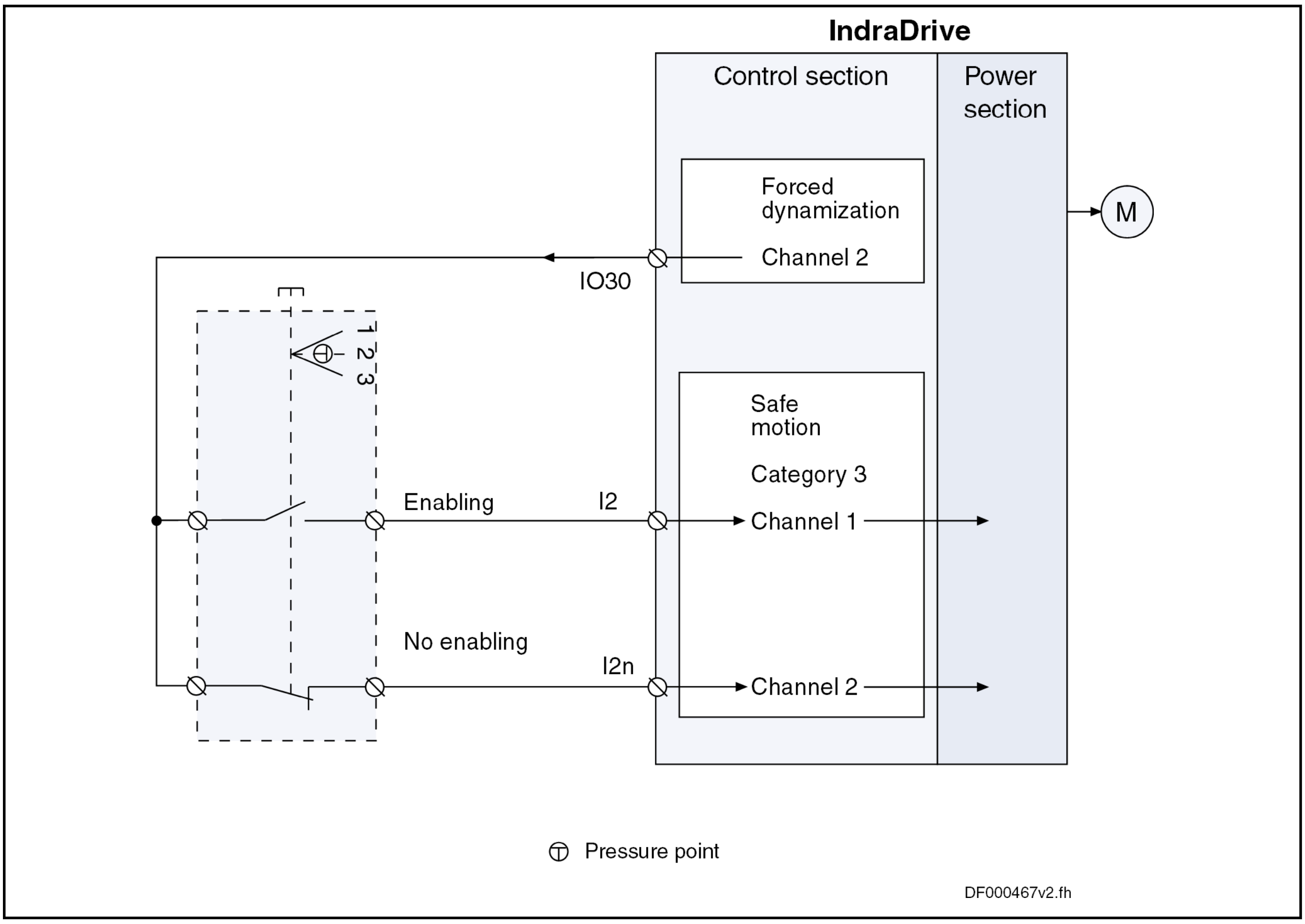


Fig. 7-4: Enabling control with three positions

7.4 Hold-to-run control device (safe hold-to-run pushbutton)

Control devices for safety-relevant applications must comply with PL d according to EN ISO 13849-1 Category 3. If this Performance Level cannot be reached, this function has to be combined with an enabling control.

☞ Possible control devices for initiating a safely-monitored motion:

- Single-channel hold-to-run pushbuttons (+/- direction) combined with a dual-channel enabling control. Enabling control is controlled according to PL d Category 3 as per EN ISO 13849-1.
- Single-channel preselection switches (+/- direction) combined with a dual-channel enabling control. Enabling control is at the same time hold-to-run pushbutton. Enabling control is controlled according to PL d Category 3 as per EN ISO 13849-1.
- Dual-channel hold-to-run pushbuttons (+/- direction). Hold-to-run control is controlled according to PL d Category 3 as per EN ISO 13849-1.

7.5 Temporary inspections or visual checks in the danger zone

If "Safe stop 2" is selected in special mode, a workpiece check can be carried out in the processing area / danger zone, for example.

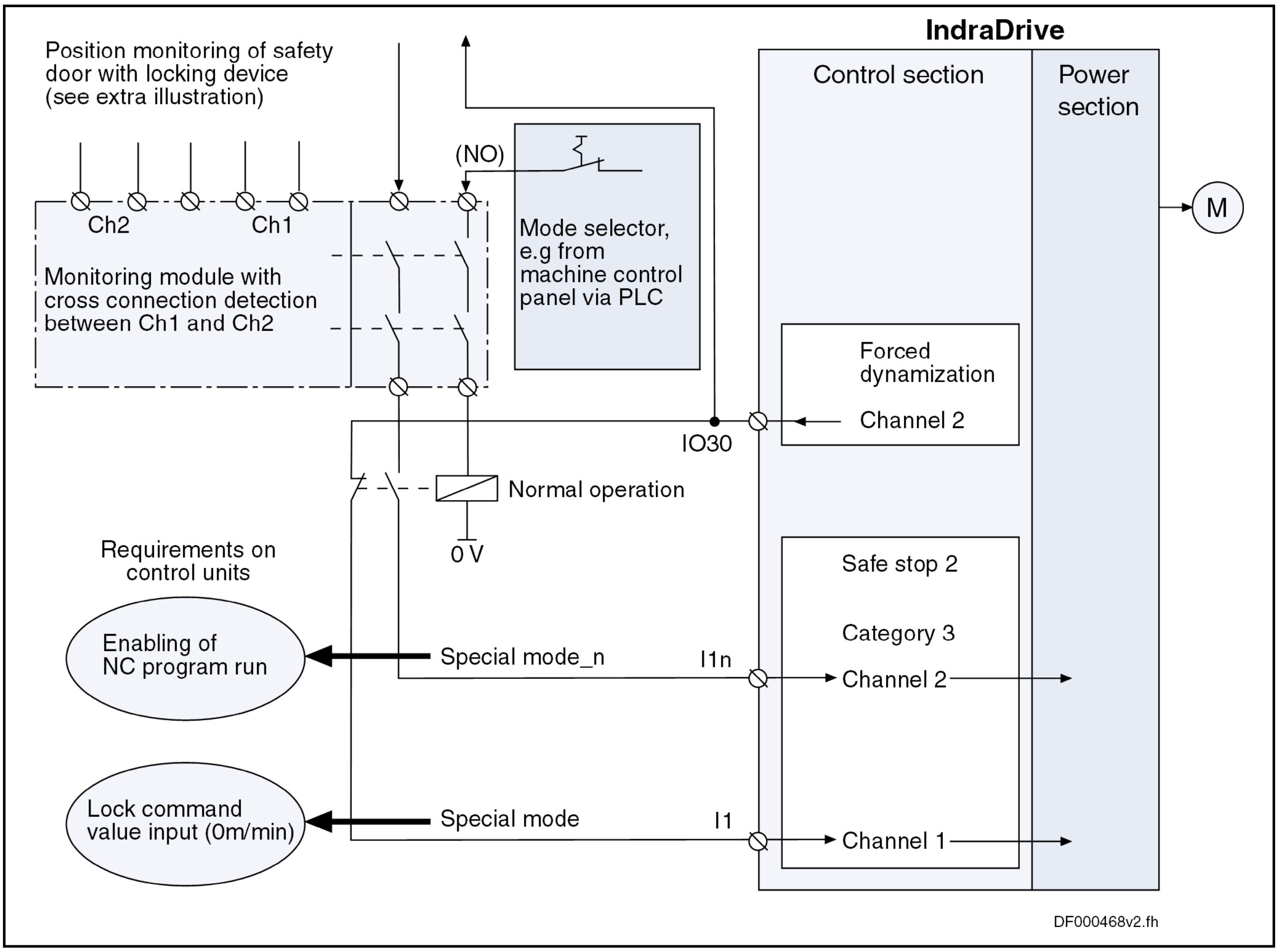

IndraDrive
Control section
Power section
M
Position monitoring of safety door with locking device (see extra illustration)
(NO)
Ch2
Ch1
Monitoring module with cross connection detection between Ch1 and Ch2
Mode selector, e.g from machine control panel via PLC
Forced dynamization
Channel 2
IO30
Normal operation
0 V
Requirements on control units
Enabling of NC program run
Special mode_n
I1n
Safe stop 2
Category 3
Channel 2
Lock command value input (0m/min)
Special mode
I1
Channel 1
DF000468v2.fh

Fig. 7-5: "Safe stop 2", drive is monitored for standstill

In special mode, movement for a visual check in the processing area / danger zone can be executed by actuating the enabling control (selecting Safely-limited speed) and by means of the travel command.

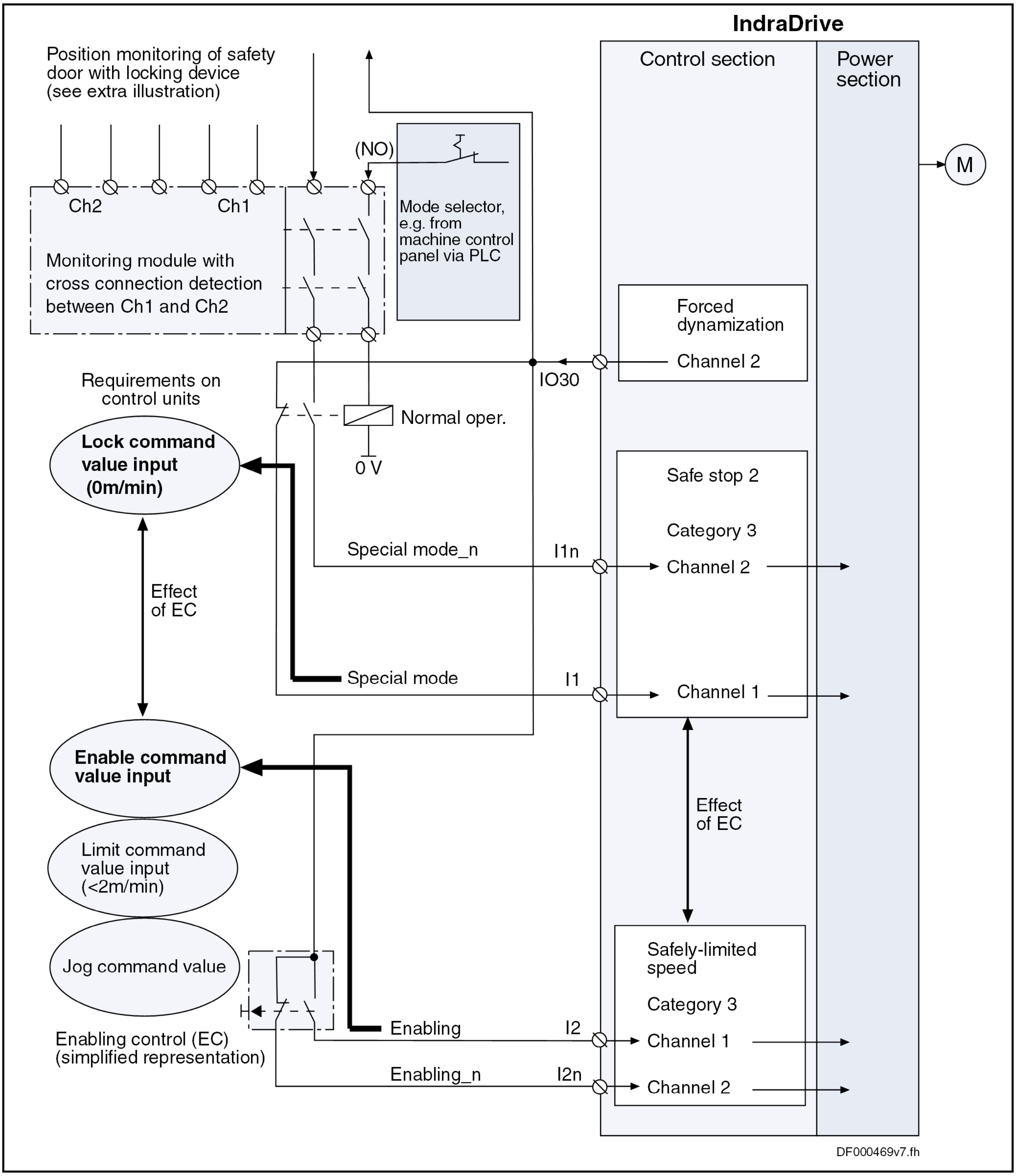

IndraDrive
Control section
Power section
M
Position monitoring of safety door with locking device (see extra illustration)
(NO)
Mode selector, e.g. from machine control panel via PLC
Ch2
Ch1
Monitoring module with cross connection detection between Ch1 and Ch2
Forced dynamization
Channel 2
IO30
Requirements on control units
Normal oper.
0 V
Lock command value input (0m/min)
Safe stop 2
Category 3
Special mode_n
I1n
Channel 2
Effect of EC
Special mode
I1
Channel 1
Enable command value input
Effect of EC
Limit command value input (<2m/min)
Safely-limited speed
Jog command value
Category 3
Enabling
I2
Channel 1
Enabling control (EC) (simplified representation)
Enabling_n
I2n
Channel 2
DF000469v7.fh

Fig. 7-6: "Safe stop 2" / "Safely-limited speed", drive is monitored for standstill / motion

7.6 Working when drive is without torque/force

If, for example, tools are to be changed manually, the function "Safe stop 1 (Emergency stop)" must be activated (separate switch in addition to the mode selector and the enabling control); in this way, it is possible to manually move the shaft using the tool spindle.

The power supply to the motor is interrupted in a safe way. No standstill monitor is active. "Safe stop 1 (Emergency stop)" cannot be disabled by actuating the enabling control.

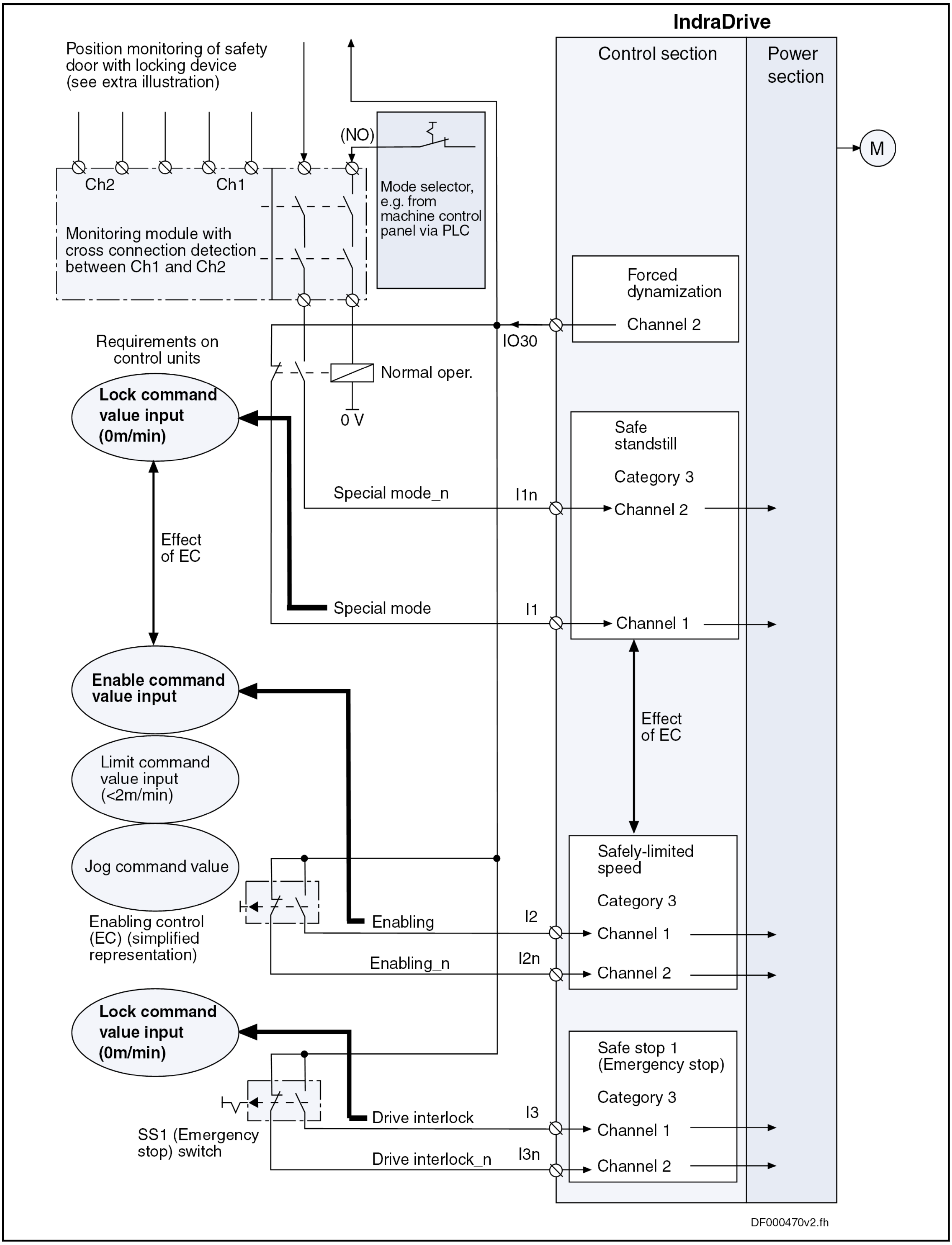

IndraDrive
Control section
Power section
M
Position monitoring of safety door with locking device (see extra illustration)
(NO)
Ch2
Ch1
Mode selector, e.g. from machine control panel via PLC
Monitoring module with cross connection detection between Ch1 and Ch2
Forced dynamization
Channel 2
IO30
Requirements on control units
Normal oper.
0 V
Lock command value input (0m/min)
Safe standstill
Category 3
Special mode_n
I1n
Channel 2
Effect of EC
Special mode
I1
Channel 1
Enable command value input
Effect of EC
Limit command value input (<2m/min)
Jog command value
Safely-limited speed
Category 3
Enabling
I2
Channel 1
Enabling control (EC) (simplified representation)
Enabling_n
I2n
Channel 2
Lock command value input (0m/min)
Safe stop 1 (Emergency stop)
Category 3
Drive interlock
I3
Channel 1
SS1 (Emergency stop) switch
Drive interlock_n
I3n
Channel 2
DF000470v2.fh

Fig. 7-7: "Safe stop 1 (Emergency stop)", power supply to the drive is interrupted

Examples of application

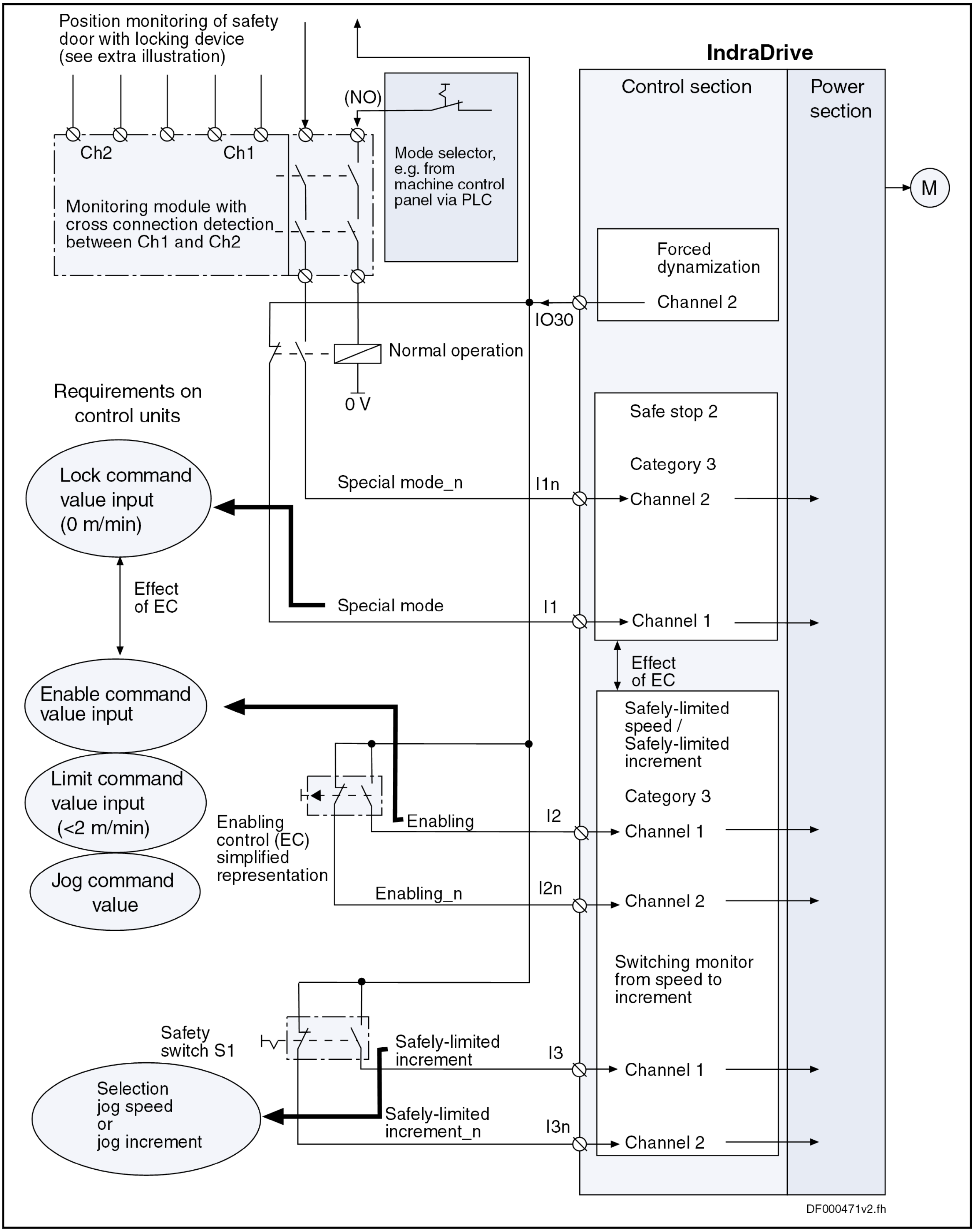

Position monitoring of safety door with locking device (see extra illustration)
IndraDrive
Control section
Power section
(NO)
Mode selector, e.g. from machine control panel via PLC
Ch2
Ch1
Monitoring module with cross connection detection_ between Ch1 and Ch2
M
Forced dynamization
Channel 2
IO30
Normal operation
0 V
Requirements on control units
Safe stop 2
Category 3
Lock command value input (0 m/min)
Special mode_n
I1n
Channel 2
Effect of EC
Special mode
I1
Channel 1
Effect of EC
Enable command value input
Safely-limited speed / Safely-limited increment
Category 3
Limit command value input (<2 m/min)
Enabling
I2
Channel 1
Enabling control (EC) simplified representation
Jog command value
Enabling_n
I2n
Channel 2
Switching monitor from speed to increment
Safety switch S1
Safely-limited increment
I3
Channel 1
Selection jog speed or jog increment
Safely-limited increment_n
I3n
Channel 2
DF000471v2.fh

Fig. 7-8: "Safely-limited speed" or "Safely-limited increment", drive is monitored for speed/standstill or increment/standstill

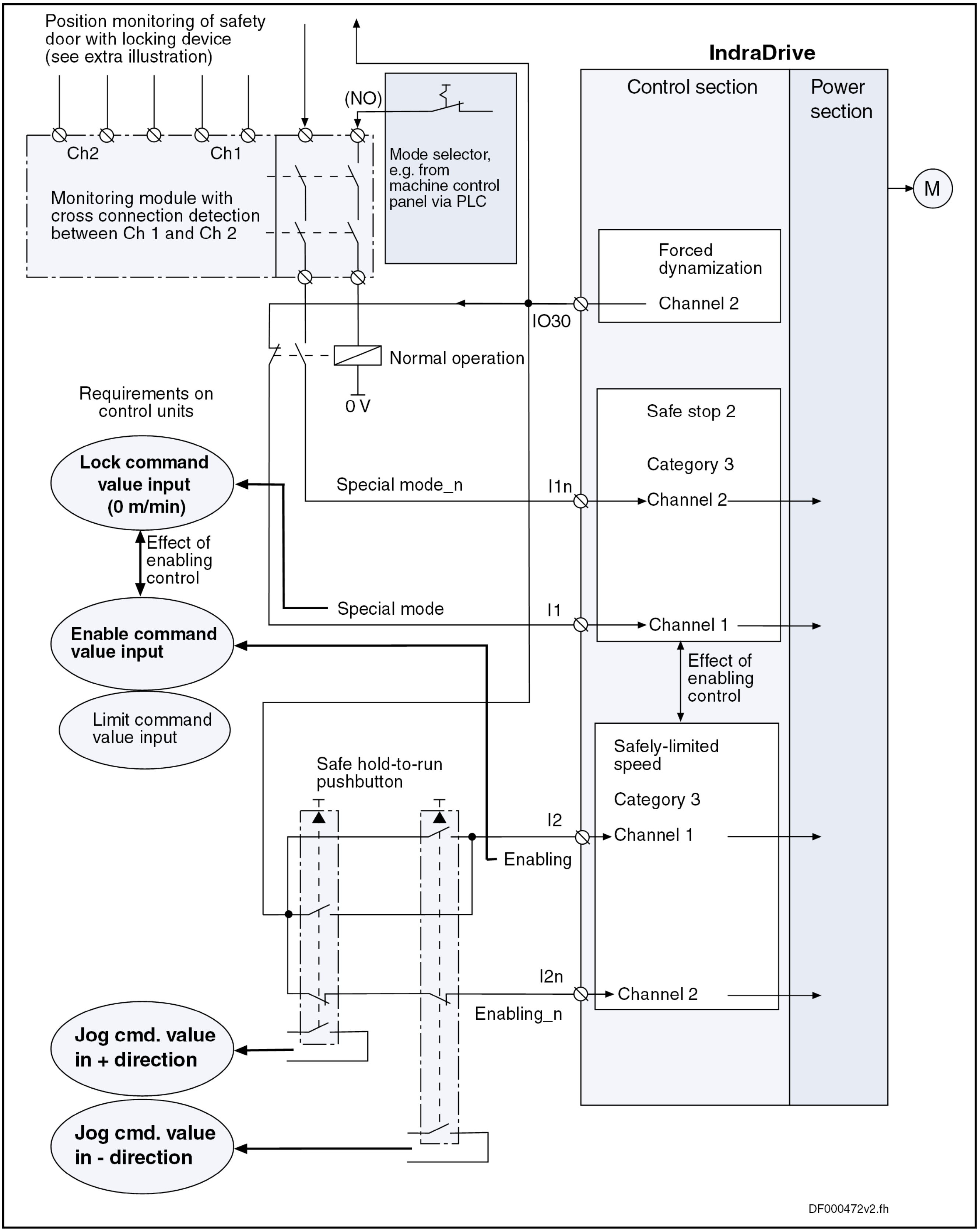

Position monitoring of safety door with locking device (see extra illustration)
Ch2
Ch1
Monitoring module with cross connection detection between Ch 1 and Ch 2
(NO)
Mode selector, e.g. from machine control panel via PLC
IndraDrive
Control section
Power section
M
Forced dynamization
Channel 2
IO30
Normal operation
0 V
Requirements on control units
Lock command value input (0 m/min)
Effect of enabling control
Enable command value input
Limit command value input
Safe stop 2
Category 3
Special mode_n
I1n
Channel 2
Special mode
I1
Channel 1
Effect of enabling control
Safely-limited speed
Category 3
Safe hold-to-run pushbutton
I2
Channel 1
Enabling
I2n
Channel 2
Enabling_n
Jog cmd. value in + direction
Jog cmd. value in - direction
DF000472v2.fh

Fig. 7-9: Hold-to-run control device (safe hold-to-run pushbutton)

☞ For information on the safe hold-to-run pushbuttons, please see "Hold-to-run control device (safe hold-to-run pushbutton)".

7.7 Drive groups for different danger zones

The figure below shows two machining areas of one machine. Each of these machining areas forms a separate danger zone.

The illustrated operating status is as follows:

- Danger zone A is in normal operation with drives A1, A2 and A3. The access door is closed.
- Danger zone B is in special mode with an open safety door and with drives B1, B2 and B3. One person is doing setup work or insertion work in the danger zone.

The door locking device is enabled or locked by the diagnosis master of a drive that belongs to the corresponding danger zone. Via the bidirectional connection I/O20, all drives in the corresponding danger zone are queried when switching from normal operation to special mode.

By means of the enabling control (not shown in the figure), the person can now move the drives in danger zone B.

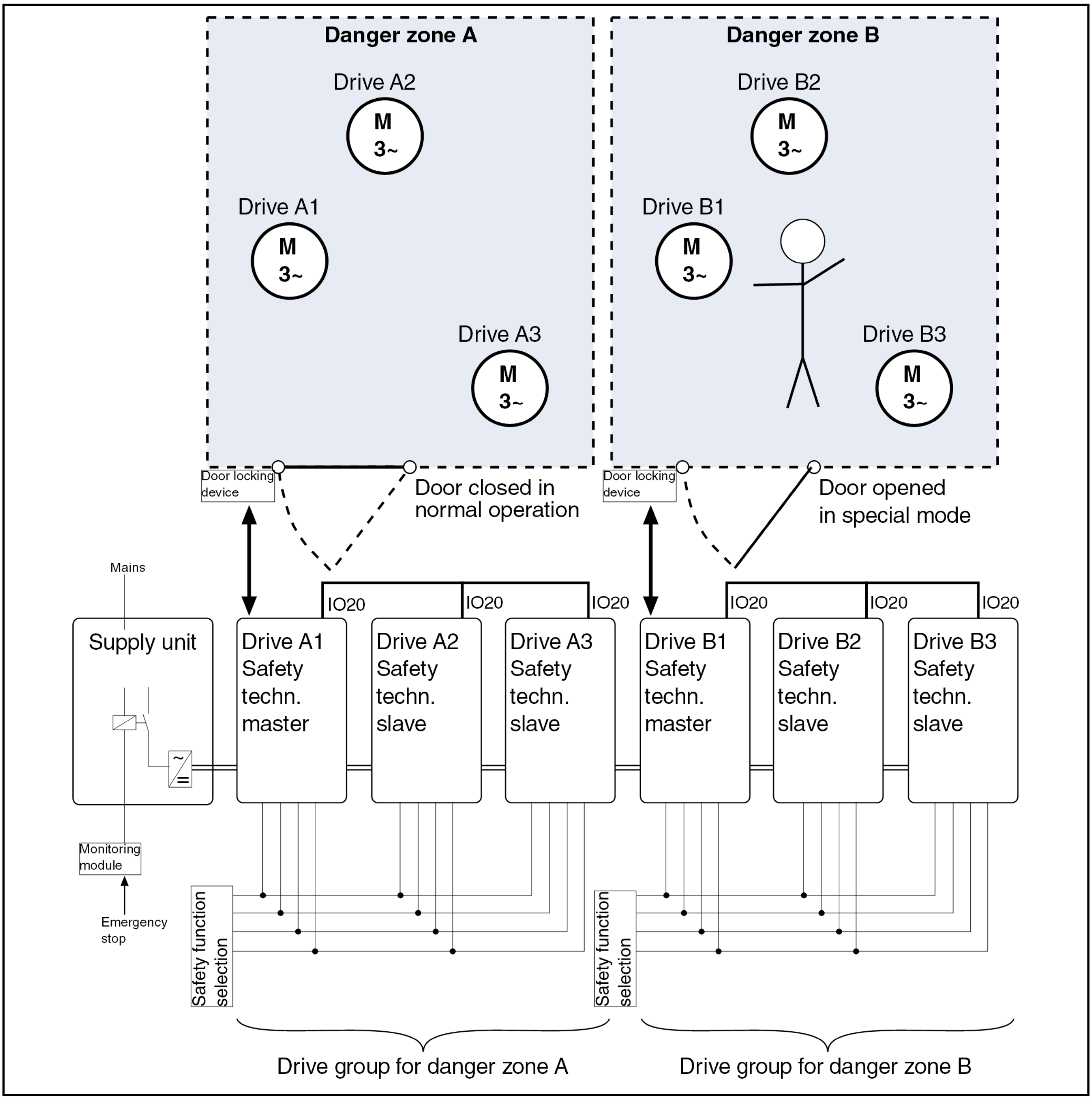

Danger zone A
Drive A2
M 3~
Drive A1
M 3~
Drive A3
M 3~
Danger zone B
Drive B2
M 3~
Drive B1
M 3~
Drive B3
M 3~
Door locking device
Door closed in normal operation
Door locking device
Door opened in special mode
Mains
IO20
IO20
IO20
IO20
IO20
IO20
Supply unit
Drive A1 Safety techn. master
Drive A2 Safety techn. slave
Drive A3 Safety techn. slave
Drive B1 Safety techn. master
Drive B2 Safety techn. slave
Drive B3 Safety techn. slave
Monitoring module
Emergency stop
Safety function selection
Safety function selection
Drive group for danger zone A
Drive group for danger zone B

Fig. 7-10: Drive groups for different danger zones

7.8 Safe control of the door locking devices of several safety doors

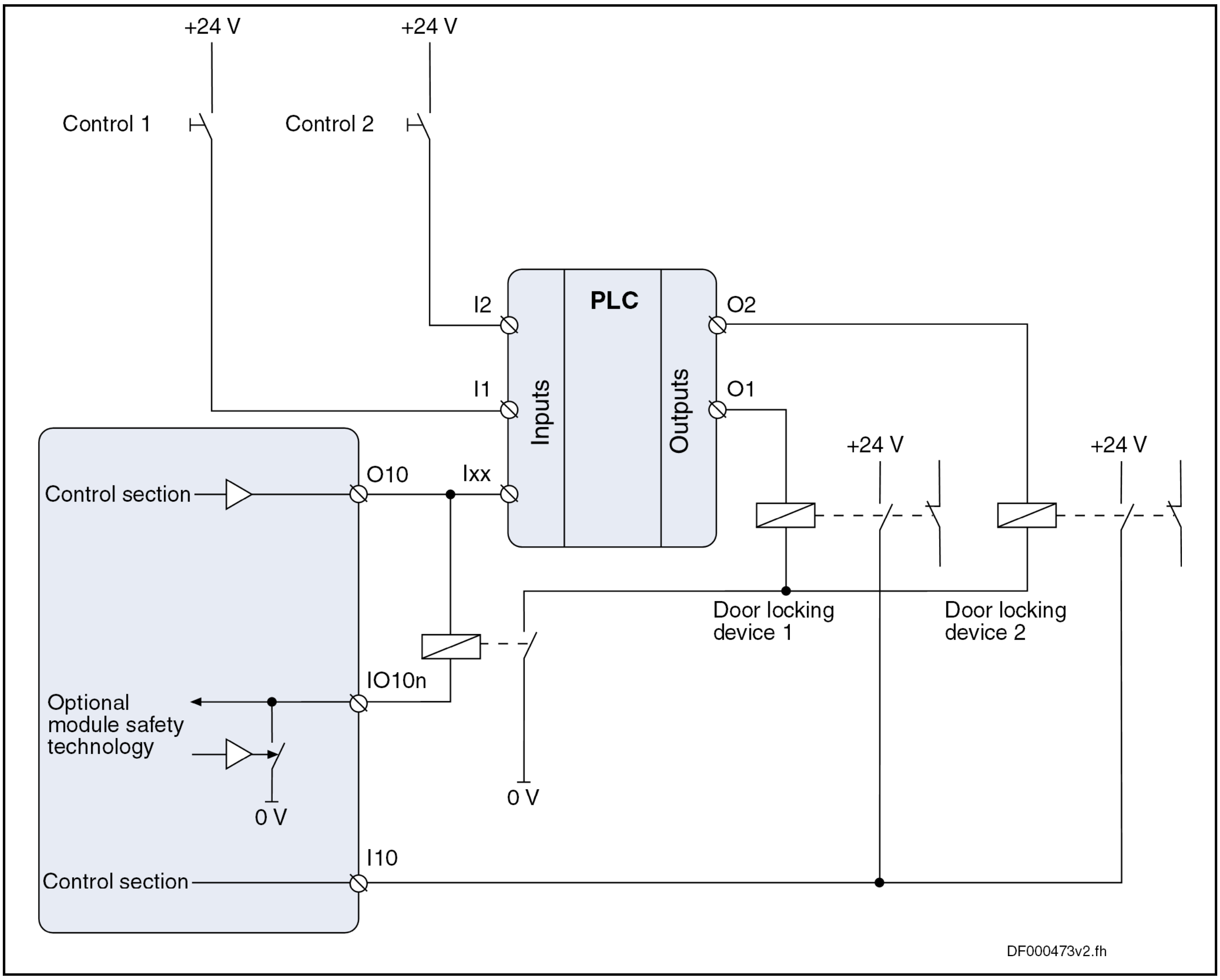


Fig. 7-11: Safe control of the door locking devices of two safety doors, with selection via standard PLC

8 Commissioning the safety technology

8.1 Introduction

The integrated safety technology is a dual-channel system in which a second processor redundantly carries out the monitoring functions. The processor uses the known system data of encoder, mechanics and scaling of the main system and stores them in the system/parameter memory. Changing these data is no longer allowed after safety technology has been commissioned. Changes are detected and acknowledged with error / warning. After the system was changed, it is necessary to commission the safety technology again.

All direct safety technology parameters are characterized by double input which is realized in such a way that individual parameters have to be written by a list of two equal values. Tables are of double size, the same table being attached as a copy. This allows a validation test of the data to be carried out, also in the case of an input via SERCOS monitor.

After parameterization and using the parameter verification tool made available by IndraWorks, the user has to verify all safety technology parameters and write-protect them by a password to be assigned by the user. The safety technology is activated at the same time that the password is assigned.

☞ For commissioning the safety technology, you should always use the current release of the corresponding firmware version and of the IndraWorks commissioning software.

Otherwise, take the corresponding manufacturer information on detected and solved problems into account and verify their relevance for the machine application.

For information on the current release and the manufacturer information, please refer to the "eBusiness Portal" under http://www.boschrexroth.com/portal.

8.2 Prerequisites for using integrated safety technology

8.2.1 General information

The IndraDrive system (axis / spindle / roll) consists of the components control section, power section and motor.

By the interaction of hardware and software components, IndraDrive provides the "Integrated Safety Technology".

☞ The mechanical parts of power transmission, such as gear and motor, and those of the safety devices (brakes, fall-down protection, arresting device, ...) shall be designed to withstand the occurring static and dynamic stresses (e.g., dual weight of the load).

The safety factor and the sizing are application-specific and have to be defined by the customer.

For the maximum gear input torque, too, a safety factor in relation to the maximum motor torque has to be taken into account. This also applies to motor-gearbox combinations by Bosch Rexroth. (See also documentation of the respective gearbox.)

8.2.2 Required drive firmware

The drive-integrated safety technology is a functionality only scalable by means of the hardware and does **not require any** additional **enabling of functional firmware packages**.

The integrated safety functions according to IEC 61508 via I/Os (optional module "S2") and the "Safe torque off" function (optional module "L2") can be used with the firmware version MPx07VRS and above.

See also Functional Description of firmware "Firmware types"

8.2.3 Required control section configuration

General information

To use the integrated safety technology of Rexroth IndraDrive controllers, the drive controller has to be configured/equipped with the corresponding optional safety technology module.

Optional safety technology module "Safe Torque Off" (L2)

Using the function "Safe torque off" requires the optional safety technology module "Safe Torque Off" (L2). The optional module "Safe Torque Off" can be configured for the following control sections:

- Single-axis BASIC UNIVERSAL (CSB01.1**C**)
- Single-axis BASIC SERCOS (CSB01.1N-**SE**)
- Single-axis BASIC PROFIBUS (CSB01.1N-**PB**)
- Single-axis BASIC Analog (CSB01.1N-**AN**)
- Single-axis ADVANCED (CSH01.1**C** and CSH01.3**C**)
- Double-axis BASIC UNIVERSAL (CDB01.1**C**)

☞ For pin assignments and technical data of the optional safety technology module "L2", please refer to the Appendix: "L2 - Safe Torque Off".

Optional safety technology module "Safe Motion" (S2)

The following control sections can use the integrated safety functions via I/Os, if they have been configured with the optional safety technology module (S2):

- Single-axis ADVANCED (CSH01.1**C** and CSH01.3**C**)
- Double-axis BASIC UNIVERSAL (CDB01.1**C**)

☞ Using the integrated safety technology requires one optional module "Safe Motion" (S2) **per axis** in conjunction with the firmware component.

For pin assignments and technical data of the optional safety technology module "S2", please refer to the Appendix: "S2 - Safe Motion".

PROFIsafe

The following control sections can use the integrated safety functions via PROFIBUS (PROFIsafe), if they have been realized with the optional safety technology module (S2) and the master communication PROFIBUS (PB):

- Single-axis ADVANCED (CSH01.1**C-PB** and CSH01.3**C-PB**)

- Double-axis BASIC UNIVERSAL (CDB01.1**C-PB**)

See also "Project Planning Manual for Control Section"

☞ Using the integrated safety technology requires one optional module "Safe Motion" (S2) **per axis** in conjunction with the firmware component and one PROFIBUS (PB) master communication module.

For pin assignments and technical data of the optional safety technology module "S2", please see the Appendix: "S2 - Safe Motion".

8.2.4 Required power sections

All power sections of the IndraDrive system have been designed for using the integrated safety technology.

8.2.5 Required motors and measuring systems

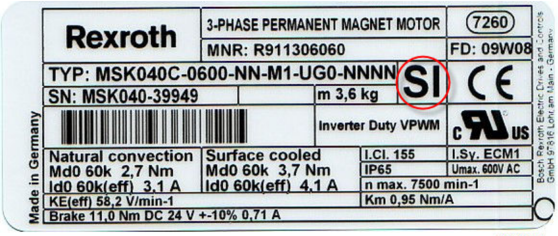
Rexroth motors

In conjunction with the optional safety technology module "Safe Torque Off" (L2), there are no specific requirements on the motor and the measuring system.

In conjunction with the optional safety technology module "Safe Motion", the following Rexroth **motors** can be used:

Motor line	Motor type code (placeholders "GG"/"G" and "B", see legend)	Encoder (placeholders "GG"/"G", see legend)	$\text{PFH}_{\text{Encoder}}$[2]	Brake (placeholder "B", see legend)	λ_{Brake}[3]	Suited for "Safe Motion"
IndraDyn S: MSK, MKE						
MSK	MSKxxxx-xxxx-NN-**GG**-Ux**B**-xxxx	S1, M1	$10*10^{-9}$ 1/h (at a DC of 90%)	0, 1, 2, 3	40 $*10^{-9}$ 1/h	All (with/ without safety technology label[1])
		S2, M2	$30*10^{-9}$ 1/h (at a DC of 90%)			Only with safety technology label[1]
MKE	MKExxxx-xxx-**G**x**B**-xxxN	A, C	$10*10^{-9}$ 1/h (at a DC of 90%)	0, 1	40 $*10^{-9}$ 1/h	All (with/ without safety technology label[1])
		B, D	$30*10^{-9}$ 1/h (at a DC of 90%)			Only with safety technology label[1]
IndraDyn A: MAD, MAF						
MAF	MAFxxxx-xxxx-xx-**GG**-xx**B**-xx-xx	S2, M2, C0	$30*10^{-9}$ 1/h (at a DC of 90%)	0, 1, 2, 3	40 $*10^{-9}$ 1/h	Only with safety technology label[1]
MAD	MADxxxx-xxxx-xx-**GG**-xx**B**-xx-xx					
MAx EEX		S6, M6				

x	"Don't care" positions in motor type code irrelevant for the requirements of integrated safety technology according to IEC61508
GG/G	Placeholders for position in type code at which encoder type is encoded
B	Placeholder for position in type code at which brake type is encoded
1)	The safety technology label is to be found on the type plate
2)	The specified value is PFH_d, i.e. the probability of dangerous failures
3)	Probability of **all failures** of the brake, **not only the number of dangerous failures**



Rexroth
3-PHASE PERMANENT MAGNET MOTOR
7260
MNR: R911306060
FD: 09W08
TYP: MSK040C-0600-NN-M1-UG0-NNNN
SI
CE
SN: MSK040-39949
m 3,6 kg
Inverter Duty VPWM
c UL us
Natural convection
Md0 60k 2,7 Nm
Id0 60k(eff) 3,1 A
Surface cooled
Md0 60k 3,7 Nm
Id0 60k(eff) 4,1 A
I.Cl. 155
I.Sy. ECM1
IP65
Umax. 600V AC
n max. 7500 min-1
KE(eff) 58,2 V/min-1
Km 0,95 Nm/A
Brake 11,0 Nm DC 24 V +-10% 0,71 A
Made in Germany
Bosch Rexroth Electric Drives and Controls GmbH 97816 Lohr am Main - Germany

DB000490

Fig. 8-1: Example of safety technology label on type plate

☞ "Mission Time" and "Proof Test" interval

- The "Mission Time" of all components used has to be observed and complied with. After the "Mission Time" of a component has elapsed, the component has to be discarded or replaced. It is not allowed to continue operating the component!
- The "Mission Time" of the motors listed in the above table is 175,200 h (20 years).
- After the component was discarded ("Mission Time" has elapsed), it has to be ensured that the component cannot be reused (e.g., by disabling it).
- If a component (with valid "Mission Time") is decommissioned, the "Mission Time" has to be recorded and continued when the component is commissioned again.
- The "Proof Test" has not been specified for Rexroth motors. Therefore, the "Mission Time" cannot be reset by a "Proof Test".

Third-party motors / optional measuring systems

In conjunction with the optional safety technology module "Safe Torque Off" (L2), there are no specific requirements on the motor and the measuring system.

In conjunction with the optional safety technology module "Safe Motion", the requirements on the **measuring system** used which are mentioned below must be complied with for **third-party motors** so that the measuring system can be used as a safety technology encoder:

☞ If it is not a motor encoder but an optional encoder which has been connected to the optional slot X4 (X4.1 and X4.2 for double-axis devices), this encoder must comply with the requirements below.

☞ Please observe that the encoder can also be evaluated by the corresponding encoder option (EN1, EN2, ENS) (see "Project Planning Manual for the control section").

When using the optional safety technology module "S2", it is **always** the encoder at the optional slot **X4** (X4.1 and X4.2 for double-axis devices) which is evaluated for the safety functions.

Sine/cosine encoder

Sine/cosine encoders must comply with the following requirements so that they can be used as safety technology encoders:

- **Signal generation:** The analog position signals (sin, cos) have to be generated and processed in analog form. Synthetic signal generation is not allowed.
- **Signal transmission:** The analog position signals (sin, cos) have to be transmitted in differential form. The differential signal amplitude levels have to be between 0.6 V_{pp} and 1.2 V_{pp}.

☞ When the safety functions "Safely-monitored position" and "Safely-limited position" are used, the encoder must have a HIPERFACE® or EnDat interface by which the absolute position generated encoder-internally can be read.

If such an interface is not available or if a firmware smaller than MP*-07V08 is used, the following **remaining risk** must be taken into consideration: The accumulation of transmission errors can cause a position offset. The occurred position offset can be removed by homing.

- **Mechanics:** The connection of encoder shaft and motor shaft or encoder housing and motor housing, and the fixing device of the reading head of linear encoders has to be dimensioned such that accidental loosening or breakage of the connection can be excluded (e.g., 20-fold overdimensioning).

☞ Take remaining risks into consideration: see marginal note"Important instructions regarding inadequate connections of encoder shaft and motor shaft or encoder housing and motor housing".

- **Reliability:** The "Mission Time" and the "Proof Test Interval" of the encoder have to be complied with. After the "Mission Time" has elapsed, the encoder has to be decommissioned. When the "Proof Test Interval" is over, a "Proof Test" has to be carried out with the encoder **or** it has to be decommissioned.
- **Wiring "encoder - IndraDrive":** The encoder has to be directly connected to the optional slot X4 (X4.1 and X4.2 for double-axis devices) (additional mere plug-in connectors are allowed). Branches to other evaluation devices, interconnecting active units or switching between encoders are not allowed.

Resolver

Resolvers must comply with the following requirements so that they can be used as safety technology encoders:

- **Signal generation:** The analog position signals have to be generated in mere analog form. Synthetic signal generation or any further signal processing is not allowed.
- **Signal transmission:** The analog position signals have to be transmitted in differential form. The differential signal amplitude levels have to be between 7.7 V_{pp} and 10.5 V_{pp} (related to an excitation voltage of 18.2 V_{pp} at 4 kHz).
- **Mechanics:** The connection of encoder shaft and motor shaft or encoder housing and motor housing has to be dimensioned such that accidental loosening or breakage of the connection can be excluded (e.g., 20-fold overdimensioning).

☞ Take remaining risks into consideration: see marginal note"Important instructions regarding inadequate connections of encoder shaft and motor shaft or encoder housing and motor housing".

- **Reliability:** The "Mission Time" and the "Proof Test Interval" of the encoder have to be complied with. After the "Mission Time" has elapsed, the encoder has to be decommissioned. When the "Proof Test Interval" is over, a "Proof Test" has to be carried out with the encoder **or** it has to be decommissioned.
- **Wiring "encoder - IndraDrive":** The encoder has to be directly connected to the optional slot X4 (X4.1 and X4.2 for double-axis devices) (additional mere plug-in connectors are allowed). Branches to other evaluation devices, interconnecting active units or switching between encoders are not allowed.

Important instructions regarding inadequate connections of encoder shaft and motor shaft or encoder housing and motor housing

If it cannot be excluded that the connection of encoder shaft and motor shaft or encoder housing and motor housing accidentally loosens or breaks, take the following **remaining risks** into consideration:

- **Combination "rotary or linear encoder with synchronous motor"**: Possible incorrect orientation of the commutation can cause positive feedback of the current control loop. In this case, the velocity can inadmissibly increase before the monitoring function triggers.
- **"Optional load-side encoder" or combination "rotary encoder with asynchronous motor":** The encoder can move with the shaft by an angle limited by the connection cable which causes an angle offset. This can result in dangerous movements.

  Loosening of the material measure (e.g., encoder shaft breakage) should not cause any allowed signals; if this error cannot be excluded, take the following residual risk into consideration: The motor shaft can move at maximum slip speed.

8.2.6 Allowed motor holding brakes

When the safety function "Safe braking and holding system" (with the option "Safe Motion") is to be used, both brakes must comply with the following requirements:

Motor holding brake

- **Control:** The brake must have been designed is such a way that the holding torque of the brake takes effect in the de-energized state (e.g., electrically releasing friction surface brake).
- **Electrical connection:**
  - The electrical connections of the brake should not have ground reference.
  - The allowed voltage range of the brake has to be 24 V_{DC}±10%.
  - The brake current in the activated state should not be more than a maximum of 2.5 A.
- **Mechanics:** Friction surface brakes are allowed as motor holding brakes. It is not allowed to operate form-fitting brakes as motor holding brakes. The static holding torque of the brake has to be dimensioned such that the maximum weight of the load of the axis can be safely held. For more detailed information on the dimensioning of the brake, please refer to the corresponding C-standard.

☞ In addition to the static holding torque of the brake, the required dynamic braking torque of the brake has to be considered. The dynamic braking torque of the brake has a direct influence on the behavior of the axis in the case of error and needs to be taken into account in the risk analysis (see chapter "Safe braking and holding system", marginal note "Risk analysis").

- **Reliability:** The brake must have been authorized for ambient temperatures from 0 to 40°C.

Redundant holding brake

- **Control:** The brake must have been designed is such a way that the holding torque of the brake takes effect in the de-energized state (e.g., electrically releasing friction surface brake).
- **Electrical connection:**
  - The electrical connections of the brake should not have ground reference.
  - The allowed voltage range of the brake has to be 24 V_{DC}±10%.
  - The brake current in the activated state has to be between 0.1 A and 6 A.
  - The inductance of the operating coil should not be more than a maximum of 750 mH.
- **Mechanics:** Both friction surface brakes and form-fitting brakes are allowed as redundant holding brakes. The static holding torque of the brake has to be dimensioned such that the maximum weight of the load of the axis can be safely held. For more detailed information on the dimensioning of the brake, please refer to the corresponding C-standard.

☞ In addition to the static holding torque of the brake, the required dynamic braking torque of the brake has to be considered. The dynamic braking torque of the brake has a direct influence on the behavior of the axis in the case of error and needs to be taken into account in the risk analysis (see chapter "Safe braking and holding system", marginal note "Risk analysis").

- **Reliability:** The brake must have been authorized for ambient temperatures from 0 to 40°C.

8.2.7 Required commissioning tools

Safe Torque Off

One of the following tools is required for commissioning the optional safety technology module "Safe Torque Off":

- Any commissioning tool for visualizing and modifying parameters
- IndraWorks commissioning software with safety technology wizard

Safe Motion

The following tool is required for commissioning the optional safety technology module "Safe Motion":

- IndraWorks commissioning software (at least version 09V08) with safety technology wizard and parameter verification tool

8.3 Commissioning the "Safe torque off" function (optional safety technology module "L2")

8.3.1 Overview

The "Safe torque off" function can preferably be commissioned using the dialog of the same name in the IndraWorks commissioning software, or manually.

☞ The following commissioning steps describe commissioning using the "Safe torque off" dialog. For commissioning with a different commissioning tool, the corresponding parameters which have to be set are listed.

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ If external force influences, together with danger for persons or machines, are to be expected with the safety function "Safe torque off", e.g. due to the weight of the load in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation.

⇒ In this case, all cases of operation occurring in the application have to be taken into account, including mains failure and tripped fuses.

⇒ In the case of danger to persons, Bosch Rexroth recommends the Rexroth Safe braking and holding system.

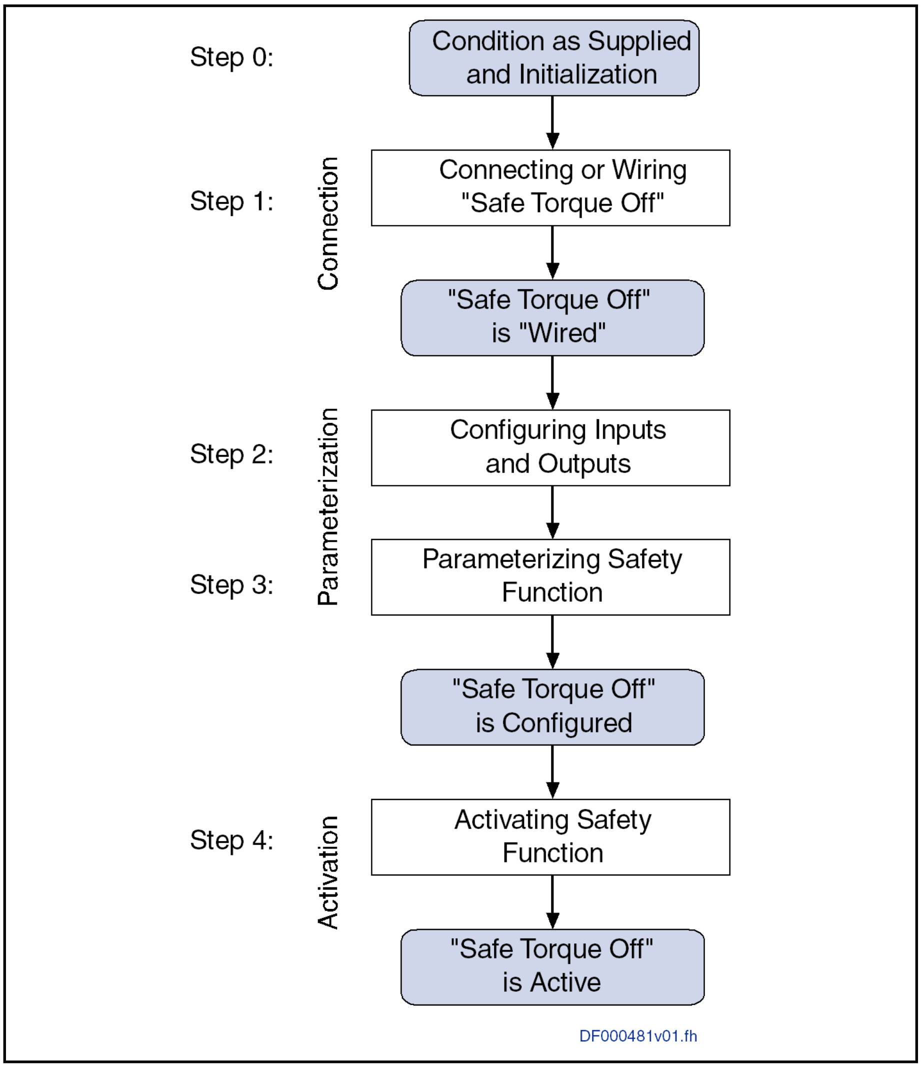

Step 0:
Condition as Supplied and Initialization
Step 1:
Connection
Connecting or Wiring "Safe Torque Off"
"Safe Torque Off" is "Wired"
Step 2:
Parameterization
Configuring Inputs and Outputs
Step 3:
Parameterizing Safety Function
"Safe Torque Off" is Configured
Step 4:
Activation
Activating Safety Function
"Safe Torque Off" is Active
DF000481v01.fh

Fig. 8-2: Overview - commissioning steps of the "Safe torque off" function

8.3.2 Commissioning steps

Step 0: Condition as supplied and initialization

The "Safe torque off" function is always active and cannot be deactivated. **In the condition as supplied**, the following default parameter setting is active:

- Selection configuration: N/C - N/O combination
- Time interval of forced dynamization: 8 hours

After the booting process, the drive system is in the operating status "STO"; i.e., the output stage has been switched off via two channels. Depending on the selection, safety is acknowledged or not.

When the drive is switched from **operating mode to parameter mode**, the functionality of the "Safe torque off" function is maintained, i.e. according to the selection, the "Safe torque off" function becomes active or not.

Step 1: Connecting and wiring the "Safe torque off" function

The connection and wiring of the "Safe torque off" function depends on the option used to make the selection and carry out the acknowledgment at the drive:

- Selection via N/C - N/O combination:
  - Connection N/C: STO n (X41/2)
  - Connection N/O: STO B (X41/3)

  - Connect unassigned input STO A (X41/1) to 0 V
- Selection with two N/C contacts:
  - Connection N/C: STO n (X41/2)
  - Connection N/C: STO A (X41/1)
  - Connect unassigned input STO B (X41/3) to 0 V
- Acknowledgment: See "Safe torque off (STO)"
  - Connection supply for acknowledgment potential: STO Q (X41/4)
  - Connection acknowledgment or inverted acknowledgment: STO Q1 (X41/5) or STO Q2 (X41/6)

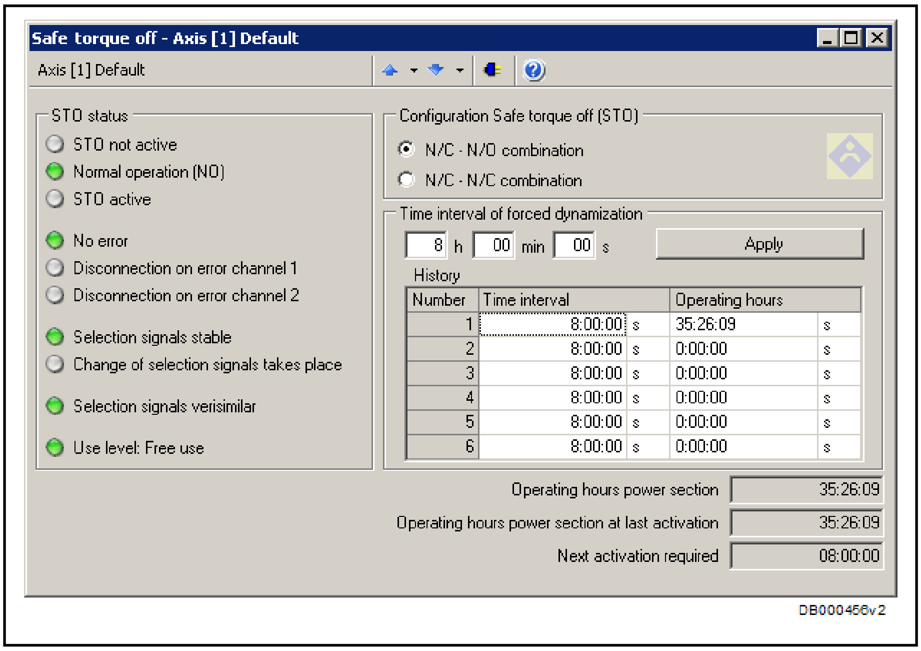
☞ Depending on the "Safety Integrity Level" (SIL) to be attained, the following input and output circuits are allowed:

- **SIL1:** The "Safe torque off" function can be controlled either directly by the operator (via switch) or by a safety technology master (e.g., safety PLC).
- **SIL2:** The "Safe torque off" function can be controlled either directly by the operator (via switch) or by a safety technology master (e.g., safety PLC) which attains SIL 2/PL d or higher.

  The feedback has to be evaluated via a safety technology master, which attains SIL 2/PL d or higher, or by directly controlling a safety technology actuator (e.g., safety door).
- **SIL3:** The "Safe torque off" function has to be controlled and the feedback has to be evaluated **by a safety technology master** which complies with SIL3/PL e (e.g., safety PLC).

Step 2: Configuring the inputs and outputs

With the "Safe torque off" function, only the inputs can be configured (call the IndraWorks dialog: **Safety technology** ▸ **Safe torque off**).


Safe torque off - Axis [1] Default

Axis [1] Default

STO status
○ STO not active
● Normal operation (NO)
○ STO active
● No error
○ Disconnection on error channel 1
○ Disconnection on error channel 2
● Selection signals stable
○ Change of selection signals takes place
● Selection signals verisimilar
● Use level: Free use

Configuration Safe torque off (STO)
◉ N/C - N/O combination
○ N/C - N/C combination

Time interval of forced dynamization
8 h 00 min 00 s Apply

History

Number	Time interval		Operating hours	
1	8:00:00	s	35:26:09	s
2	8:00:00	s	0:00:00	s
3	8:00:00	s	0:00:00	s
4	8:00:00	s	0:00:00	s
5	8:00:00	s	0:00:00	s
6	8:00:00	s	0:00:00	s

Operating hours power section 35:26:09
Operating hours power section at last activation 35:26:09
Next activation required 08:00:00

DB000456v2

Fig. 8-3: IndraWorks dialog "Safe torque off"

Switch the drive to the parameter mode (phase 2 or PM) before starting the parameter setting. In the dialog section "Configuration Safe torque off (STO)" of the IndraWorks dialog "Safe torque off", the selection can be parameterized. The only possible combinations are "N/C - N/O" or "N/C - N/C" (P-0-0101, Configuration for STO selector).

Step 3: Parameterizing the safety function

In the dialog section "Time interval of forced dynamization" of the IndraWorks dialog "Safe torque off", enter the time interval within which the safety function "Safe torque off" has to be activated with the drive controller being active (P-0-0103, Time interval of forced dynamization). The time that has been set is activated with the "Apply" button.

☞ Depending on the "Safety Integrity Level" to be attained, the following time intervals are allowed for forced dynamization:

- **SIL1:** No forced dynamization required (⇒set time interval to 168 hours).
- **SIL2:** The time interval for forced dynamization cannot be longer than a maximum of **168 hours**.
- **SIL3:** The time interval for forced dynamization cannot be longer than a maximum of **24 hours**. (When guards are used, the test interval can be extended if a successful test was carried out directly before the safety area is enabled).

Step 4: Activating / deactivating the safety function

☞ Before selecting the safety function "Safe torque off", shut down the drive system using the command value input and reset drive enable. There is no drive-controlled stopping process!

The safety function "Safe torque off" is automatically activated when switching to the operating mode (phase 4 or OM) for the first time, and afterwards it is active in the parameter mode, too. It cannot be deactivated. Changes in the parameter setting will take immediate effect.

☞ Via the dialog section "STO status" of the IndraWorks dialog "Safe torque off", the following aspects can be diagnosed:

- "STO not active" is active (red), when the optional safety technology module "Safe Torque Off" has not yet been activated, i.e. the axis has not yet reached phase4 (OM) since the drive had been switched on.
- "Normal operation (NO)" is active (green), when the optional safety technology module "Safe Torque Off" has been activated and the safety function "Safe torque off" has not been selected.
- "STO active" is active (green), when the optional safety technology module "Safe Torque Off" has been activated and the safety function "Safe torque off" has been selected.
- "No error" is active (green), if currently there is no safety error present.
- "Disconnection on error channel 1" is active (red), if the safety channel 1 has detected an error.
- "Disconnection on error channel 2" is active (red), if the safety channel 2 has detected an error.
- "Selection signals stable" is active (green), if the selection signals have reached a stable state, i.e. the signals do not incessantly change (e.g., switch bouncing).
- "Change of selection signals takes place" is active (green), if a change of the selection signals is detected.
- "Selection signals verisimilar" can change between green and red. "Green" signals that the selection signals are verisimilar and the selection can be made. "Red" signals that the selection signals are not verisimilar (e.g., one channel has been selected and the other one has not); in this case, the selection cannot be made.
- "Use level":
  - "Green" signals that the drive firmware used has been tested and released for using the safety function "Safe torque off".
  - "Red" signals that the firmware currently available in the drive has not been released for operation with the optional safety technology module "Safe Torque Off" and consequently cannot be used.

8.4 Commissioning the optional safety technology module "Safe Motion" (S2)

8.4.1 Overview

Safety technology has to be commissioned via the safety technology wizard in the IndraWorks commissioning software.

☞ The following commissioning steps describe the commissioning by means of the safety technology wizard on the basis of IndraWorks 11V06.

☞ For commissioning the safety technology, you should always use the current release of the corresponding firmware version and of the IndraWorks commissioning software.

Otherwise, take the corresponding manufacturer information on detected and solved problems into account and verify their relevance for the machine application.

For information on the current release and the manufacturer information, please refer to the "eBusiness Portal" under http://www.boschrexroth.com/portal.

When using the safety functions, the following safety instructions must be observed:

⚠ DANGER **Lethal injury and/or property damage caused by unintended axis motion!**

⇒ If external force influences, together with danger for persons or machines, are to be expected when using the safety functions, e.g. due to the weight of the load in the case of a vertical axis, this motion has to be safely prevented by additional measures, e.g. a mechanical brake or a weight compensation.

⇒ In this case, all cases of operation occurring in the application have to be taken into account, including mains failure and tripped fuses.

⇒ In the case of danger to persons, Bosch Rexroth recommends the Rexroth Safe braking and holding system.

⚠ WARNING **Injury and/or property damage caused by deviation from standstill position!**

⇒ When using the Safe stop 2 or the Safely-limited speed for axes with external force influences, the drive controller might possibly no longer be able to keep the axis in position in the case of error situations (e.g., mains failure, controller defect). When the error case occurs, the axis has to be kept in position by additional measures (e.g., mechanical brake).

⇒ In the time between the occurrence of the error and the triggering of a holding device, axis motion can occur. This has to be taken into account for the risk assessment of the installation.

⇒ In the case of danger to persons, Bosch Rexroth recommends using the Rexroth Safe braking and holding system.

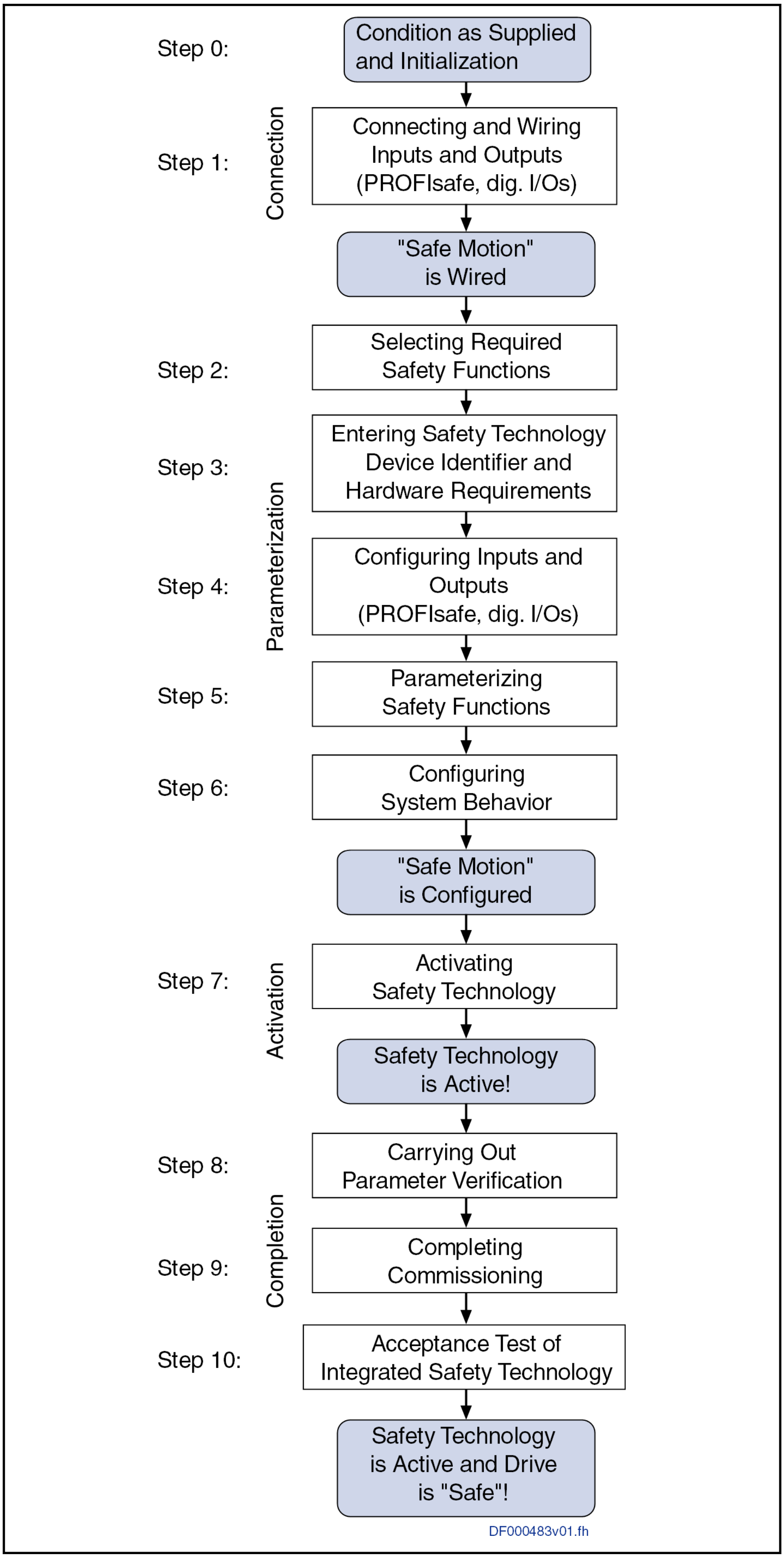

Step 0:
Condition as Supplied and Initialization
Step 1:
Connection
Connecting and Wiring Inputs and Outputs (PROFIsafe, dig. I/Os)
"Safe Motion" is Wired
Step 2:
Selecting Required Safety Functions
Step 3:
Parameterization
Entering Safety Technology Device Identifier and Hardware Requirements
Step 4:
Configuring Inputs and Outputs (PROFIsafe, dig. I/Os)
Step 5:
Parameterizing Safety Functions
Step 6:
Configuring System Behavior
"Safe Motion" is Configured
Step 7:
Activation
Activating Safety Technology
Safety Technology is Active!
Step 8:
Completion
Carrying Out Parameter Verification
Step 9:
Completing Commissioning
Step 10:
Acceptance Test of Integrated Safety Technology
Safety Technology is Active and Drive is "Safe"!
DF000483v01.fh

Fig. 8-4: Overview - commissioning steps of integrated safety technology

8.4.2 Commissioning steps

Step 0: Condition as supplied and initialization

In the **condition as supplied**, safety technology is not active; the status of "P-0-3207, Safety technology password level" is "0". The drive can be commissioned in the "normal" way.

When using the safety function "Safe braking and holding system", set the redundant holding brake, for the "normal" commissioning of the drive, to the setting-up mode (P-0-3300, Redundant holding brake: Configuration).

If the safety technology is not active, the system parameters are invalid and neither validation tests nor data comparisons are carried out. The safety parameters are set to default values and the write protection is disabled. "INDRASAVE" has been entered as the default password in "P-0-3206, Safety technology password". Under these circumstances, it is possible to preload the safety parameters from a parameter file (when drive configurations are copied).

After the booting process, the drive system is in the operating status "Safe stop 1"; i.e., the output stage has been switched off via two channels.

When the drive is switched from **operating mode to parameter mode**, the system, too, automatically goes to "Safe stop 1".

System initializations and repeated setting of encoder evaluation take place when the drive is switched (again) to the operating mode. Only in the operating mode does the evaluation of the safety technology selection inputs take place and the drive, if necessary, is switched to another operating status!

Step 1: Connecting or wiring the safety functions

The connection or wiring of the safety functions depends on the possibility used to make the selection and carry out the acknowledgment, and on the configuration of the device. This is why the I/Os in the examples of application are symbolically named "I1" to "I4", "I1n" to "I4n", "I10", "O10", "IO10n", "IO20" and "IO30" and do not comply with the terminal designations at the device.

There are the following wiring options:

- **Channel 1 and channel 2 via digital I/Os of the drive** (see "Safety technology I/O")
- **Channel 1 via standard master communication and channel 2 via digital I/Os of the drive** (see ""Safe motion" in conjunction with a master communication")
- **Channel 1 and channel 2 via PROFIsafe** (see "PROFIsafe")

Using safety technology functions that need the "Safe homing procedure" (e.g., "Safely-monitored position") requires an additional hardware input via which the additional home switch can be read in. The home switch has to be connected to one of the inputs ("I1n" to "I4n") on connector X41.

When using the safety function "Safe braking and holding system", wire the control and diagnostic signals of HAT ("HAT-Steuer", "HAT-Diagnose") in addition to the signals for selection and acknowledgment.

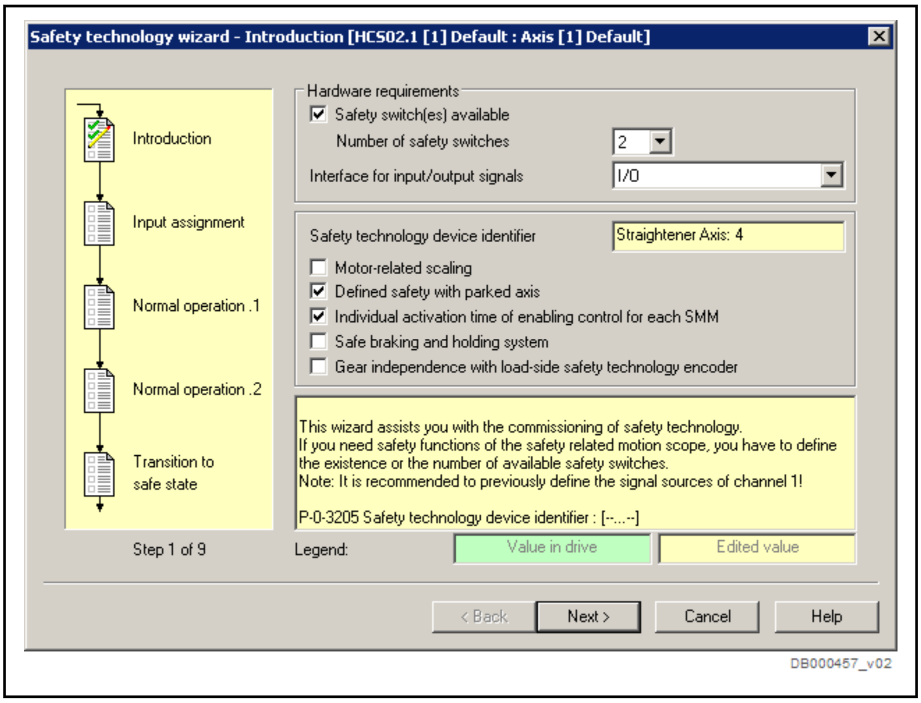
Step 2: Selecting required safety functions

See "Overview of safety functions"

☞ When user-defined scalings for position, velocity, acceleration and torque or force are used, the following parameterizations are **not allowed**:

- Scaling factors unequal 1
- Rotational position resolution unequal $360*10^n$ (n=1, 2, 3…)

Step 3: Entering safety technology device identifier and hardware requirements



Safety technology wizard - Introduction [HCS02.1 [1] Default : Axis [1] Default]

Hardware requirements
☑ Safety switch(es) available
Number of safety switches: 2
Interface for input/output signals: I/O

Safety technology device identifier: Straightener Axis: 4
☐ Motor-related scaling
☑ Defined safety with parked axis
☑ Individual activation time of enabling control for each SMM
☐ Safe braking and holding system
☐ Gear independence with load-side safety technology encoder

This wizard assists you with the commissioning of safety technology.
If you need safety functions of the safety related motion scope, you have to define the existence or the number of available safety switches.
Note: It is recommended to previously define the signal sources of channel 1!

P-0-3205 Safety technology device identifier : [--...--]

Fig. 8-5: Safety technology wizard in IndraWorks (Note: The contents of the dialog depend on the firmware used / the IndraWorks version used)

- Switch drive to parameter mode
- Start safety technology wizard in IndraWorks
- In the dialog section "Hardware requirements",
  - enter number of safety switches (S1, S2) used (this is required for following sequence of safety technology wizard).
  - select via which interface the safety technology inputs and outputs are read.
    - I/O: when using I/Os or I/Os and master communication
    - PROFIsafe: when using PROFIsafe
- In text field "Safety technology device identifier", enter an identifier of the device on which safety technology was commissioned (e.g., machine type, unit, drive for .. axis/spindle).

  This device identifier is required for identifying the backup of safety technology data. The corresponding parameter is "P-0-3205, Safety technology device identifier".
- Tick the check box "Motor-related scaling", if the scaling cannot be changed any more after safety technology commissioning. For example, when using parameter set switching (load gear switching) or gear switching in the parameter mode.

  The corresponding parameter is "P-0-3210, Safety technology configuration".

☞ When using the "Safe homing procedure" function, do not activate the "motor-related scaling"!

- Tick the check box "Defined safety with parked axis", if the drive is to acknowledge safety when the drive function "parking axis" is selected.

  The corresponding parameter is "P-0-3210, Safety technology configuration".

☞ The control bit signals safety which has to result from the risk analysis of the installation. Using the function for axes with long coasting times (grinding wheels, spindles, rolls, ...) must be excluded.

- Tick the check box "Individual activation time of enabling control for each SMM", if individual monitoring of the activation time of enabling control is to be parameterized for each special mode "Safe motion" (SMM1 to SMM4). If the check box is not selected, collective monitoring of the activation time of enabling control is active for all special modes "Safe motion" (SMM1 to SMM4).

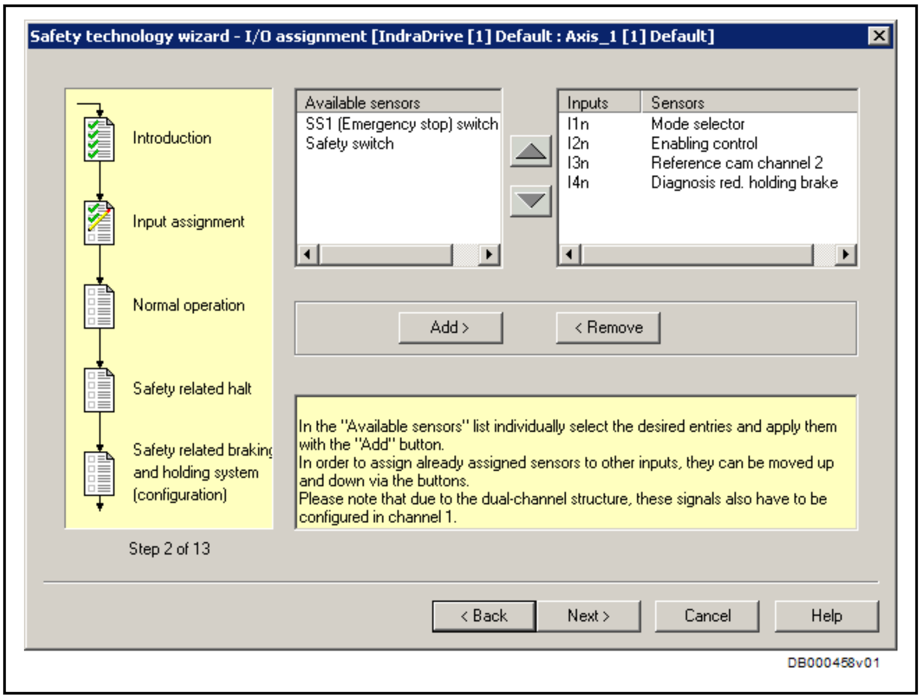
  The corresponding parameter is "P-0-3239, Configuration of global safety technology functions".
- Via the check box "Safe braking and holding system", activate this safety function. (If the safety function "Safe braking and holding system" is selected, the following dialogs are automatically adjusted accordingly.)
- Tick the check box "Gear independence with load-side safety technology encoder", when the encoder relevant to safety technology has been mounted on the load side and an existing switchable gear is to be used. If the check box is not selected, the gear ratio between motor and load should not be changed any more after safety technology commissioning.

  The corresponding parameter is "P-0-3210, Safety technology configuration".
- Apply the inputs with "Next".

Step 4: Configuring inputs and outputs

There are two variants of configuration for the inputs and outputs, depending on the interface set in the previous step ("I/O" or "PROFIsafe").

Interface "I/O":



Safety technology wizard - I/O assignment [IndraDrive [1] Default : Axis_1 [1] Default]

Available sensors
SS1 (Emergency stop) switch
Safety switch

Inputs	Sensors
I1n	Mode selector
I2n	Enabling control
I3n	Reference cam channel 2
I4n	Diagnosis red. holding brake

In the "Available sensors" list individually select the desired entries and apply them with the "Add" button.
In order to assign already assigned sensors to other inputs, they can be moved up and down via the buttons.
Please note that due to the dual-channel structure, these signals also have to be configured in channel 1.

Fig. 8-6: "I/O assignment" dialog, if "Interface"="I/O"

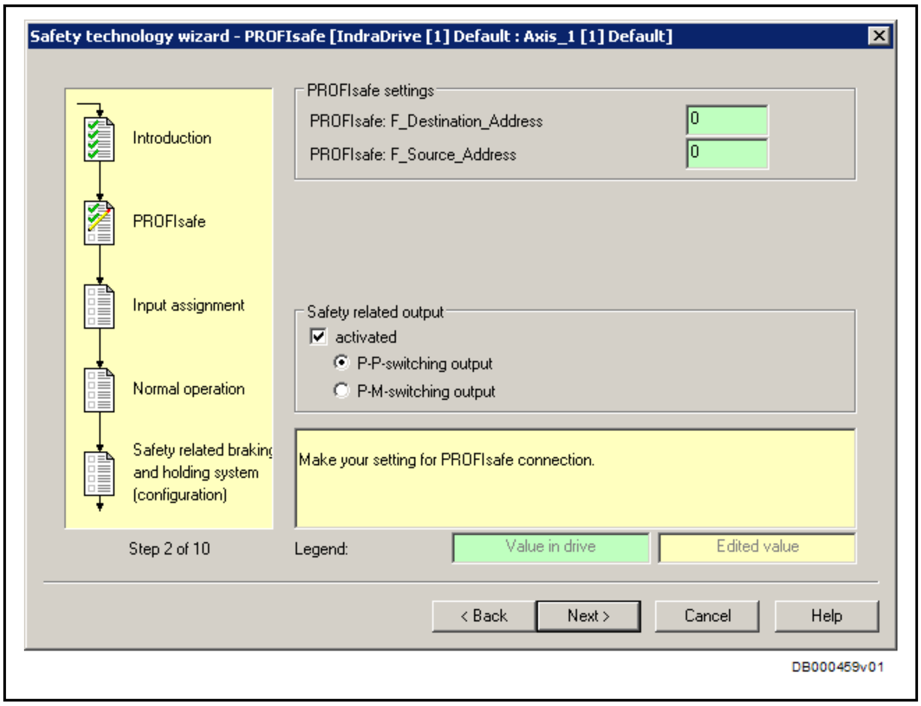
- From the "Available sensors" list, highlight the safety technology sensors used and assign them to an input of channel 2 using "Add". If required, change the assignment to the inputs using the two arrow keys.

  The corresponding parameter is "P-0-3211, Safety technology I/O configuration list, channel 2".

☞ The physical inputs for channel 1 have to be separately determined using the appropriate parameterization (see "Step 1: Connecting or wiring the safety functions" on page 206).

- Apply the inputs with "Next".

"PROFIsafe" interface:


Safety technology wizard - PROFIsafe [IndraDrive [1] Default : Axis_1 [1] Default]

PROFIsafe settings

PROFIsafe: F_Destination_Address: 0

PROFIsafe: F_Source_Address: 0

Safety related output

☑ activated

● P-P-switching output

○ P-M-switching output

Make your setting for PROFIsafe connection.

Step 2 of 10

Legend: 🟩 Value in drive 🟨 Edited value

Fig. 8-7: "PROFIsafe" dialog, if "Interface"="PROFIsafe" (Note: The contents of the dialog depend on the firmware used / the IndraWorks version used)

- In the text field "PROFIsafe: F_Destination_Address", enter the target address of the safe communication connection.

  For further information, please see description of "P-0-3290, PROFIsafe: F_Destination_Address".

- In the text field "PROFIsafe: F_Source_Address", enter the source address of the safe communication connection.

  For further information, please see description of "P-0-3291, PROFIsafe: F_Source_Address"

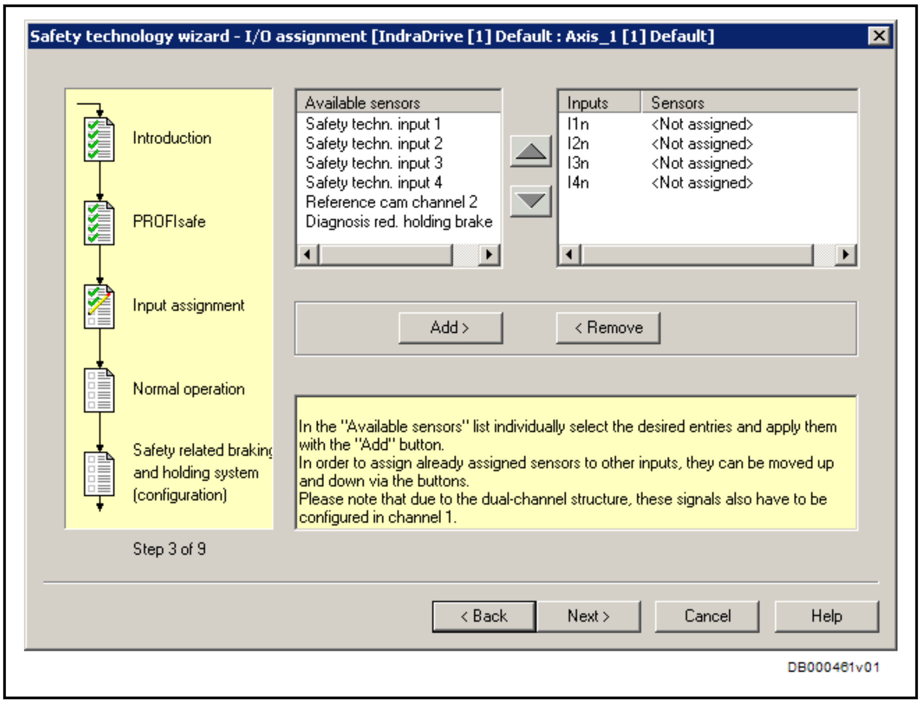
- In the dialog section named "Safe output", activate the safe output. Select either Plus-Plus-switching output or Plus-Minus-switching output.

  The corresponding parameter is "P-0-3295, Safety technology field bus configuration".

- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.

- Apply the inputs with "Next".



Safety technology wizard - I/O assignment [IndraDrive [1] Default : Axis_1 [1] Default]

Available sensors
Safety techn. input 1
Safety techn. input 2
Safety techn. input 3
Safety techn. input 4
Reference cam channel 2
Diagnosis red. holding brake

Inputs	Sensors
I1n	<Not assigned>
I2n	<Not assigned>
I3n	<Not assigned>
I4n	<Not assigned>

In the "Available sensors" list individually select the desired entries and apply them with the "Add" button.
In order to assign already assigned sensors to other inputs, they can be moved up and down via the buttons.
Please note that due to the dual-channel structure, these signals also have to be configured in channel 1.

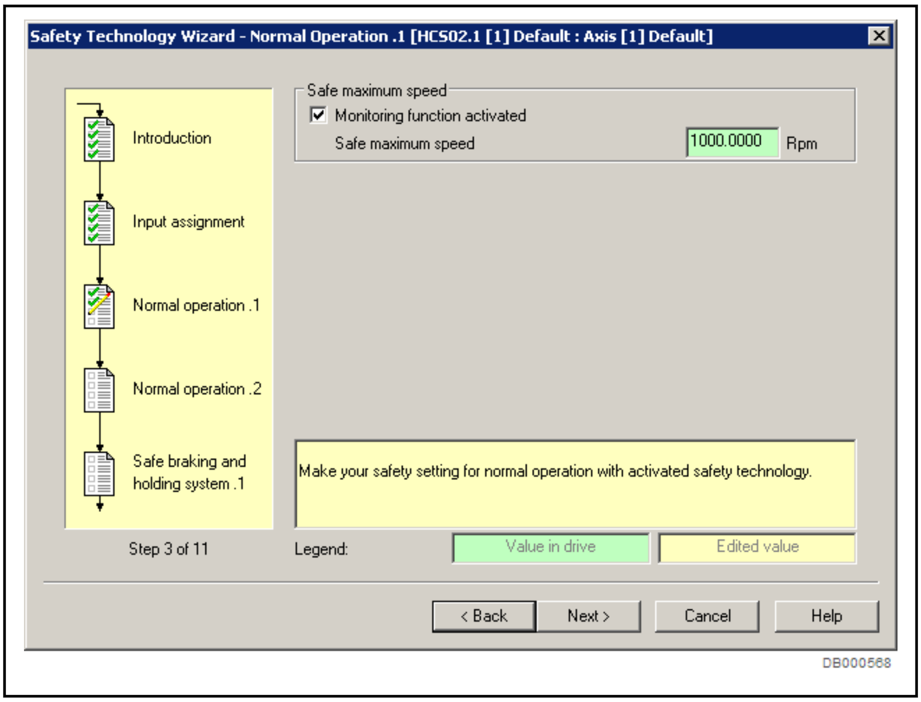
Fig. 8-8: "I/O assignment" dialog, if "Interface"="PROFIsafe"

- From the "Available sensors" list, highlight the safety technology sensors used and assign them to an input of channel 2 using "Add". If required, change the assignment to the inputs using the two arrow keys.

  The corresponding parameter is "P-0-3211, Safety technology I/O configuration list, channel 2".
- Apply the inputs with "Next".

Step 5: Parameterizing the safety functions

Parameterizing normal operation



Safety Technology Wizard - Normal Operation .1 [HCS02.1 [1] Default : Axis [1] Default]

Safe maximum speed
☑ Monitoring function activated
Safe maximum speed 1000.0000 Rpm

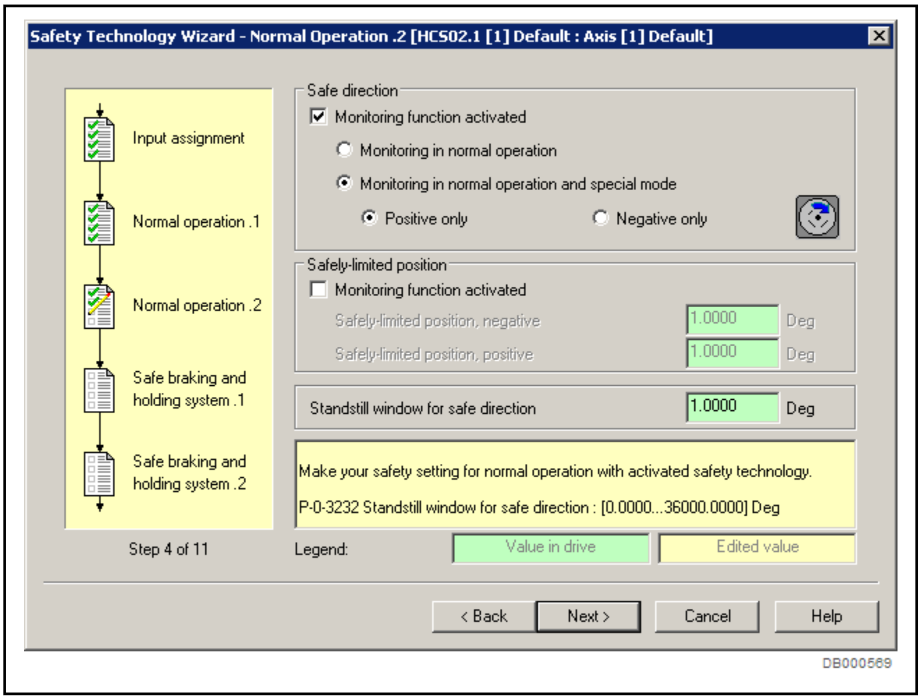
Make your safety setting for normal operation with activated safety technology.

Legend: 🟩 Value in drive 🟨 Edited value

Fig. 8-9: 1. Dialog for settings of normal operation

- In the dialog section "Safe maximum speed", activate the monitoring function for safe maximum speed ("P-0-3239, Configuration of global safety technology functions"). When the monitoring function has been activated, enter the maximum effective speed limit which is to be monitored both in normal operation and in special mode (e.g., SMM) ("P-0-3234, Safe maximum speed").
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.
- Apply the inputs with "Next".



Safety Technology Wizard - Normal Operation .2 [HCS02.1 [1] Default : Axis [1] Default]

Safe direction
☑ Monitoring function activated
○ Monitoring in normal operation
● Monitoring in normal operation and special mode
● Positive only ○ Negative only

Safely-limited position
□ Monitoring function activated
Safely-limited position, negative 1.0000 Deg
Safely-limited position, positive 1.0000 Deg

Standstill window for safe direction 1.0000 Deg

Make your safety setting for normal operation with activated safety technology.
P-0-3232 Standstill window for safe direction : [0.0000...36000.0000] Deg

Step 4 of 11

Legend: 🟩 Value in drive 🟨 Edited value

Fig. 8-10: 2. Dialog for settings of normal operation

Dialog section "Safe direction"

- MPx07V08 and below: Global monitoring of the direction of motion can be parameterized (takes effect in normal operation and in special mode; by activating the function, individual monitoring functions of the direction of motion of special modes motion are deactivated).
- *MPx07V10 and above:*
  – Monitoring of the "Safe direction" can be configured for normal operation and special mode (by activating the function, individual monitoring functions of the direction of motion of special modes motion are deactivated), or

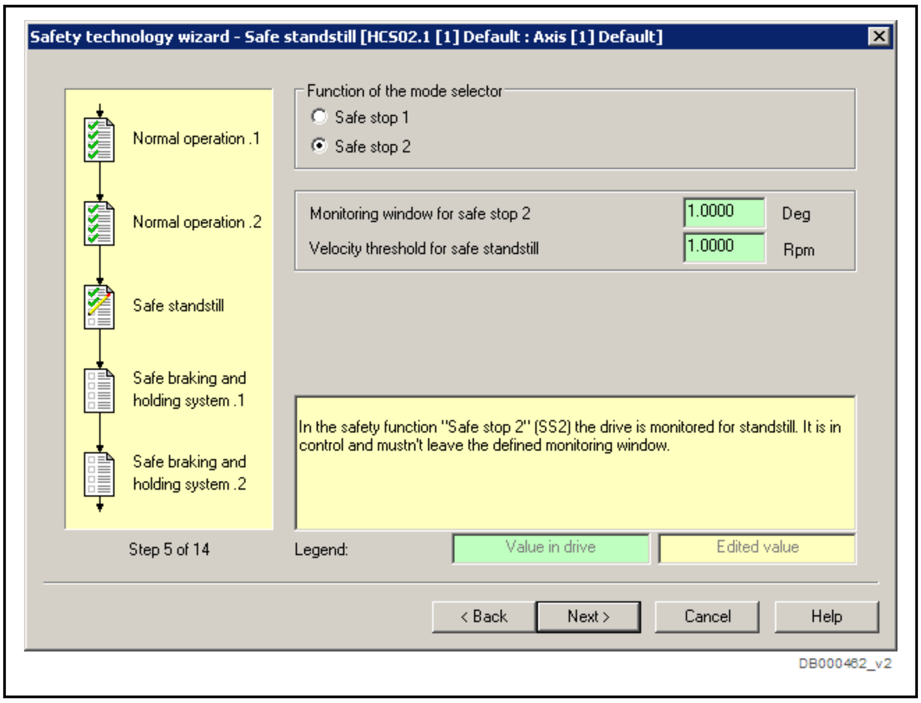
- it can be configured in such a way that it is **only** active in normal operation.

For monitoring the direction of motion, you have to parameterize the standstill window ("P-0-3232, Standstill window for safe direction").

- In the dialog section "Safely-limited position", activate the corresponding safety function. To do this, enter both end positions and the standstill window for the safe direction. The corresponding parameters are:
  - P-0-3232, Standstill window for safe direction
  - P-0-3235, Safely-limited position, positive
  - P-0-3236, Safely-limited position, negative
  - P-0-3239, Configuration of global safety technology functions
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.
- Apply the inputs with "Next".

Parameterizing the functions for "Safe standstill"


Safety technology wizard - Safe standstill [HCS02.1 [1] Default : Axis [1] Default]

Function of the mode selector
○ Safe stop 1
● Safe stop 2

Monitoring window for safe stop 2: 1.0000 Deg
Velocity threshold for safe standstill: 1.0000 Rpm

In the safety function "Safe stop 2" (SS2) the drive is monitored for standstill. It is in control and mustn't leave the defined monitoring window.

Fig. 8-11: Dialog for settings of Safe standstill

- In the dialog section "Function of the mode selector", select whether transition to the safety function "Safe stop 1" or to the safety function "Safe stop 2" is to take place when the mode selector is selected.

The corresponding parameter is "P-0-3210, Safety technology configuration".

- The field "Monitoring window for safe stop 2" is only visible, when "Safe stop 2" has been selected. Enter the maximum allowed travel distance in this field. Maximum allowed travel distance refers to actual position available at point of time when safe stop 2 is activated.

  The corresponding parameter is "P-0-3230, Monitoring window for safe stop 2".
- In the field "Velocity threshold for safe standstill", enter the velocity threshold for the special mode "Safe standstill" or for the safety function "Safe torque off".

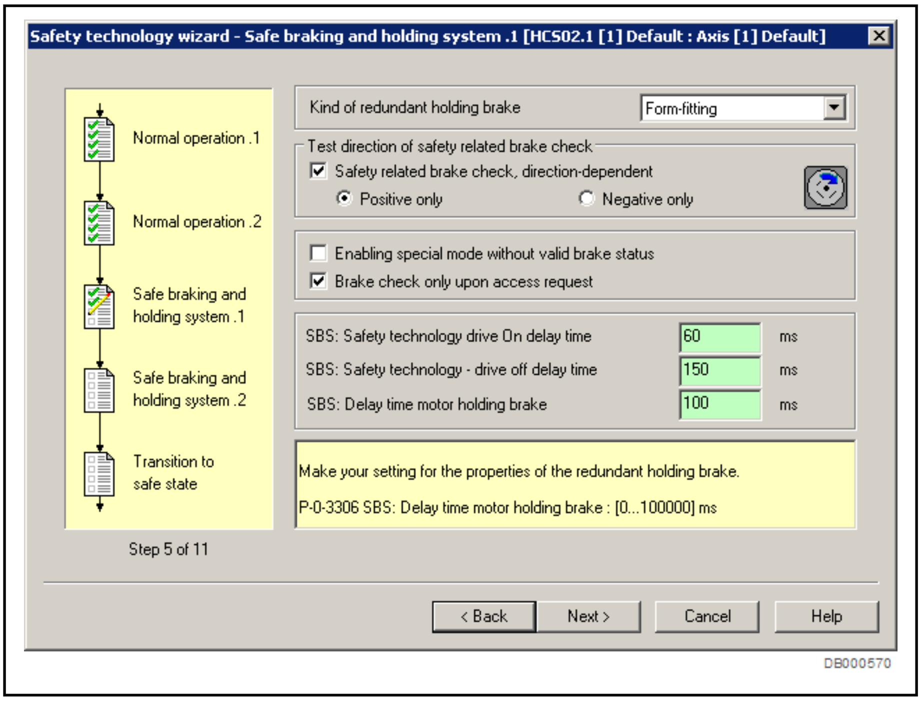
  The corresponding parameter is "P-0-3233, Velocity threshold for safe standstill".
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.
- Apply the inputs with "Next".

☞ For further information on commissioning, see "Safety functions in special mode "Safe standstill"".

Parameterizing the Safe braking and holding system

☞ The following dialogs are only displayed, when the Safe braking and holding system has been parameterized in the start dialog of the safety technology wizard.



Safety technology wizard - Safe braking and holding system .1 [HCS02.1 [1] Default : Axis [1] Default]

Kind of redundant holding brake: Form-fitting

Test direction of safety related brake check

☑ Safety related brake check, direction-dependent

● Positive only ○ Negative only

☐ Enabling special mode without valid brake status

☑ Brake check only upon access request

SBS: Safety technology drive On delay time	60	ms
SBS: Safety technology - drive off delay time	150	ms
SBS: Delay time motor holding brake	100	ms

Make your setting for the properties of the redundant holding brake.

P-0-3306 SBS: Delay time motor holding brake : [0...100000] ms

Step 5 of 11

Fig. 8-12: 1. "Safe braking and holding system" dialog

- In the "Kind of redundant holding brake" field, select the design of the redundant holding brake. It is possible to choose between form-fitting and friction surface brake.

  The corresponding parameter is "P-0-3300, Redundant holding brake: Configuration".

- Via the dialog section "Test direction of safe brake check", it is possible to have the brake check carried out in one direction only. This is necessary, for example, when such brakes are used which generate holding torque in one direction only.

  The corresponding parameter is "P-0-3300, Redundant holding brake: Configuration".

- Tick the check box "Enabling special mode without valid brake status", if the command "C6200 Command Enabling SM without valid brake status" is to be enabled. Before using the command, observe the explanations in chapter "Enabling the special mode without valid brake status".

  The corresponding parameter is "P-0-3300, Redundant holding brake: Configuration".

- Special case: To avoid interrupting the automatic operation at a "random" point, it is possible with MPx08 and above to tick the "Brake check only upon access request" check box. In this case, the brake check will not be requested in normal operation.

⚠ WARNING **Dangerous movements! Danger to life, risk of injury, serious injury or property damage!**

Configuring the special case "brake check only upon access request" is only allowed if it has been ensured by appropriate measures that the user in normal operation cannot access the danger zone of a gravity-loaded axis. The machine manufacturer must carry out a risk analysis.

As the brake check request is missing in normal operation, the holding system check risks not being carried out over longer operating times or downtimes. The user is responsible for carrying out a brake check in regular intervals by means of the command "C2100 Command Holding system check", because only this procedure guarantees that the holding torques of motor brake and redundant holding brake are sufficient!

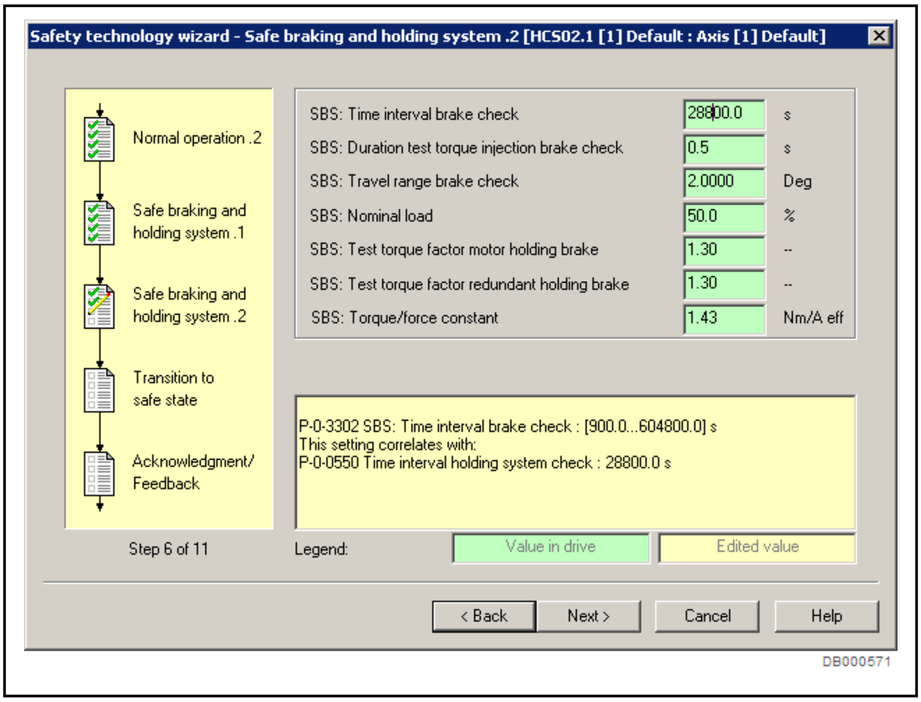
- **MPx08 and above:** By the appropriate value in the field "SBS: Safety technology drive On delay time", the time for releasing the brakes (motor brake or redundant holding brake) and the delay in the control by the "HAT" control module (60 ms) can be taken into account. Enter the higher value.

  The corresponding parameter is "P-0-3305, SBS: Safety technology drive On delay time".
- In the field "SBS: Safety technology - drive off delay time", enter the clamping delay of the motor brake or redundant holding brake used and the delay in the control by the "HAT" control module (60 ms). When drive enable is switched off, the drive remains under torque for this time to bridge the clamping delay of the brakes and prevent the axis from moving down. Enter the higher value. The value entered in this field should be used in the parameter "S-0-0207, Drive off delay time", too.

  The corresponding parameter is "P-0-3307, SBS: Safety technology - drive off delay time".
- Using the field "SBS: Delay time motor holding brake", it is possible to parameterize the trigger behavior of the motor holding brake and of the redundant holding brake. The value corresponds to a minimum delay between the control of both brakes. If the redundant holding brake is to be controlled together with the motor holding brake, set the value to "0".

  The corresponding parameter is "P-0-3306, SBS: Delay time motor holding brake".
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.
- Apply the inputs with "Next".


Safety technology wizard - Safe braking and holding system .2 [HCS02.1 [1] Default : Axis [1] Default]
Normal operation .2
Safe braking and holding system .1
Safe braking and holding system .2
Transition to safe state
Acknowledgment/ Feedback
Step 6 of 11
Legend:
Value in drive
Edited value
< Back
Next >
Cancel
Help
DB000571

SBS: Time interval brake check	28800.0	s
SBS: Duration test torque injection brake check	0.5	s
SBS: Travel range brake check	2.0000	Deg
SBS: Nominal load	50.0	%
SBS: Test torque factor motor holding brake	1.30	--
SBS: Test torque factor redundant holding brake	1.30	--
SBS: Torque/force constant	1.43	Nm/A eff

P-0-3302 SBS: Time interval brake check : [900.0...604800.0] s
This setting correlates with:
P-0-0550 Time interval holding system check : 28800.0 s

Fig. 8-13: "Safe braking and holding system" dialog

- In the field "SBS: Time interval brake check", parameterize the maximum allowed time within which the brake check has to be repeated. This time and the parameter "P-0-0550, Time interval holding system check" should be parameterized identically.

  The corresponding parameter is "P-0-3302, SBS: Time interval brake check".

- Using the field "SBS: Duration test torque injection brake check", it is possible to parameterize how long the torque is applied to the axis in individual test steps of the brake check. The suggested value should only be increased, if the total test torque cannot be applied to the brake during the parameterized time due to mechanical properties (e.g., backlash).

  The corresponding parameter is "P-0-3311, SBS: Duration test torque injection brake check".

- In the field "SBS: Travel range brake check", it is possible to parameterize the allowed travel distance during the brake check. The suggested value should only be increased, if due to backlash between brake and motor, a greater travel distance is required to successfully check the brake.

  The corresponding parameter is "P-0-3310, SBS: Travel range brake check".

- In the field "SBS: Nominal load", enter the greatest load occurring in operation. The unit is "%" and refers to the nominal torque of the motor (T_N corresponds to 100%). The value entered in this field should be used in the parameter "P-0-0547, Nominal load of holding system", too. If the value to be parameterized is unknown, it can be determined by means of the parameter "P-0-0551, Current load torque".

  The corresponding parameter is "P-0-3303, SBS: Nominal load".

- **MPx08 and above:** The value entered in the "Test torque factor motor holding brake" field is multiplied with the torque parameterized in "SBS:

Nominal load". This allows the test torque of the motor holding brake to be modified.

The corresponding parameter is "P-0-3316, SBS: Test torque factor motor holding brake".

- **MPx08 and above:** The value entered in the "Test torque factor redundant holding brake" field is multiplied with the torque parameterized in "SBS: Nominal load". This allows the test torque of the redundant holding brake to be modified.

  The corresponding parameter is "P-0-3317, SBS: Test torque factor redundant holding brake".
- In the field "SBS: Torque/force constant", enter the torque/force constant of the motor. Take the value from the type plate of the motor or the parameter "P-0-0051, Torque/force constant".
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.
- Apply the inputs with "Next".

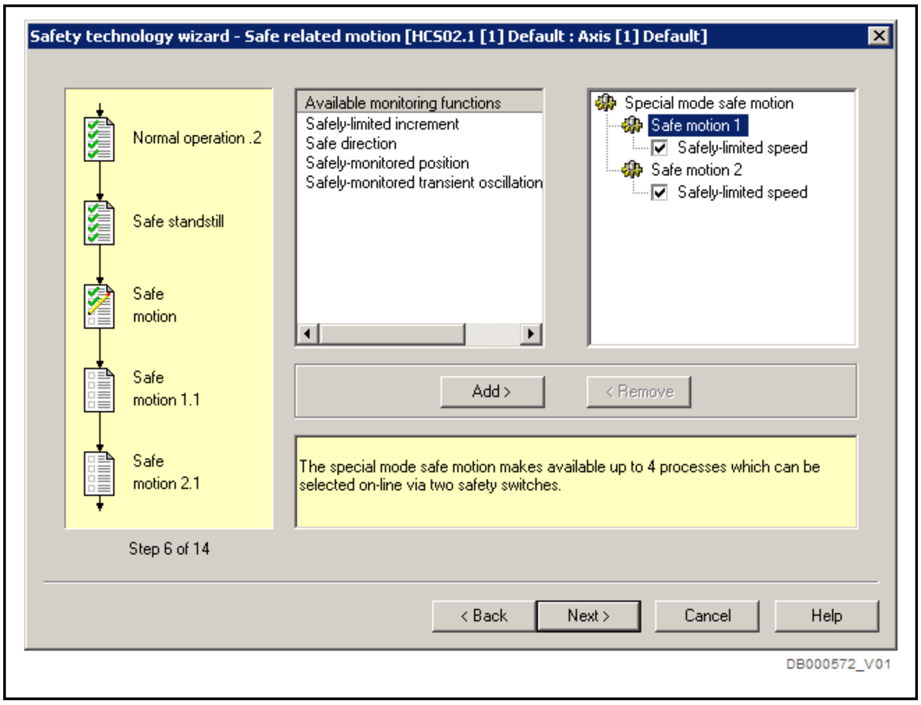
☞ For further information on commissioning, see "Safety function"Safe braking and holding system"".

Parameterizing the functions for "Safe motion"

In the following dialogs, make all the settings for Safe motion. The number of the following dialogs depends on the settings previously made. The parameter setting for Safe motion is explained using the example of Safe motion 1. The parameter setting for other Safe motions is made in the same way.

☞ For the special mode "Safe motion", it is possible to create up to four different parameter sets:

- P-0-3240, Configuration of safe motion 1
- P-0-3250, Configuration of safe motion 2
- P-0-3260, Configuration of safe motion 3
- P-0-3270, Configuration of safe motion 4



Safety technology wizard - Safe related motion [HCS02.1 [1] Default : Axis [1] Default]

Available monitoring functions
Safely-limited increment
Safe direction
Safely-monitored position
Safely-monitored transient oscillation

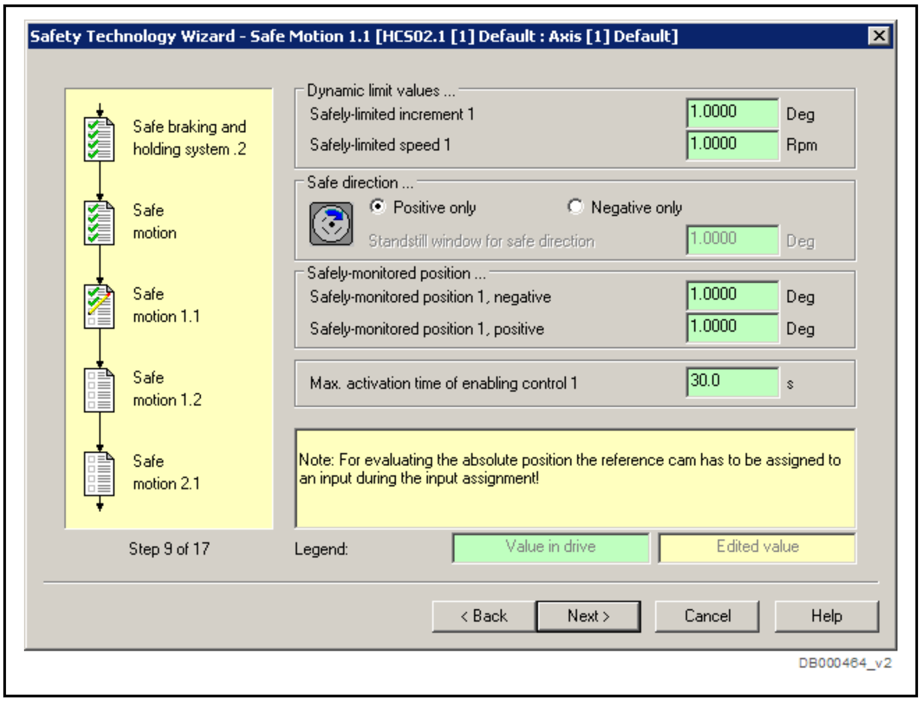
Special mode safe motion
- Safe motion 1
  - ☑ Safely-limited speed
- Safe motion 2
  - ☑ Safely-limited speed

The special mode safe motion makes available up to 4 processes which can be selected on-line via two safety switches.

Fig. 8-14: Start dialog for settings of Safe motion

- Select the monitoring functions to be applied to Safe motion 1: From the list of available monitoring functions, highlight the monitoring functions which are used and assign them to the Safe motion using "Add". Undo an incorrect selection using "Remove". "Safely-limited speed" is always part of Safe motion and cannot be deselected. The corresponding parameter is "P-0-3240, Configuration of safe motion 1".
- Apply the inputs with "Next".

☞ For further information on commissioning, see "Safety functions in special mode "Safe motion" (SMM)".



Safety Technology Wizard - Safe Motion 1.1 [HCS02.1 [1] Default : Axis [1] Default]

Dynamic limit values ...

Safely-limited increment 1: 1.0000 Deg

Safely-limited speed 1: 1.0000 Rpm

Safe direction ...

● Positive only ○ Negative only

Standstill window for safe direction: 1.0000 Deg

Safely-monitored position ...

Safely-monitored position 1, negative: 1.0000 Deg

Safely-monitored position 1, positive: 1.0000 Deg

Max. activation time of enabling control 1: 30.0 s

Note: For evaluating the absolute position the reference cam has to be assigned to an input during the input assignment!

Step 9 of 17

Legend: 🟩 Value in drive 🟨 Edited value

Fig. 8-15: Dialog for settings of Safe motion

- The "Safely-limited increment 1" field only takes effect in the special mode "Safe motion 1" (SMM1).

  In this field, by entering a numerical value, define a relative position window for SMM1 which is opened with the beginning of SMM1. For the duration of SMM1, the drive can be freely moved within this position window.

☞ The increment for the respective parameter set can be defined using the following parameters:

- P-0-3243, Safety-limited increment 1
- P-0-3253, Safety-limited increment 2
- P-0-3263, Safety-limited increment 3
- P-0-3273, Safety-limited increment 4

- In the "Safely-limited speed 1" field, define the speed threshold (bipolar) for the safety function "Safely-limited speed".

  The safety function "Safely-limited speed" is always active in the special mode "Safe motion 1".

☞ The speed threshold that is monitored can be defined for each parameter set using the following parameters:

- P-0-3244, Safely-limited speed 1
- P-0-3254, Safely-limited speed 2
- P-0-3264, Safely-limited speed 3
- P-0-3274, Safely-limited speed 4

- In the respective special mode "Safe motion", the axis may only be moved in the parameterized direction when the monitoring function of the direction of motion has been activated. In the dialog section "Safe direction...", determine the direction of Safe motion (positive or negative).

☞ If global monitoring of the direction of motion has been parameterized, it is active in the special mode "Safe motion", too. In the special mode "Safe motion", it is impossible to parameterize a differing direction of motion!

☞ The Safe direction that is monitored can be defined for each parameter set using the following parameters:

- P-0-3240, Configuration of safe motion 1
- P-0-3250, Configuration of safe motion 2
- P-0-3260, Configuration of safe motion 3
- P-0-3270, Configuration of safe motion 4

- The dialog section "Safe direction..." also contains a field called "Standstill window for safe direction". The value entered in this field determines how far the axis may move in the direction which has not been enabled.

  The corresponding parameter is "P-0-3232, Standstill window for safe direction".

☞ It is impossible to make any input in the field called "Standstill window for safe direction" when the safety function "Safely-limited position" has been activated in the "Normal operation" dialog. The standstill window thereby has already been parameterized.

- In the dialog section "Safely-monitored position...", define the upper and lower position limit which cannot be passed in the respective special mode "Safe motion".

☞ The upper and lower position limits that are monitored can be defined for each parameter set using the following parameters:

- P-0-3241, Safely-monitored position 1, positive
- P-0-3242, Safely-monitored position 1, negative
- P-0-3251, Safely-monitored position 2, positive
- P-0-3252, Safely-monitored position 2, negative

- In text field "Max. activation time of enabling control" or "Max. activation time of enabling control 1", enter the maximum allowed time for activating the enabling control. At the latest when the entered time is over, the enabling control has to be deactivated; i.e. the special mode "Safe motion" is temporary.

  The corresponding parameter is "P-0-3222, Max. activation time of enabling control" or in the case of an individual activation time of enabling control for each special mode "Safe motion":

  – P-0-3246, Max. activation time of enabling control 1

  – P-0-3256, Max. activation time of enabling control 2

  – P-0-3266, Max. activation time of enabling control 3

  – P-0-3276, Max. activation time of enabling control 4

⚠ WARNING **Dangerous movements!**

Danger to life, risk of injury, serious injury or property damage by switching off the monitoring of activation time!

You can do without the monitoring of the activation time, if it is not common practice to use an enabling control in your industrial sector and if constant motion does not represent any danger.

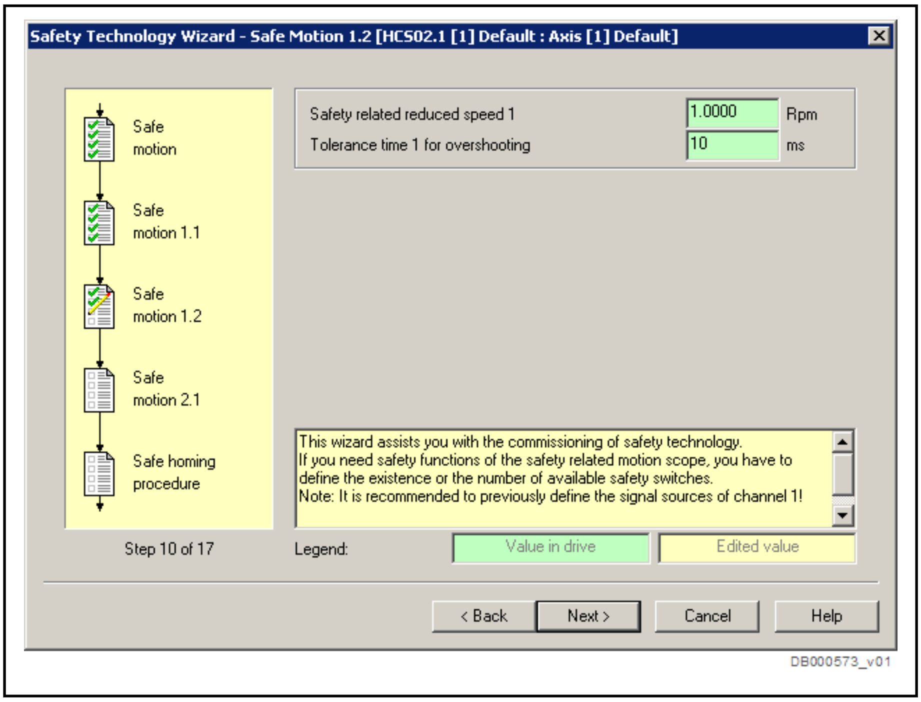
The machine manufacturer is responsible for the monitoring of the activation time and his risk analysis has to show his responsibility.

"P-0-3222, Max. activation time of enabling control"="0" deactivates the time monitoring of the special mode "safe motion"; this also applies to the individual activation times of enabling control P-0-3246, P-0-3256, P-0-3266 and P-0-3276.

- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.
- Apply the inputs with "Next".

With MPx08 and above, the monitoring function "Safely-monitored transient oscillation" is available. When this monitoring function has been selected, in the following dialog enter a limit value for the speed in the transient oscillation process (Safely-reduced speed) and the tolerance time for the overshooting of the speed.


Safety Technology Wizard - Safe Motion 1.2 [HCS02.1 [1] Default : Axis [1] Default]

Safety related reduced speed 1: 1.0000 Rpm
Tolerance time 1 for overshooting: 10 ms

This wizard assists you with the commissioning of safety technology.
If you need safety functions of the safety related motion scope, you have to define the existence or the number of available safety switches.
Note: It is recommended to previously define the signal sources of channel 1!

Fig. 8-16: Dialog for "Safely-monitored transient oscillation"

- In the "Safely-reduced speed 1" field, define the speed threshold (bipolar) for the safety function "Safely-monitored transient oscillation". This threshold only takes effect in the special mode "Safe motion 1" (SMM1).

☞ The speed threshold that is monitored can be defined for each parameter set using the following parameters:

- P-0-3247, Safely-reduced speed 1
- P-0-3257, Safely-reduced speed 2
- P-0-3267, Safely-reduced speed 3
- P-0-3277, Safely-reduced speed 4

- The "Tolerance time 1 for overshooting" field only takes effect in the special mode "Safe motion 1" (SMM1).

  In the field, define the time during which the actual speed may be above the "Safely-reduced speed 1" in SMM1. For this time, the velocity is monitored with regard to the "Safely-limited speed 1".

☞ The increment for the respective parameter set can be defined using the following parameters:

- P-0-3248, Tolerance time 1 for overshooting
- P-0-3258, Tolerance time 2 for overshooting
- P-0-3268, Tolerance time 3 for overshooting
- P-0-3278, Tolerance time 4 for overshooting

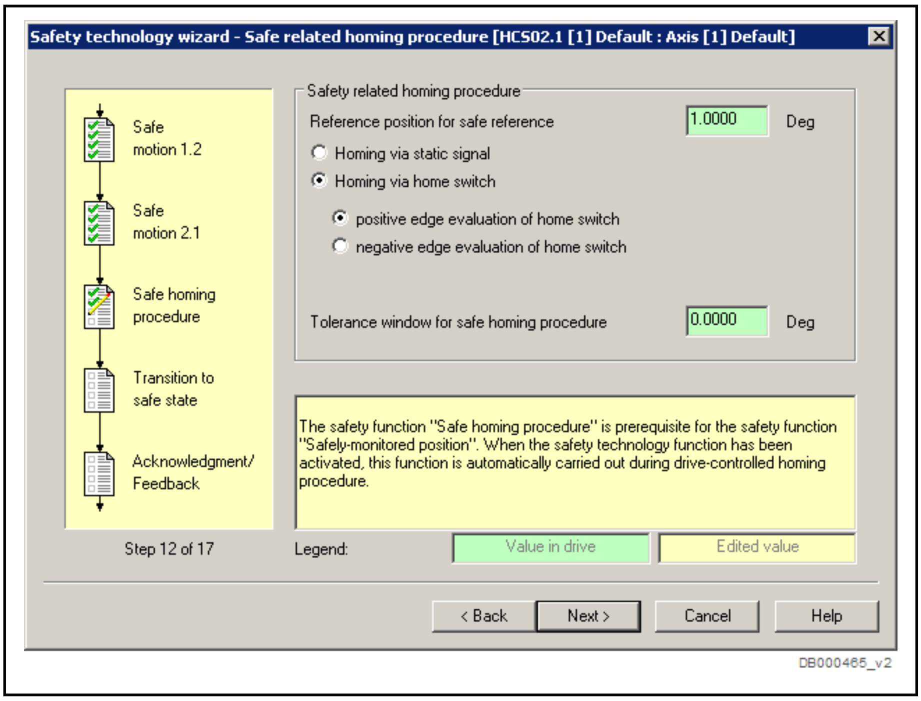
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.

- Apply the inputs with "Next".

Parameterizing the additional and auxiliary functions

In the following dialog, make all the settings for additional functions which are relevant both to the special mode "Safe standstill" and to the special mode "Safe motion". Only such dialogs are displayed in which it is necessary to make settings due to the parameterizations made before.


Safety technology wizard - Safe related homing procedure [HCS02.1 [1] Default : Axis [1] Default]

Safety related homing procedure
Reference position for safe reference: 1.0000 Deg
○ Homing via static signal
● Homing via home switch
● positive edge evaluation of home switch
○ negative edge evaluation of home switch
Tolerance window for safe homing procedure: 0.0000 Deg

The safety function "Safe homing procedure" is prerequisite for the safety function "Safely-monitored position". When the safety technology function has been activated, this function is automatically carried out during drive-controlled homing procedure.

Fig. 8-17: IndraWorks dialog for parameterizing the additional and auxiliary function "Safe homing procedure"

- In the text field "Reference position for safe reference", determine the position value for channel 2. The value takes effect as actual position value after the command "C4000 Homing procedure command channel 2" has been executed.

  The corresponding parameter is "P-0-3231, Reference position for safe reference".
- Then determine whether the reference signal for channel 2 is to be evaluated statically or dynamically. In the case of dynamic evaluation (home switch), the evaluation can refer to the positive or negative edge.

  The corresponding parameter is "P-0-3210, Safety technology configuration".

☞ Dynamization cannot be carried out for the home switch / the cam!

- In the text field "Tolerance window for safe homing procedure", set the maximum allowed deviation of the actual position values of channel 1 and 2 during the execution of the command "C4000 Homing procedure command channel 2".

  The corresponding parameter is "P-0-3229, Tolerance window for safe homing procedure".

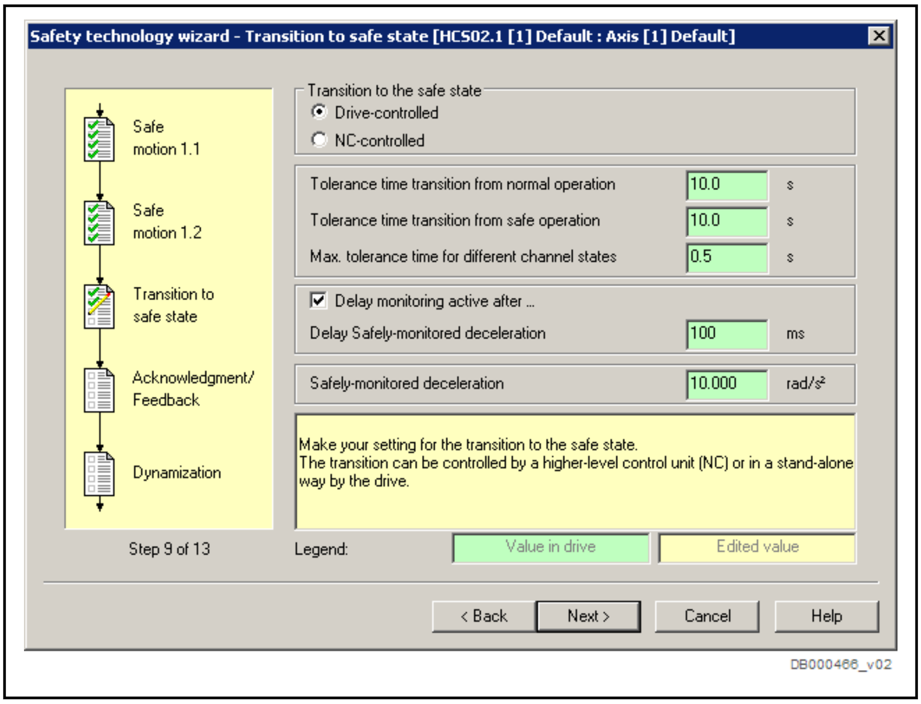
☞ For further information on commissioning, see "Safe homing procedure".

- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.
- Apply the inputs with "Next".

Step 6: Configuring the system behavior

Configuring the transition to the safe state



Safety technology wizard - Transition to safe state [HCS02.1 [1] Default : Axis [1] Default]

Transition to the safe state
● Drive-controlled
○ NC-controlled

Tolerance time transition from normal operation	10.0	s
Tolerance time transition from safe operation	10.0	s
Max. tolerance time for different channel states	0.5	s

☑ Delay monitoring active after ...

Delay Safely-monitored deceleration	100	ms
Safely-monitored deceleration	10.000	rad/s²

Make your setting for the transition to the safe state.
The transition can be controlled by a higher-level control unit (NC) or in a stand-alone way by the drive.

Step 9 of 13

Legend: 🟩 Value in drive 🟨 Edited value

Fig. 8-18: Dialog for settings for transition to the safe state

- Select whether the transition to the safe state is to take place in drive-controlled or NC-controlled form.

  The corresponding parameter is "P-0-3210, Safety technology configuration".

☞ For further information on the transition to the safe state, see "Transition to safe state".

For further information on commissioning, see "Safely-monitored stopping process".

- In the text field "Tolerance time transition from normal operation", enter the maximum time made available within which, in the case of transitions from normal operation to a safety function, the command value system of the drive must have been adjusted to the new safety function.

  The corresponding parameter is "P-0-3220, Tolerance time transition from normal operation".
- In the text field "Tolerance time transition from safe operation", enter the maximum time made available within which, in the case of transitions from one safety function to another, the command value system of the drive must have been adjusted.

  The corresponding parameter is "P-0-3225, Tolerance time transition from safe operation".
- In the text field "Max. tolerance time for different channel states", enter the maximum allowed time during which the selection of the monitoring channels 1 and 2 may differ without an error being generated.

  The corresponding parameter is "P-0-3221, Max. tolerance time for different channel states".
- In the text field "Delay Safely-monitored deceleration", it is possible to parameterize, for the transition processes, the time span after which deceleration monitoring becomes "active". To deactivate the delay, enter the value "0".

  The corresponding parameter is "P-0-3226, Delay Safely-monitored deceleration".

  MPx07V10 and above: If a value unequal "0" is entered in the text field "Delay Safely-monitored deceleration", the monitoring function can be deactivated for the duration of the "Delay Safely-monitored deceleration" by activating the check box "Delay monitoring active after ...". In this case, only the configured monitoring functions for "normal operation and special mode" are active (see chapter "Safety functions in normal operation and in special mode"). The corresponding parameter is "P-0-3210, Safety technology configuration".
- In the text field "Safely-monitored deceleration", enter the deceleration which is preset for the drive by the control unit during the stopping processes.

  The corresponding parameter is "P-0-3282, Safely-monitored deceleration".
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

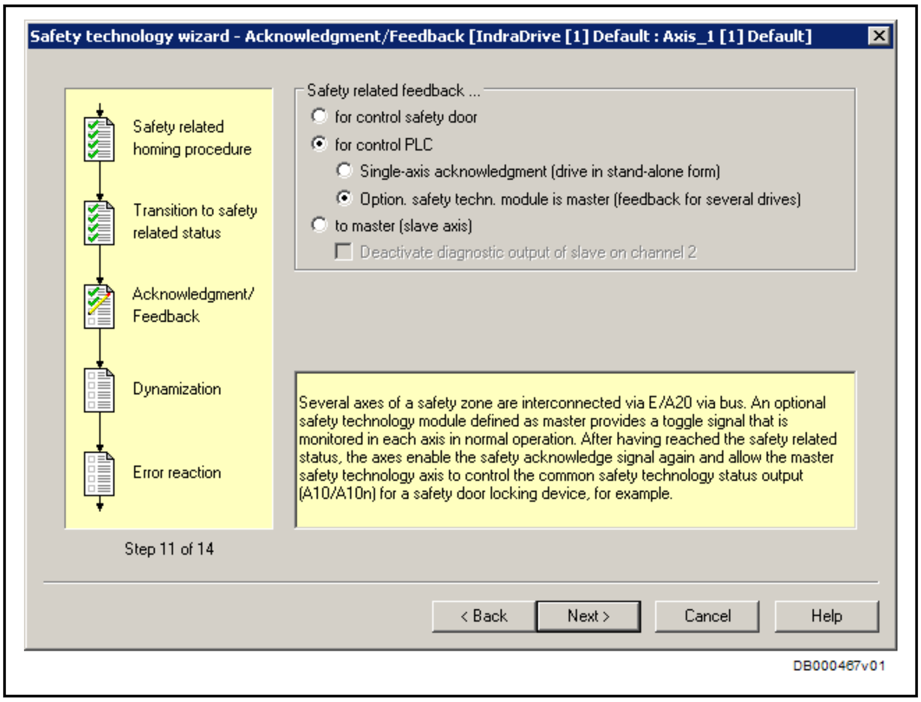
  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.

- Apply the inputs with "Next".

Configuring the outputs for feedback of safety functions

In the following dialog, make the settings for diagnosis and acknowledgment of safety, as well as for safe feedback.

☞ No settings are required if PROFIsafe is used, because feedback to the safety PLC is transmitted via the F-data.



Safety technology wizard - Acknowledgment/Feedback [IndraDrive [1] Default : Axis_1 [1] Default]

Safety related feedback ...
○ for control safety door
● for control PLC
○ Single-axis acknowledgment (drive in stand-alone form)
● Option. safety techn. module is master (feedback for several drives)
○ to master (slave axis)
☐ Deactivate diagnostic output of slave on channel 2

Several axes of a safety zone are interconnected via E/A20 via bus. An optional safety technology module defined as master provides a toggle signal that is monitored in each axis in normal operation. After having reached the safety related status, the axes enable the safety acknowledge signal again and allow the master safety technology axis to control the common safety technology status output (A10/A10n) for a safety door locking device, for example.

Step 11 of 14

Fig. 8-19: IndraWorks D dialog for diagnosis and acknowledgment of safety, as well as for safe feedback (Note: The contents of the dialog depend on the firmware used / the IndraWorks version used)

- The axis can be parameterized in such a way that it gives safe feedback in the form of
  - "control safety door",
  - "control PLC" or
  - as "slave axis" within a safety zone to the feedback master.

  If "for control PLC" is selected, it is possible to choose whether the axis works in stand-alone form: "Single-axis acknowledgment", or gives safe feedback for a safety zone: "Option. safety techn. module is master".

- When setting up safety zones, one master for diagnosis and acknowledgment has to be parameterized for each zone. Set all other drives in this zone as slaves. If the I/Os on the optional safety technology module (connector X41) are wired as a bus (e.g., via ribbon cable), the diagnostic output has to be deactivated for all slaves ("Deactivate diagnostic output of slave on channel 2"). If a single safety technology axis, which is not to acknowledge safety, is commissioned, this axis has to be parameterized with "for control PLC" / "Option. safety techn. module is master". The corresponding parameter is "P-0-3210, Safety technology configuration".

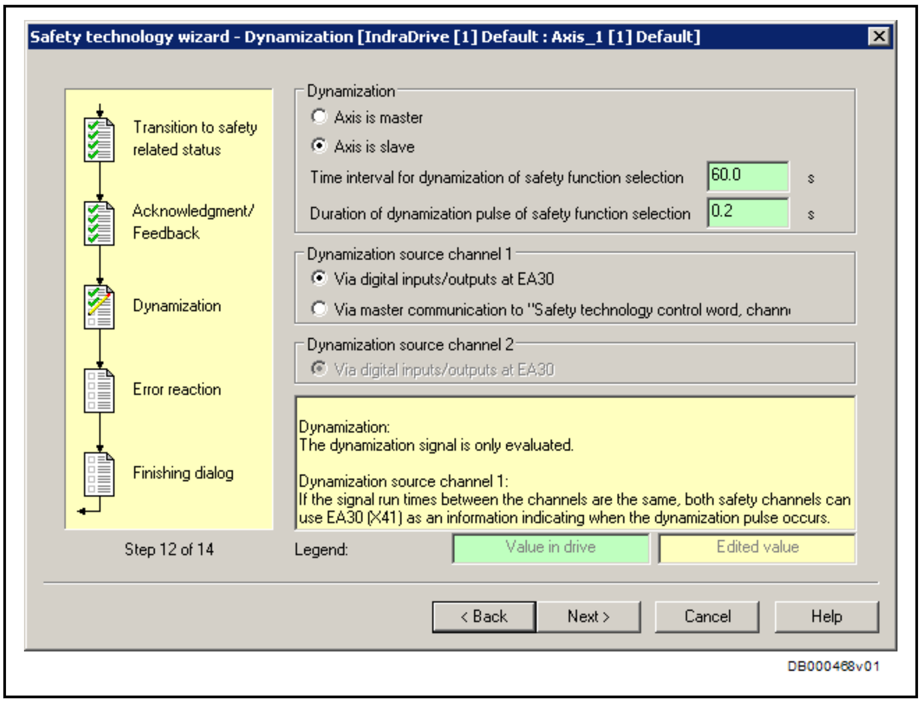
☞ It is possible to have a maximum of 25 drives in one safety zone!

☞ For further information on commissioning, see "Feedback of safety technology operating states to the peripherals".

- Apply the inputs with "Next".

Dynamization

☞ Using PROFIsafe does not require dynamization.



Safety technology wizard - Dynamization [IndraDrive [1] Default : Axis_1 [1] Default]

Dynamization
○ Axis is master
● Axis is slave
Time interval for dynamization of safety function selection: 60.0 s
Duration of dynamization pulse of safety function selection: 0.2 s

Dynamization source channel 1
● Via digital inputs/outputs at EA30
○ Via master communication to "Safety technology control word, chann

Dynamization source channel 2
● Via digital inputs/outputs at EA30

Dynamization:
The dynamization signal is only evaluated.

Dynamization source channel 1:
If the signal run times between the channels are the same, both safety channels can use EA30 (X41) as an information indicating when the dynamization pulse occurs.

Legend: Value in drive | Edited value

Fig. 8-20: Dialog for settings of forced dynamization of inputs

- In the dialog section named "Dynamization", select whether the axis is to carry out the dynamization of the safety zone ("Axis is master"), or whether a different axis or the higher-level control unit is to carry out dynamization ("Axis is slave").

  The corresponding parameter is "P-0-3210, Safety technology configuration".

- In the text field "Time interval for dynamization of safety function selection", define the cycle time in which forced dynamization is to take place.

  If the axis has been parameterized as **dynamization master**, in this field set the time interval in which the axis is to carry out dynamization.

  If the axis has been parameterized as **dynamization slave**, in this field set the time within which dynamization must have taken place.

  The corresponding parameter is "P-0-3223, Time interval for dynamization of safety function selection".

☞ "Time interval for dynamization of safety function selection" has an effect on the reaction time, because during the dynamization of safety function selection, the evaluation of the selection signals inevitably has to be suspended. This is why the time should not be too short.

- In the text field "Duration of dynamization pulse of safety function selection", define the maximum duration of the dynamization pulse.

  If the axis has been parameterized as **dynamization master**, in this field set the duration of the dynamization pulse with which the axis is to carry out dynamization.

  If the axis has been parameterized as **dynamization slave**, in this field enter the maximum length which the dynamization pulse may have. An externally generated dynamization signal can be shorter, but should not be shorter than the **minimum pulse width** of **30 ms**!

  The corresponding parameter is "P-0-3224, Duration of dynamization pulse of safety function selection".

☞ The "duration of dynamization pulse of safety function selection" has an effect on the reaction time, because during the dynamization of safety function selection the evaluation of the selection signals inevitably has to be suspended. This is why the duration should not be too long.

- In the dialog section named "Dynamization source channel 1", select via which path the channel 1 gets the information as to when dynamization takes place. If the signal run times of selection via channel 1 and channel 2 are equal, it is possible to select "Via digital inputs/outputs at IO30" in this dialog section. If the selection information of channel 1 is transmitted via the master communication, or if the signal run times of selection of the two channels differ due to other reasons, select "Via master communication to Safety technology control word, channel 1". This selection also has to be made if the axis is a dynamization master.

  The corresponding parameter is "P-0-3210, Safety technology configuration".

☞ With the dynamization type "Via master communication to Safety technology control word, channel 1", the substitute for input I30 has to be supplied in "P-0-3212, Safety technology control word, channel 1" for channel 1, and IO30 has to be supplied on connector X41 for channel 2.

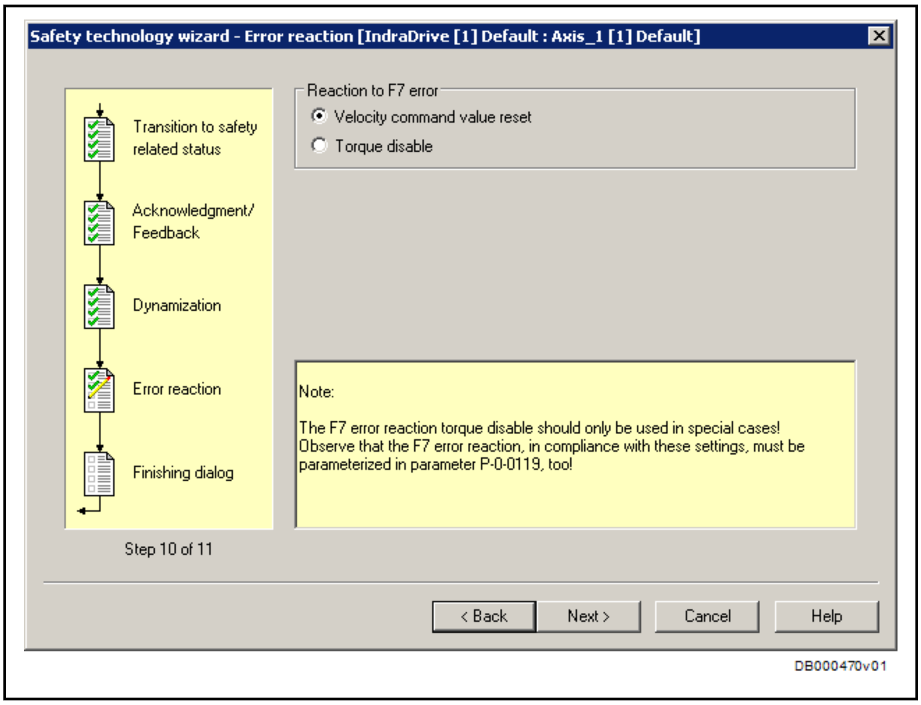
- Apply the inputs with "Next".
- Confirm the changed safety technology parameters by repeating the input.

  All values marked with green background color in the safety technology wizard were read directly from the drive and not edited by the user. If the value is marked with yellow background color, it was edited by the user and has not yet been written to the drive. Every input applied to safety technology parameters has to be verified by a second input. In the safety technology wizard, inputs are cleared in the corresponding edit fields and remain highlighted with yellow color. To assist you with the repeated input, the initial input value is displayed below in the notice field.

- Apply the inputs with "Next".

Error reaction

In the following dialog, it is possible to set the error reaction of the drive to safety technology errors.


Safety technology wizard - Error reaction [IndraDrive [1] Default : Axis_1 [1] Default]

Reaction to F7 error

● Velocity command value reset
○ Torque disable

Note:

The F7 error reaction torque disable should only be used in special cases! Observe that the F7 error reaction, in compliance with these settings, must be parameterized in parameter P-0-0119, too!

Fig. 8-21: Dialog for setting error reaction to safety technology errors

- In the dialog section "Reaction to F7 error", it is possible to parameterize the error reaction of the axis to safety technology errors.

  The corresponding parameter is "P-0-3210, Safety technology configuration".

☞ The setting made for the F7 error reaction in this dialog section has to comply with the settings in P-0-0119.

⚠ WARNING Dangerous movements!

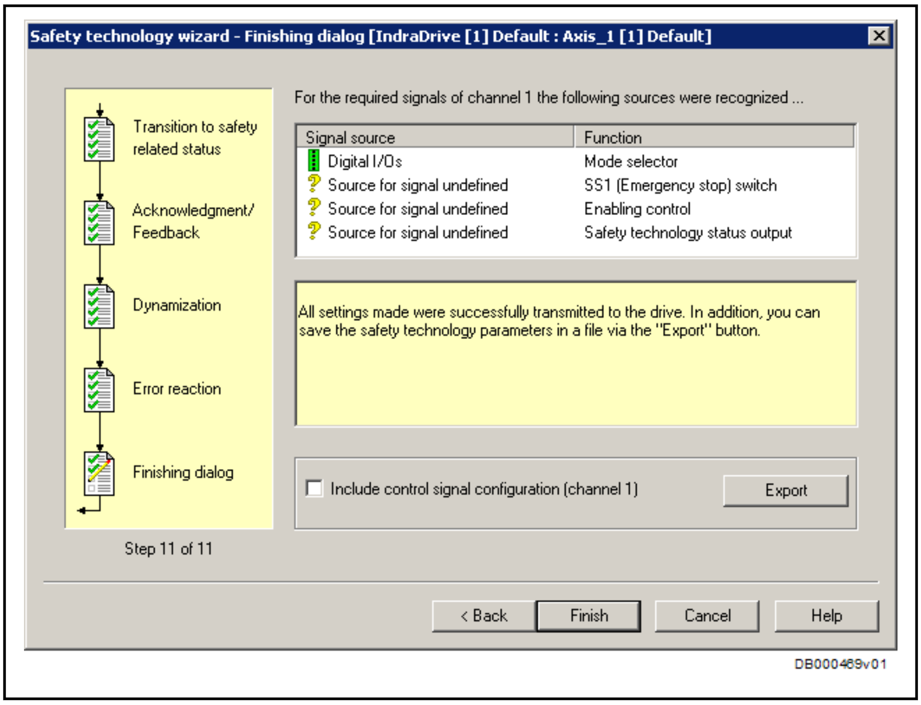
Danger to life, risk of injury, serious injury or property damage by F7 error reaction "torque disable"!

The F7 error reaction "torque disable" should only be used when forced deceleration by velocity command value reset generally causes problems, e.g. in the case of mechanically coupled axes.

The machine manufacturer is responsible for the F7 error reaction "torque disable" and his risk analysis has to show his responsibility.

- Apply the inputs with "Next".

Finishing the parameter setting



Safety technology wizard - Finishing dialog [IndraDrive [1] Default : Axis_1 [1] Default]

For the required signals of channel 1 the following sources were recognized ...

Signal source	Function
Digital I/Os	Mode selector
? Source for signal undefined	SS1 (Emergency stop) switch
? Source for signal undefined	Enabling control
? Source for signal undefined	Safety technology status output

All settings made were successfully transmitted to the drive. In addition, you can save the safety technology parameters in a file via the "Export" button.

□ Include control signal configuration (channel 1)

Fig. 8-22: Finishing the parameter setting

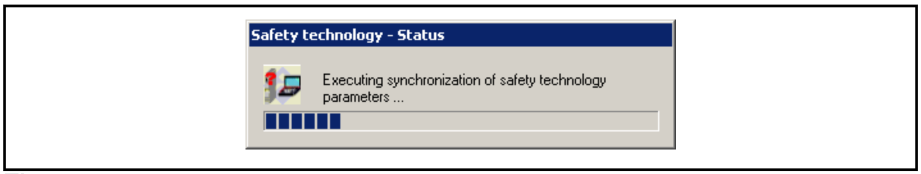
In the finishing dialog, the first check is run to find out whether a source was found for all parameterized inputs/outputs (I/Os) of channel 1. If there is no source available for a signal, "?" appears in the "Signal source" column and the "Source for signal undefined" message is generated. Commissioning via the safety technology wizard can nevertheless continue in unmodified form. The missing signal has to be assigned afterwards.

- Using the "Export" button, it is possible to save the safety technology setting, that was made, in a parameter file. It is possible to include the control signal configuration for channel 1 in the backup.

☞ It is impossible to replace the control section with the exported parameter file, because the parameter "P-0-3208, Backup of safety techn. data channel 2", which is relevant for replacing the control section, is not contained in this parameter file!

- With the "Finish" button, the safety technology wizard is completed, the drive switched to phase 4 and the command "P-0-3204, C3000 Synchronize and store safety technology IDN command" is started.

  By the execution of the command "P-0-3204, C3000 Synchronize and store safety technology IDN command", channel 2 applies the safety parameters of channel 1 and stores them in the safety memory.



Safety technology - Status

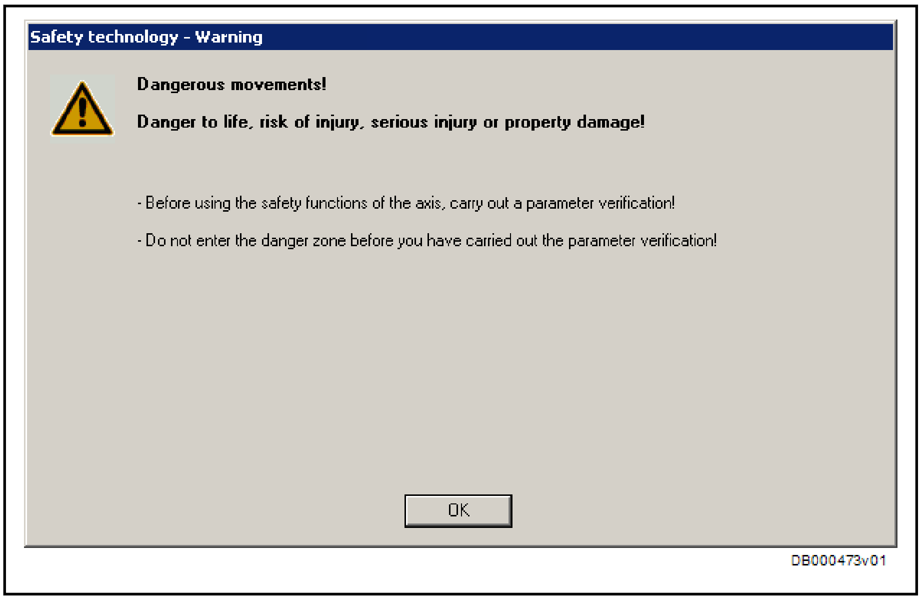
Executing synchronization of safety technology parameters ...

Figure name DB000100

Fig. 8-23: Synchronizing the safety technology parameters

☞ In the case of switching errors, the command cannot be automatically started; it has to be restarted manually after the switching errors have been fixed.

- Afterwards, the following notice concerning the parameter verification appears and has to be confirmed with "OK". The safety technology may only be used after the parameter verification has been carried out successfully.



Safety technology - Warning

Dangerous movements!

Danger to life, risk of injury, serious injury or property damage!

- Before using the safety functions of the axis, carry out a parameter verification!

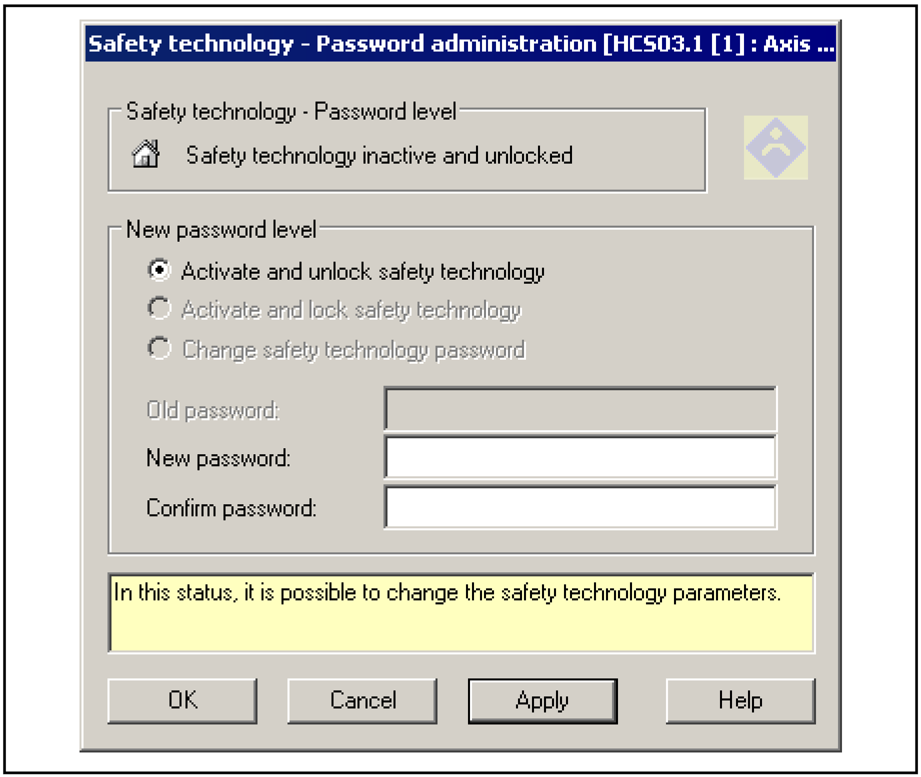
- Do not enter the danger zone before you have carried out the parameter verification!

Fig. 8-24: Notice concerning parameter verification

Step 7: Activating / deactivating safety technology

Activating the safety technology

After the safety technology parameters were successfully synchronized and stored, the safety technology has to be activated.



Safety technology - Password administration [HCS03.1 [1] : Axis ...

Safety technology - Password level

Safety technology inactive and unlocked

New password level

● Activate and unlock safety technology

○ Activate and lock safety technology

○ Change safety technology password

Old password:

New password:

Confirm password:

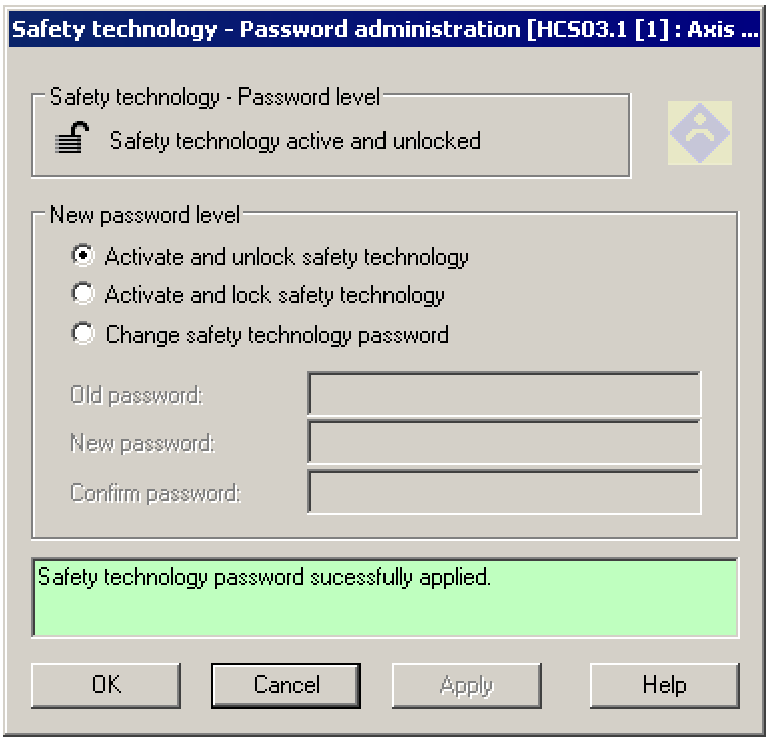
In this status, it is possible to change the safety technology parameters.

Figure name DB000101

Fig. 8-25: Safety technology – password administration

- Safety technology is activated by inputting the safety technology password (P-0-3206, Safety technology password) and confirming it using the "Apply" button.

  Safety technology now is active and unlocked. In this state, it is possible to change the safety technology parameters without entering the password. After every change, the command "P-0-3204, C3000 Synchronize and store safety technology IDN command" has to be executed again in order to apply the change.



Safety technology - Password administration [HCS03.1 [1] : Axis ...

Safety technology - Password level

Safety technology active and unlocked

New password level

● Activate and unlock safety technology

○ Activate and lock safety technology

○ Change safety technology password

Old password:

New password:

Confirm password:

Safety technology password sucessfully applied.

Figure name DB000102

Fig. 8-26: Safety technology – password administration

In the safety technology password administration, it is now possible to write-protect the safety technology parameters using the "Activate and lock safety technology" field.

☞ When the drive is switched off, safety technology is automatically locked.

Deactivating the safety technology

Executing the command "S-0-0262, C07_x Load defaults procedure command" (with "P-0-4090, Configuration for loading default values"="A5") deactivates safety technology. The system parameters then are invalid and neither validation tests nor data comparisons are carried out. The safety technology parameters are set to their default values again.

☞ The execution of the command "S-0-0262, C07_x Load defaults procedure command" cannot be undone. In the case of changes to safety-relevant parameters, it is necessary to subsequently carry out the safety technology commissioning with safety technology acceptance test again!

If there are no changes required, the safety technology can be activated again according to the procedure for replacing the control section.

☞ Deactivating a drive within a safety zone causes the error F3131 at other drive modules that have been equipped with the optional module "Safe Motion". **The safety of a zone can only be guaranteed, if all drives run with active safety technology.**

Step 8: Carrying out parameter verification

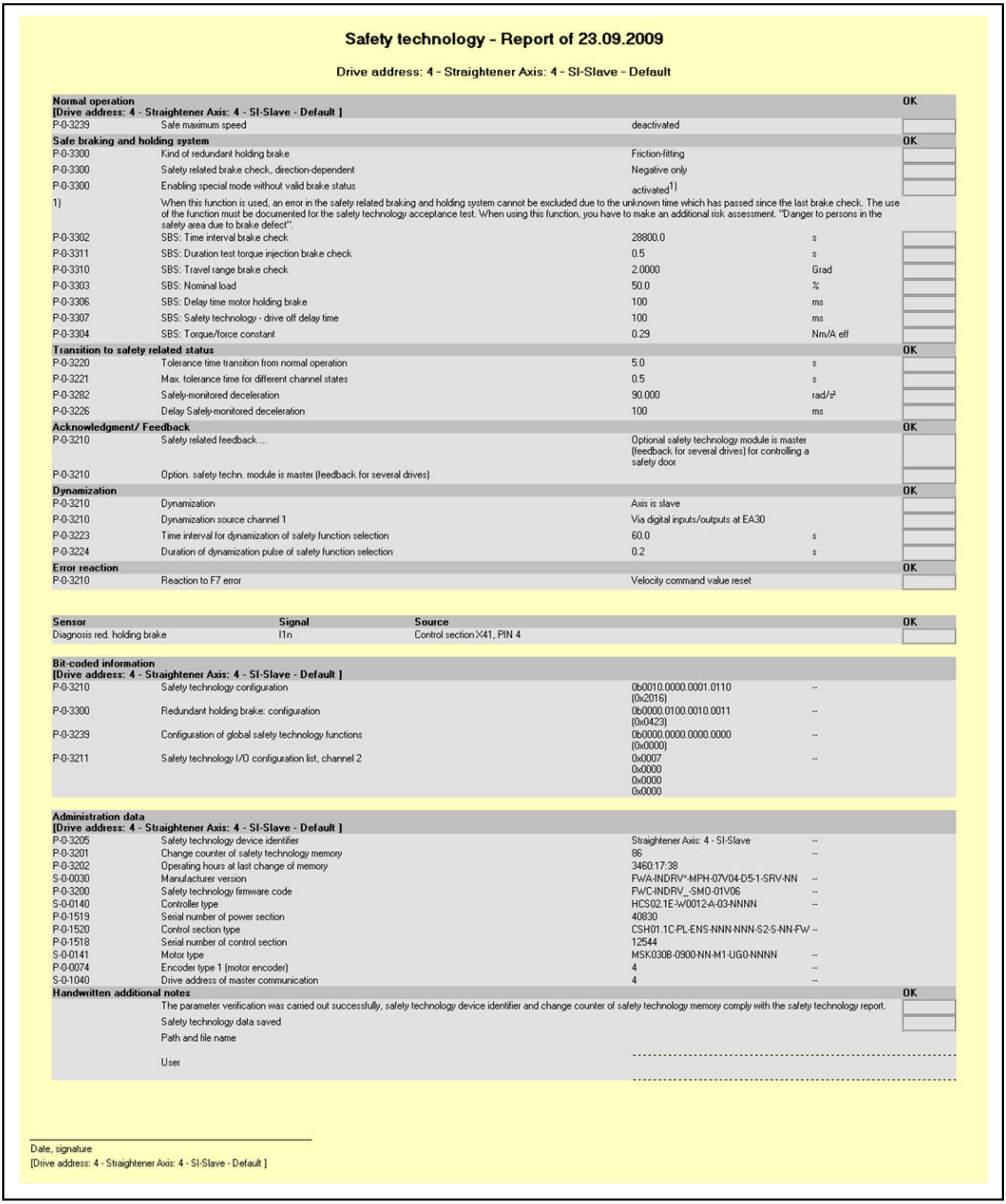
Upon completed parameterization and activation of safety technology, the parameter verification has to be carried out before the safety functions are used for the first time. With the parameter verification, the following aspects are to be checked/verified:

- Check as to whether the parameterization active in the drive complies with the planned or projected parameters for this axis.
- Verification of the active parameterization as compared to the safety technology report in order to detect possible transmission errors.

Carrying out the parameter verification requires the safety technology report and the parameter verification tool. The safety technology report can be called and printed in IndraWorks as follows:

1. Open window "Safety technology/Diagnosis".
2. Right side of window displays safety technology report.
3. Open context menu on left side of window by clicking right mouse button.
4. Select **Safety technology report ▸ Print.**

   Safety technology report can now be printed.



Safety technology - Report of 23.09.2009

Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default

Normal operation [Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]				**OK**
P-0-3239	Safe maximum speed	deactivated		□
Safe braking and holding system				**OK**
P-0-3300	Kind of redundant holding brake	Friction-fitting		□
P-0-3300	Safety related brake check, direction-dependent	Negative only		□
P-0-3300	Enabling special mode without valid brake status	activated[1)]		□
1)	When this function is used, an error in the safety related braking and holding system cannot be excluded due to the unknown time which has passed since the last brake check. The use of the function must be documented for the safety technology acceptance test. When using this function, you have to make an additional risk assessment. "Danger to persons in the safety area due to brake defect".			
P-0-3302	SBS: Time interval brake check	28800.0	s	□
P-0-3311	SBS: Duration test torque injection brake check	0.5	s	□
P-0-3310	SBS: Travel range brake check	2.0000	Grad	□
P-0-3303	SBS: Nominal load	50.0	%	□
P-0-3306	SBS: Delay time motor holding brake	100	ms	□
P-0-3307	SBS: Safety technology - drive off delay time	100	ms	□
P-0-3304	SBS: Torque/force constant	0.29	Nm/A eff	□
Transition to safety related status				**OK**
P-0-3220	Tolerance time transition from normal operation	5.0	s	□
P-0-3221	Max. tolerance time for different channel states	0.5	s	□
P-0-3282	Safely-monitored deceleration	90.000	rad/s²	□
P-0-3226	Delay Safely-monitored deceleration	100	ms	□
Acknowledgment/ Feedback				**OK**
P-0-3210	Safety related feedback ...	Optional safety technology module is master (feedback for several drives) for controlling a safety door		□
P-0-3210	Option. safety techn. module is master (feedback for several drives)			□
Dynamization				**OK**
P-0-3210	Dynamization	Axis is slave		□
P-0-3210	Dynamization source channel 1	Via digital inputs/outputs at EA30		□
P-0-3223	Time interval for dynamization of safety function selection	60.0	s	□
P-0-3224	Duration of dynamization pulse of safety function selection	0.2	s	□
Error reaction				**OK**
P-0-3210	Reaction to F7 error	Velocity command value reset		□

Sensor	**Signal**	**Source**	**OK**
Diagnosis red. holding brake	I1n	Control section X41, PIN 4	□

Bit-coded information [Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]			
P-0-3210	Safety technology configuration	0b0010.0000.0001.0110 (0x2016)	--
P-0-3300	Redundant holding brake: configuration	0b0000.0100.0010.0011 (0x0423)	--
P-0-3239	Configuration of global safety technology functions	0b0000.0000.0000.0000 (0x0000)	--
P-0-3211	Safety technology I/O configuration list, channel 2	0x0007 0x0000 0x0000 0x0000	--

Administration data [Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]				
P-0-3205	Safety technology device identifier	Straightener Axis: 4 - SI-Slave	--	
P-0-3201	Change counter of safety technology memory	86	--	
P-0-3202	Operating hours at last change of memory	3460:17:38		
S-0-0030	Manufacturer version	FWA-INDRV*-MPH-07V04-D5-1-SRV-NN	--	
P-0-3200	Safety technology firmware code	FWC-INDRV_-SMO-01V06	--	
S-0-0140	Controller type	HCS02.1E-W0012-A-03-NNNN	--	
P-0-1519	Serial number of power section	40830		
P-0-1520	Control section type	CSH01.1C-PL-ENS-NNN-NNN-S2-S-NN-FW	--	
P-0-1518	Serial number of control section	12544		
S-0-0141	Motor type	MSK030B-0900-NN-M1-UG0-NNNN	--	
P-0-0074	Encoder type 1 (motor encoder)	4	--	
S-0-1040	Drive address of master communication	4	--	
Handwritten additional notes				**OK**
	The parameter verification was carried out successfully, safety technology device identifier and change counter of safety technology memory comply with the safety technology report.			□
	Safety technology data saved			□
	Path and file name	------------------------------		
	User	------------------------------		

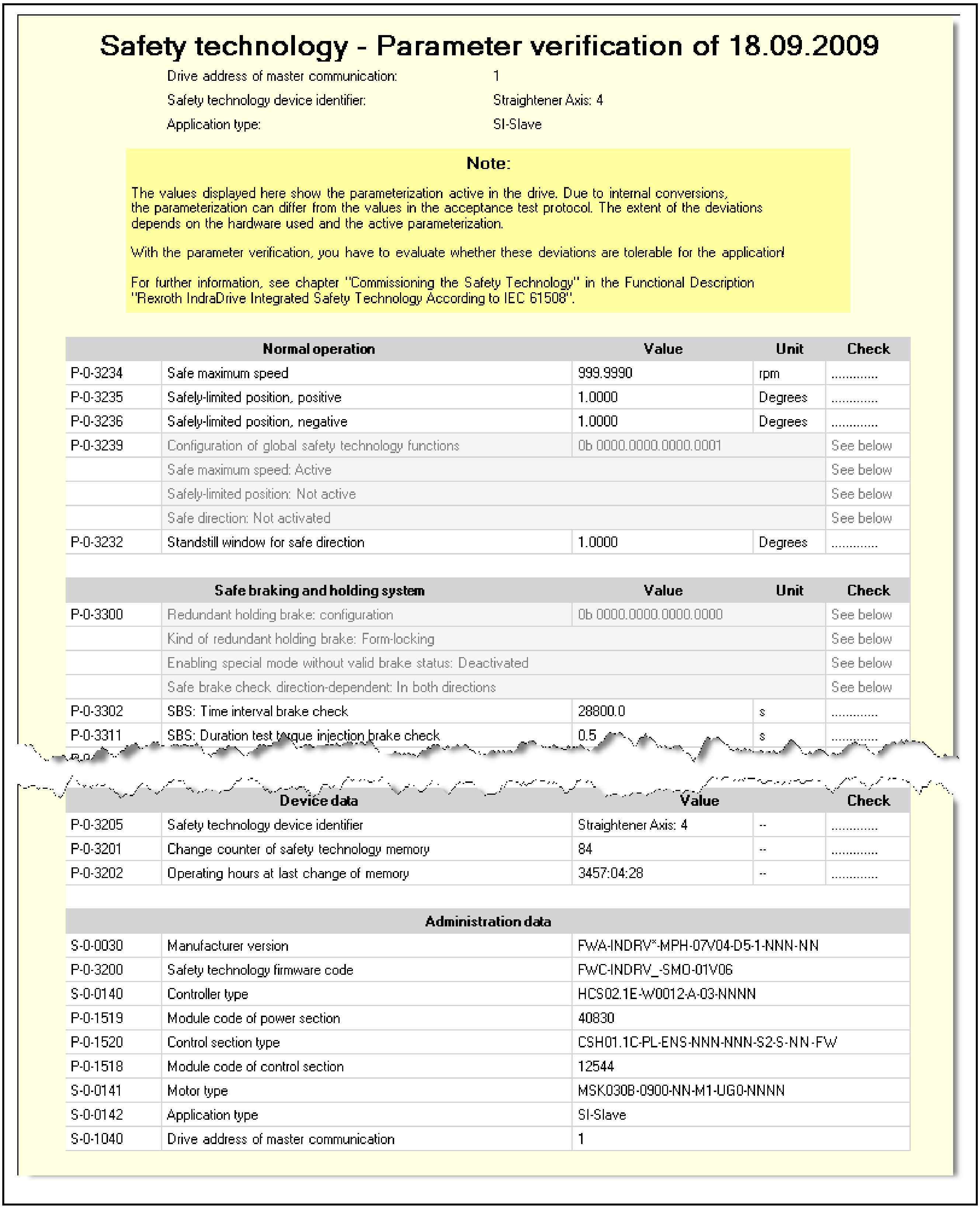
____
Date, signature
[Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]

Fig. 8-27: Example of a safety technology report

The parameter verification tool can be started in IndraWorks as follows:

1. Open window "Safety technology/Diagnosis".
2. Right side of window displays safety technology report.

3. Above safety technology report, there is the "Verify safety parameters" button. Start parameter verification tool using this button.
4. Using the menu "File / Print" in new window of parameter verification, verification can be printed.



Safety technology - Parameter verification of 18.09.2009

Drive address of master communication:	1
Safety technology device identifier:	Straightener Axis: 4
Application type:	SI-Slave

Note:

The values displayed here show the parameterization active in the drive. Due to internal conversions, the parameterization can differ from the values in the acceptance test protocol. The extent of the deviations depends on the hardware used and the active parameterization.

With the parameter verification, you have to evaluate whether these deviations are tolerable for the application!

For further information, see chapter "Commissioning the Safety Technology" in the Functional Description "Rexroth IndraDrive Integrated Safety Technology According to IEC 61508".

	Normal operation	Value	Unit	Check
P-0-3234	Safe maximum speed	999.9990	rpm	....
P-0-3235	Safely-limited position, positive	1.0000	Degrees	....
P-0-3236	Safely-limited position, negative	1.0000	Degrees	....
P-0-3239	Configuration of global safety technology functions	0b 0000.0000.0000.0001		See below
	Safe maximum speed: Active			See below
	Safely-limited position: Not active			See below
	Safe direction: Not activated			See below
P-0-3232	Standstill window for safe direction	1.0000	Degrees	....

	Safe braking and holding system	Value	Unit	Check
P-0-3300	Redundant holding brake: configuration	0b 0000.0000.0000.0000		See below
	Kind of redundant holding brake: Form-locking			See below
	Enabling special mode without valid brake status: Deactivated			See below
	Safe brake check direction-dependent: In both directions			See below
P-0-3302	SBS: Time interval brake check	28800.0	s	....
P-0-3311	SBS: Duration test torque injection brake check	0.5	s	....
P-0-				

	Device data	Value		Check
P-0-3205	Safety technology device identifier	Straightener Axis: 4	--	....
P-0-3201	Change counter of safety technology memory	84	--	....
P-0-3202	Operating hours at last change of memory	3457:04:28	--	....

	Administration data	
S-0-0030	Manufacturer version	FWA-INDRV*-MPH-07V04-D5-1-NNN-NN
P-0-3200	Safety technology firmware code	FWC-INDRV_-SMO-01V06
S-0-0140	Controller type	HCS02.1E-W0012-A-03-NNNN
P-0-1519	Module code of power section	40830
P-0-1520	Control section type	CSH01.1C-PL-ENS-NNN-NNN-S2-S-NN-FW
P-0-1518	Module code of control section	12544
S-0-0141	Motor type	MSK030B-0900-NN-M1-UG0-NNNN
S-0-0142	Application type	SI-Slave
S-0-1040	Drive address of master communication	1

Fig. 8-28: Excerpt of parameter verification

The actual verification is carried out as follows:

- The parameter verification tool displays the parameter setting active in the drive. It is first necessary to check whether this parameter setting matches the planned/configured parameters for this axis.
- Then check whether transmission errors occurred during the transmission to the drive. For this purpose, compare each parameter listed in the safety technology report to the corresponding parameter in the parameter verification tool. The values should be the same, except for possible rounding inaccuracies.

☞ When user-defined scalings for position, velocity, acceleration and torque or force are used, the following parameterizations are **not allowed**:

- Scaling factors unequal 1
- Rotational position resolution unequal 360*10^n (n=1, 2, 3…)

☞ The following rounding inaccuracies can occur during the transmission to the drive and can be tolerated:

- Velocity parameters: <1 rpm
- Position parameters: Deviations with an absolute value smaller than 2 digits (the last two digits of the value)
- Acceleration parameters: <1 rad/s^2

- In the parameter verification tool, all safety technology parameters available in the drive are displayed with their current values. However, it is only necessary to check the effective safety technology parameters listed in the safety technology report. To simplify the verification, all bit-coded parameters (such as P-0-3210) are also listed in HEX-coded form. The HEX-coded display is contained in the safety technology report in brackets after the bit-coded display. In the parameter verification tool, the corresponding parameters are listed in HEX-coded form at the end of the tool.

  If greater differences than the ones mentioned above occur when the parameters are compared (between safety technology report and parameter verification tool), proceed as follows:

  – Compare the parameters P-0-3201 "Change counter of safety technology memory" in the safety technology report and the parameter verification tool. If different counts are displayed in the parameters, generate the safety technology report again (close window and open it again), restart the parameter verification tool and carry out the verification again.

    If the counts are the same, check this:

  – Check the safety technology parameterization via the parameter editor or the parameter group and, if necessary, correct the corresponding parameter via the safety technology wizard. Afterwards, generate the safety technology report again, restart the parameter verification tool and carry out the parameter verification again.

    If different parameter values continue to occur, please do this:

  – Reboot the drive (switch control voltage off and on again) and carry out the parameter verification again.

    If different parameter values continue to occur, please do this:

– Check whether there is a more recent release of the drive firmware and IndraWorks version used and, if necessary, carry out an update. Afterwards, carry out the parameter verification again.

– If the above-mentioned remedies do not solve the problem, please contact our service department.

Step 9: Completing commissioning

Testing the safety functions

To complete the commissioning, the new parameters of the safety functions can be tested. To do this, select the safety functions one after the other and trigger the monitoring functions by means of command value input.

⚠ CAUTION **Loss of safety-relevant settings when replacing the control section!**

⇒ Save the safety technology parameters on an external storage medium ("S-0-0192, IDN-list of all backup operation data") to transfer all safety-relevant settings to the new control section in case the control section is replaced.

☞ A binary image of the safety technology data for channel 2 is contained in the parameter "P-0-3208, Backup of safety techn. data channel 2".

Acceptance test of the safety function

Change status: Every change of the safety technology memory can be assigned to an unequivocal change status which has to be documented within the scope of the safety acceptance test. The change status is stored in the following parameters:

- P-0-3201, Change counter of safety technology memory
- P-0-3202, Operating hours at last change of memory

Change history: In case you are obliged to produce supporting documents, the last states of the safety technology memory can be reproduced with the parameter "P-0-3203, Memory image of safety technology memory" using an external program.

☞ After safety technology has been commissioned, it is necessary to make a safety acceptance test (test protocol) in which the count of the change counter (P-0-3201) and the required acceptance tests are documented.

Step 10: Acceptance test

Acceptance procedure

When the machine is commissioned and in the case of any **software or hardware changes relevant to functional safety** (e.g., version upgrade of the firmware), an **acceptance test** has to be carried out by authorized staff. In case safety-relevant data are **partially changed**, they also have to be checked by means of an acceptance test.

☞ In either case, the changes and tests carried out have to be recorded.

☞ For commissioning the safety technology, you should always use the current release of the corresponding firmware version and of the IndraWorks commissioning software.

Otherwise, take the corresponding manufacturer information on detected and solved problems into account and verify their relevance for the machine application.

For information on the current release and the manufacturer information, please refer to the "eBusiness Portal" under http://www.boschrexroth.com/portal.

- It is not necessary to check all parameterized monitoring thresholds and safety functions for their effectiveness, but only one exemplary threshold or function at a time.
- The error reaction becomes physically effective.
- The correct functioning of the safety function has to be checked. To do this, it is necessary to deactivate, in the higher-level control unit, the command value limitations in the special mode for the duration of the acceptance test.

☞ The required tests for the complete safety technology acceptance test can be conducted using the instructions for the safety technology acceptance test.

Instructions for the safety technology acceptance test

Completed commissioning and successful parameter verification are the prerequisites for the subsequent acceptance test.

Each test has to be conducted for each individual axis/spindle/roll drive. Within the scope of the acceptance test, it is not necessary to check each parameterized monitoring threshold and safety function for their effectiveness, but only one exemplary threshold or function at a time. Therefore, the acceptance test is divided into the following parts:

- Checking the active scaling settings
- Checking the safety technology state machine with selection and acknowledgment
- Checking the error reaction
- Checking the additional and auxiliary functions (e.g., "Safe homing procedure")

Checking the active scaling settings

Within the scope of the acceptance test, it is necessary to check that absolute position data, relative position data, velocity, acceleration and torque data are correctly scaled in the drive. Only in this way is it possible to ensure that the parameterized monitoring thresholds take effect. For this purpose, an active limit (absolute/relative position, velocity, acceleration, torque) has to be checked for each scaling type. Proceed as follows:

- **Absolute position scaling** is used in the following parameters and corresponding safety functions:
  - P-0-3235, Safely-limited position, positive
  - P-0-3236, Safely-limited position, negative
  - P-0-3241, Safely-monitored position 1, positive
  - P-0-3242, Safely-monitored position 1, negative

  - P-0-3251, Safely-monitored position 2, positive
  - P-0-3252, Safely-monitored position 2, negative

  Depending on the axis parameterization, one or several of the above-listed parameters are active. If none of the above parameters is used in the axis, it is not necessary to check the absolute position scaling.

  To check the absolute position scaling, it is necessary to move to an active absolute position and check it. The check consists in finding out whether the drive reacts with the corresponding error message when the absolute position is passed. Example: When P-0-3241 is checked, the error F7011 is generated.

- **Relative position scaling** is used in the following parameters and corresponding safety functions:
  - P-0-3230, Monitoring window for safe stop 2
  - P-0-3232, Standstill window for safe direction
  - P-0-3243, Safely-limited increment 1
  - P-0-3253, Safely-limited increment 2
  - P-0-3263, Safely-limited increment 3
  - P-0-3273, Safely-limited increment 4
  - P-0-3310, SBS: Travel range brake check

  Depending on the axis parameterization, one or several of the above-listed parameters are active. If none of the above parameters is used in the axis, it is not necessary to check the relative position scaling.

  To check the relative position scaling, it is necessary to move to an active relative position and check it. The check consists in finding out whether the drive reacts with the corresponding error message when the relative position is passed. Example: When P-0-3243 is checked, the error F7010 is generated.

☞ If several active parameters of the relative position are available, the parameter with the highest possible parameter value should be used for the acceptance test. When checking such a parameter (e.g., P-0-3243), it is easier to detect incorrect scaling than with a low monitoring threshold (e.g., P-0-3230), because in this case scaling errors might possibly only show in one of the last decimal places.

- **Velocity scaling** is used in the following parameters and corresponding safety functions:
  - P-0-3233, Velocity threshold for safe standstill
  - P-0-3234, Safe maximum speed
  - P-0-3244, Safely-limited speed 1
  - P-0-3254, Safely-limited speed 2
  - P-0-3264, Safely-limited speed 3
  - P-0-3274, Safely-limited speed 4

  Depending on the axis parameterization, one or several of the above-listed parameters are active. If none of the above parameters is used in the axis, it is not necessary to check the velocity scaling.

To check the velocity scaling, it is necessary to move to an active velocity threshold and check it. The check consists in finding out whether the drive reacts with the corresponding error message when the velocity threshold is passed. Example: When P-0-3244 is checked, the error F7013 is generated.

- **Acceleration scaling** is used in the following parameter and the corresponding safety function:
  - P-0-3282, Safely-monitored deceleration

  With safety technology active, this parameter is always active. To check the acceleration scaling, it is necessary to move to an active acceleration threshold and check it. The check consists in finding out whether the drive reacts with the corresponding error message when the acceleration threshold is passed. Example: When the deceleration value is too low at the selection of the special mode, the error F7051 or F8135 must be generated.

- **Torque scaling** is used in the following parameter and the corresponding safety function:
  - P-0-3303, SBS: Nominal load

  This parameter is active when the safe braking and holding system is used. If the safe braking and holding system is not used in the axis, it is not necessary to check the torque scaling.

  To check the torque scaling, the following tests have to be carried out:
  - Check of permanent load monitoring:

    For this test, load the axis in normal operation with 100% to 130% of the value entered in "P-0-3303, Nominal load" When the axis is put in control in doing so, the warning E3116 must be generated.
  - Check of torque scaling during brake check: For this purpose, reduce the value of P-0-0547 by 15%. Then start the brake check (C2100). With error-free torque scaling, the brake check must be aborted with the error C2103. To complete this test item, reset P-0-0547 to its original value.

When all scalings relevant to the active safety technology parameterization have been successfully checked, proceed to the next item of the acceptance test. However, if a scaling test is negative, the acceptance test must not be continued. The cause of the scaling error first has to be removed. Afterwards, carry out the complete acceptance test again.

Checking the safety technology state machine with selection and acknowledgment

Upon successful scaling test, check the safety technology state machine of selection and acknowledgment relevant to this axis.

To check the selection, select all configured safety technology operating states once and check whether the axis acknowledges them. The selection acknowledgment can be checked by reading the operating state at the display or by reading the parameter P-0-3213.

The following safety technology operating states can have been parameterized, and the drive acknowledges them as follows:

Safety technology - Operating status	Display	S-0-0390	P-0-3213, bit 6...0
Normal operation	bb or Ab or AF	Depending on the active operation mode	0000001
Safe stop 1 (Emergency stop)	SS1ES	A0014 Safe stop 1 (Emergency stop) active	0000010
Safe standstill: Safe stop 1	SS1	A0015 Safe stop 1 active	0000100
Safe standstill: Safe stop 2	SS2	A0016 Safe stop 2 active	
Safe motion 1	Impossible to check via display, because "SMM" is displayed for each safe motion.	A0018 Special mode safe motion 1	0001000
Safe motion 2		A0019 Special mode safe motion 2	0010000
Safe motion 3		A0020 Special mode safe motion 3	0100000
Safe motion 4		A0021 Special mode safe motion 4	1000000

Afterwards, check whether the parameterized safe feedback takes effect when a special mode is selected. The check of the safe feedback depends on the parameterized safe feedback. The table below shows the possible types of safe feedback and the checks.

☞ If the safe feedback is not used or evaluated at the axis, this must be taken into consideration in the risk analysis of the installation. In this case, the test of the safe feedback described below does not have to be carried out.

Slave axes in a safety zone acknowledge their safety via I/O20 to the zone master. The test described below has to be conducted at these axes.

Safe feedback	Check of safe feedback
To master (slave axis)	• Check whether the axis acknowledges the selected special mode without error • Carry out check of zone safety during acceptance test of safety zone master
For control safety door	• Select a special mode, except for "Safe stop 1 (Emergency stop)" • Check whether all axes of the safety zone change to the special mode without error • Check the operability of the door locking device (safety door enabled in special mode and safety door locked in normal operation)
Single-axis acknowledgment (drive in stand-alone form)	• Check whether the axis acknowledges the selected special mode without error • Check whether the axis gives error-free feedback of the special mode or normal operation to the PLC for the safety zone
For control PLC, option. safety techn. module is master	• Select a special mode • Check whether all axes of the safety zone change to the special mode without error • Check whether the axis gives error-free feedback of the special mode or normal operation to the PLC for the safety zone

When the selection and acknowledgment of safety technology have been successfully checked, proceed to the next item of the acceptance test. If a selection or acknowledgment test is negative, however, the acceptance test must not be continued. The cause of the selection or acknowledgment error first has to be removed. Afterwards, carry out the complete acceptance test again.

Checking the error reaction

Upon the successful check of the safety technology state machine, the error reaction of the axis then has to be checked. When doing this, check whether the axis is able to stop the load at least with the parameterized deceleration P-0-3282 at selection (or in the case of error). This check has to be run for the "worst case" (e.g., maximum load and maximum velocity). That is to say, it is necessary to check whether the axis can be shut down without error even in the most disadvantageous but still allowed operating states.

When the safely-monitored position or the safely-limited position is used, additionally check that the available residual paths are sufficient when this position is passed (in the "worst case").

When the error reaction has been successfully checked, proceed to the next item of the acceptance test. If the error reaction check is negative, however, the acceptance test must not be continued. The cause of the error first has to be removed. Afterwards, carry out the complete acceptance test again.

Checking the additional and auxiliary functions

Upon the successful check of the error reaction, parameterized additional and auxiliary functions have to be checked. The following additional and auxiliary functions can be active in the axis:

- Safe homing procedure
- Safe parking axis
- Safe brake check

☞ Only the additional and auxiliary functions actually used in the axis have to be checked.

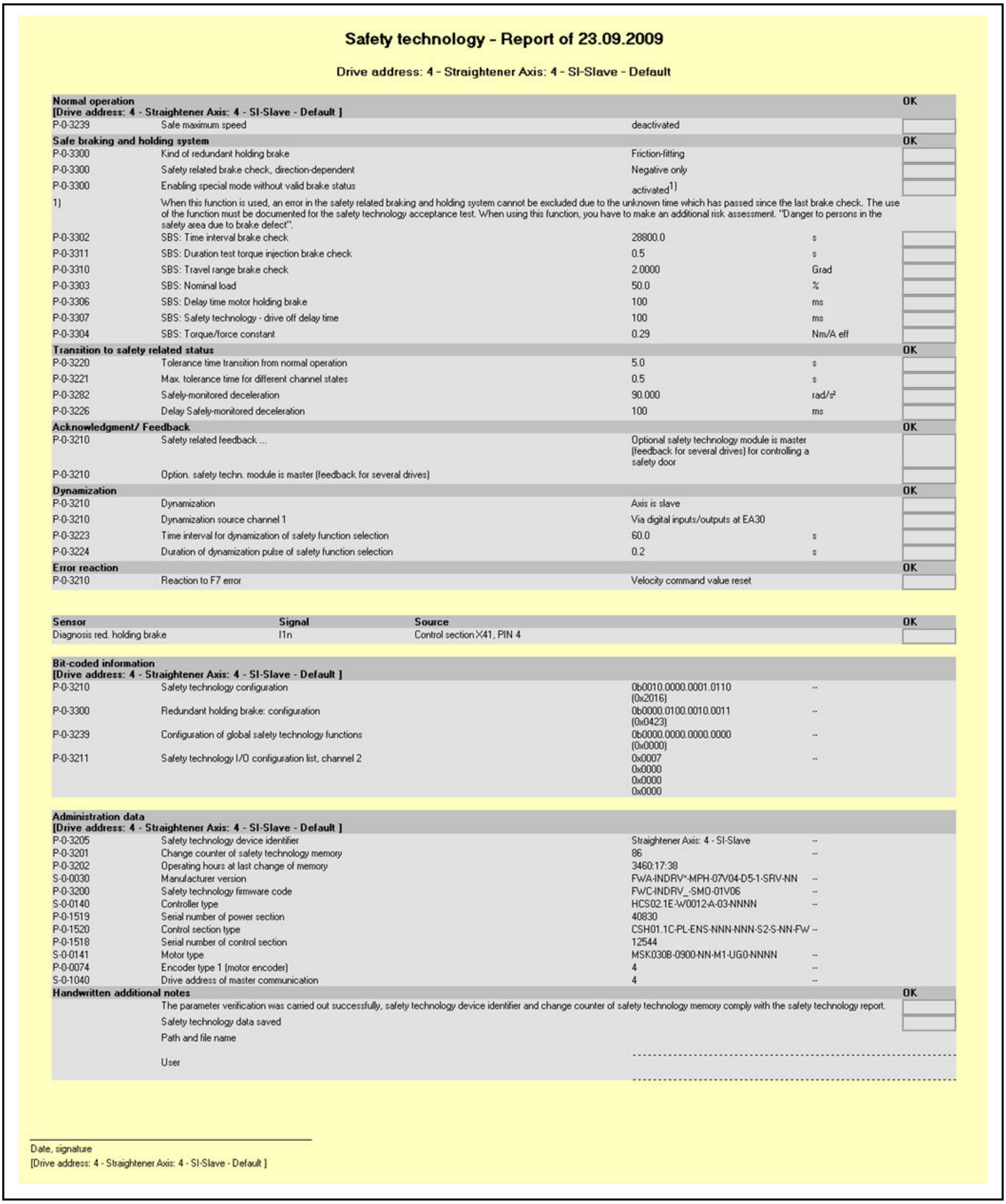
To check the additional and auxiliary functions, conduct the following tests:

- **Safe homing procedure:** When the safely-monitored position or the safely-limited position has been parameterized in the axis, the axis must be safely homed. For the acceptance test, start the safe homing procedure from different starting points. Every time this is done, the axis must home without error.
- **Safe parking axis:** When this auxiliary safety function has been parameterized, check whether it is possible to select the function without error.
- **Safe brake check:** When the safe braking and holding system is used, the auxiliary function "Safe brake check" is required to check both brakes. During the acceptance test, the following aspects have to be checked:
  - Is it possible to carry out the safe brake check at all positions, at which later on in operation the safe brake check is to be carried out, with the maximum load of the axis?
  - If there are several axes with safe braking and holding system in the installation and if the brake check is normally started simultaneously at these axes, the brake check for each axis must be triggered separately and successively during the acceptance test. This

is done to ensure that there are no wiring errors in the brake control between the axes.

Upon the successful test of the additional and auxiliary functions, the acceptance test for this axis is completed. The safety technology report with which the acceptance test was carried out must be signed and added to the machine documentation.

It is possible to generate a print-out of the safety technology report with the currently effective safety functions and corresponding values in the "Safety technology/Diagnosis" window (see example below).



Safety technology - Report of 23.09.2009

Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default

Normal operation [Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]				**OK**
P-0-3239	Safe maximum speed	deactivated		□
Safe braking and holding system				**OK**
P-0-3300	Kind of redundant holding brake	Friction-fitting		□
P-0-3300	Safety related brake check, direction-dependent	Negative only		□
P-0-3300	Enabling special mode without valid brake status	activated[1]		□
1)	When this function is used, an error in the safety related braking and holding system cannot be excluded due to the unknown time which has passed since the last brake check. The use of the function must be documented for the safety technology acceptance test. When using this function, you have to make an additional risk assessment. "Danger to persons in the safety area due to brake defect".			
P-0-3302	SBS: Time interval brake check	28800.0	s	□
P-0-3311	SBS: Duration test torque injection brake check	0.5	s	□
P-0-3310	SBS: Travel range brake check	2.0000	Grad	□
P-0-3303	SBS: Nominal load	50.0	%	□
P-0-3306	SBS: Delay time motor holding brake	100	ms	□
P-0-3307	SBS: Safety technology - drive off delay time	100	ms	□
P-0-3304	SBS: Torque/force constant	0.29	Nm/A eff	□
Transition to safety related status				**OK**
P-0-3220	Tolerance time transition from normal operation	5.0	s	□
P-0-3221	Max. tolerance time for different channel states	0.5	s	□
P-0-3282	Safely-monitored deceleration	90.000	rad/s²	□
P-0-3226	Delay Safely-monitored deceleration	100	ms	□
Acknowledgment/ Feedback				**OK**
P-0-3210	Safety related feedback ...	Optional safety technology module is master (feedback for several drives) for controlling a safety door		□
P-0-3210	Option. safety techn. module is master (feedback for several drives)			□
Dynamization				**OK**
P-0-3210	Dynamization	Axis is slave		□
P-0-3210	Dynamization source channel 1	Via digital inputs/outputs at EA30		□
P-0-3223	Time interval for dynamization of safety function selection	60.0	s	□
P-0-3224	Duration of dynamization pulse of safety function selection	0.2	s	□
Error reaction				**OK**
P-0-3210	Reaction to F7 error	Velocity command value reset		□

Sensor	**Signal**	**Source**	**OK**
Diagnosis red. holding brake	I1n	Control section X41, PIN 4	□

Bit-coded information [Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]			
P-0-3210	Safety technology configuration	0b0010.0000.0001.0110 (0x2016)	--
P-0-3300	Redundant holding brake: configuration	0b0000.0100.0010.0011 (0x0423)	--
P-0-3239	Configuration of global safety technology functions	0b0000.0000.0000.0000 (0x0000)	--
P-0-3211	Safety technology I/O configuration list, channel 2	0x0007 0x0000 0x0000 0x0000	--

Administration data [Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]				
P-0-3205	Safety technology device identifier	Straightener Axis: 4 - SI-Slave	--	
P-0-3201	Change counter of safety technology memory	86	--	
P-0-3202	Operating hours at last change of memory	3460:17:38		
S-0-0030	Manufacturer version	FWA-INDRV*-MPH-07V04-D5-1-SRV-NN	--	
P-0-3200	Safety technology firmware code	FWC-INDRV_-SMO-01V06	--	
S-0-0140	Controller type	HCS02.1E-W0012-A-03-NNNN	--	
P-0-1519	Serial number of power section	40830		
P-0-1520	Control section type	CSH01.1C-PL-ENS-NNN-NNN-S2-S-NN-FW	--	
P-0-1518	Serial number of control section	12544		
S-0-0141	Motor type	MSK030B-0900-NN-M1-UG0-NNNN	--	
P-0-0074	Encoder type 1 (motor encoder)	4	--	
S-0-1040	Drive address of master communication	4	--	
Handwritten additional notes				**OK**
	The parameter verification was carried out successfully, safety technology device identifier and change counter of safety technology memory comply with the safety technology report.			□
	Safety technology data saved			□
	Path and file name	------------------------------		
	User	------------------------------		

Date, signature
[Drive address: 4 - Straightener Axis: 4 - SI-Slave - Default]

Fig. 8-29: Example of a safety technology report

8.5 Mounting and Installing the Safe Braking and Holding System

8.5.1 Connection Diagram

Connect the control module (HAT) according to the following description.

1. The control voltage supply
   - of the power section,
   - of the assigned drive controller and
   - the control voltage supply of the control module at terminal connector X1

   should be connected to a common voltage source.
2. The control voltage supply
   - of the standard I/Os, terminal connector X31
   - the optional safety technology module (S2), terminal connector X41
   - the interface supply of the control module, terminal connector X3

   comes from a common control voltage supply. This can be the control voltage supply of the power section.

   The power supply of these three interfaces is isolated from the power supply mentioned under item 1.
3. The power supply of the optional safety technology module (Safe Motion) takes place via the connection cable RKS007 at terminal connector X3 of the control module.
4. The control module is controlled via a dynamized signal output at the standard I/O (X3/3).
5. The dynamized feedback signal of the control module is applied at the input (X3/4) of the optional safety technology module (S2).
6. The redundant holding brake is connected at terminal connector X2 of the control module.

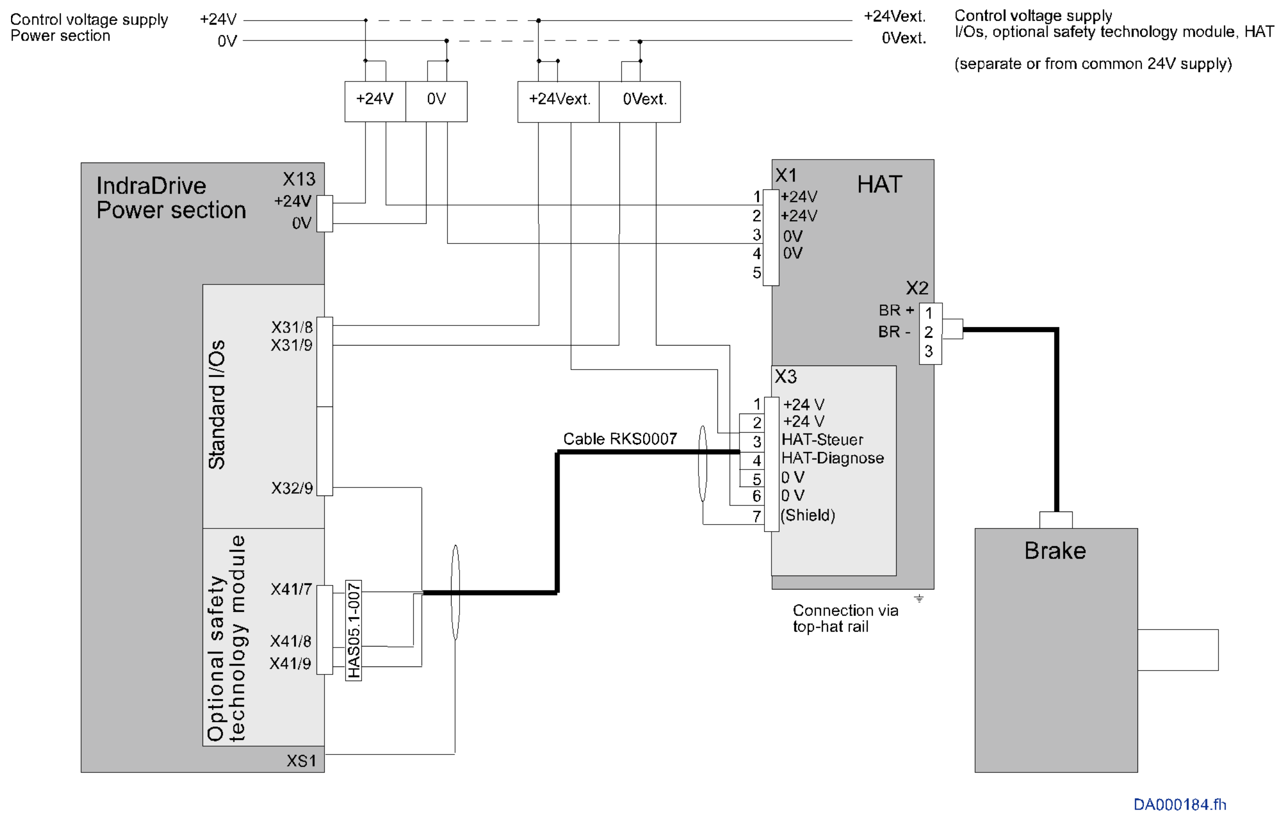


Fig. 8-30: Connection Diagram of the "Safe Braking and Holding System" at Single-Axis Drive Controllers

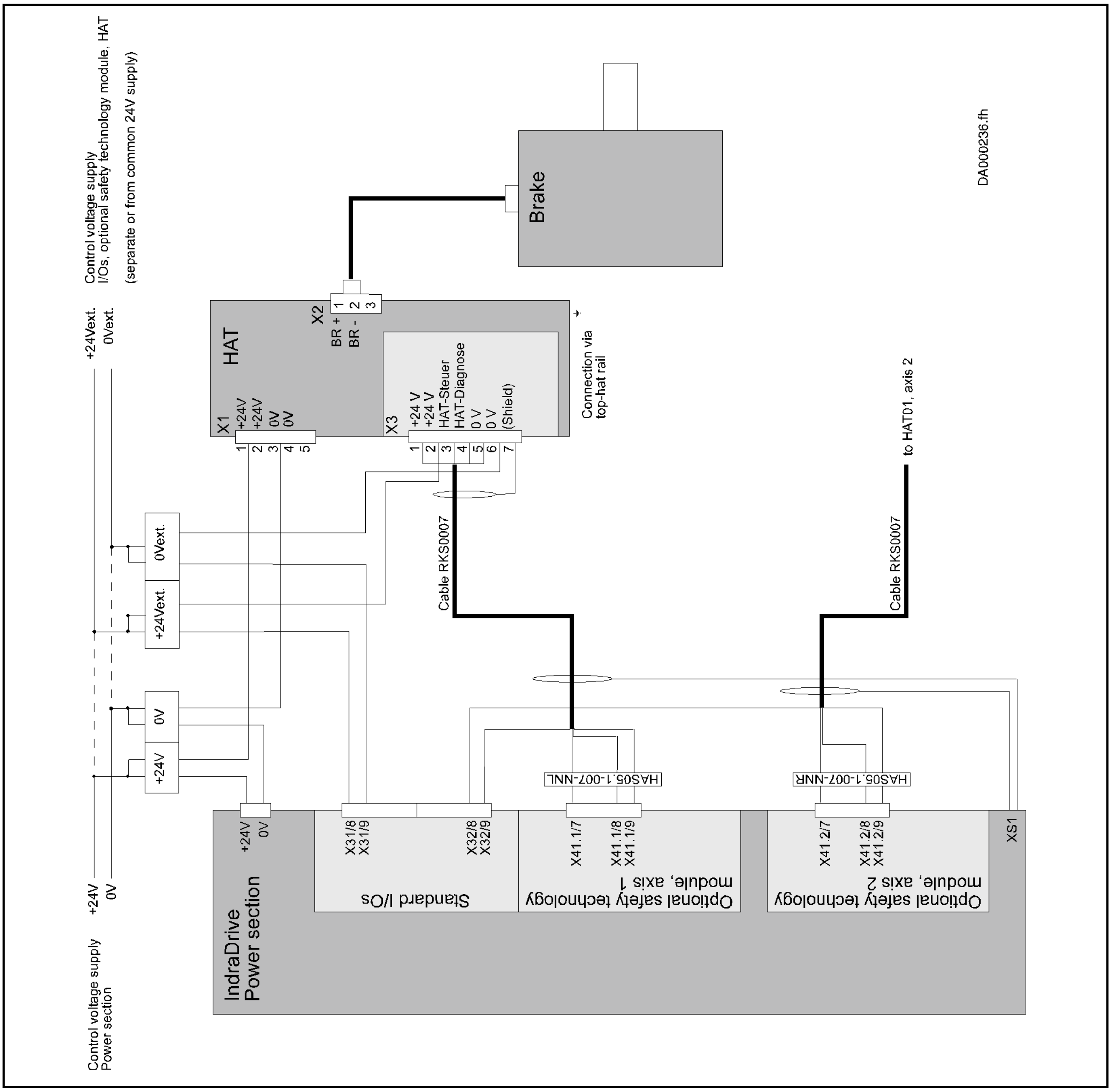


Fig. 8-31: Connection Diagram of the "Safe Braking and Holding System" at Double-Axis Drive Controllers

8.5.2 Control Module

The control module **HAT01.1-002-NNN-NN** is required for controlling the redundant holding brake. It is provided for top-hat rail mounting in the control cabinet.

8.5.3 Connection

Connecting the Control Module to the Drive Controller

Use the connection cable RKS0007 to connect the control module **HAT01.1-002-NNN-NN** to the IndraDrive controller. You can order the cable in the required length. Do not exceed the allowed maximum length of 5 m.

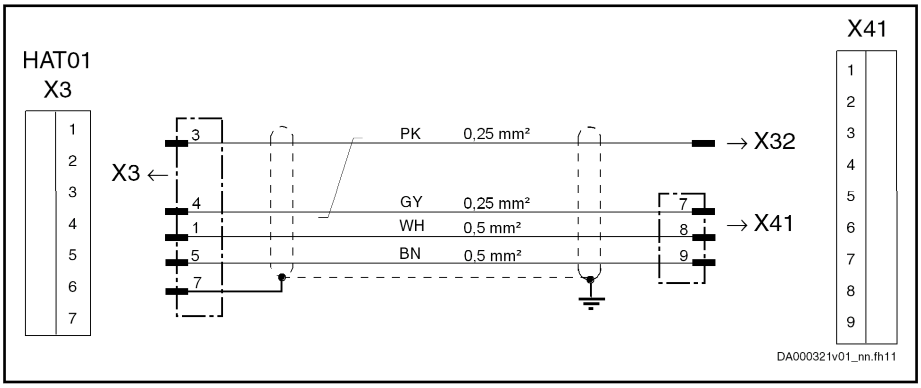


Fig. 8-32: Connection Cable RKS0007

Connecting the Redundant Holding Brake to the Control Module

Connect the redundant holding brake to the control module. When doing this, observe the specifications of the brake supplier. Establish a possible existing shield connection of the connection cable near the control module, e.g. top-hat rail clamp with Wago 790-113 and 790-124.

8.5.4 Accessories

Adapter HAS05.1-007

Use the adapter HAS05.1-007 to connect HAT to the drive controller. The adapter allows applying other signal lines, for selecting the individual safety functions, at connector X41 in addition to the connection cable RKS0007.

The exact description of the adapter is part of this documentation (see index entry "HAS05.1-007").

8.6 Commissioning Series Machines

For commissioning series machines you can use a simplified procedure for axes with the optional safety technology module "Safe Motion". To do this, the following requirements must have been fulfilled:

- The wiring of the I/Os has not changed compared to the first series machine.
- The parameter setting is the same compared to the first series machine.

When these requirements have been fulfilled, series machines can be commissioned by means of the following simplified procedure without repeated safety technology acceptance test:

1. Check wiring of I/Os.

> ☞ Before safety technology is activated, the I/O wiring must have been checked.

2. Load parameter file to drive and activate safety technology (for how to proceed, see "Replacing the Controller").
3. Save safety technology parameters and add them to safety-relevant documentation of machine:
   - Open window "Safety Technology/Diagnosis".

     => Right side of window displays acceptance test protocol, left side displays current status of safety technology.
   - Open context menu on left side of window by clicking right mouse button.
   - Select "Export safety technology parameters" and save parameters.

4. Compile new protocol with contents listed below and add it to safety-relevant documentation of machine, together with copy of safety technology report of first series machine:
   - Commissioning of series machine carried out on basis of safety technology report "safety technology device identifier (P-0-3205) of first series machine" of (date of report)
   - Safety technology device identifier (P-0-3205) is at (value)
   - Change counter of safety technology memory (P-0-3201) is at (value)
   - Operating hours at last change of memory (P-0-3202) is at (value)
   - Serial number of control section (see type plate at device)
   - Serial number of power section (see type plate at device)
   - (Date), (name), (signature)

8.7 Requirements to the Control Unit

Safety Technology Option "Safe Torque Off"

Depending on the "Safety Integrity Level" (SIL) to be attained, there are the following requirements to the control unit for the safety technology option "Safe Torque Off":

- **SIL1/SIL2:** No specific requirements to the control unit as regards control, acknowledgment and test of the safety technology option "Safe Torque Off".
- **SIL3:** Control of the safety function "Safe torque off" and evaluation of the feedback **must be carried out by a safety technology master** (e.g., safety PLC) which complies with SIL3.

  In addition, the safety technology master must test the optional safety technology module cyclically. This test must take place at least once within 24 hours. (When guards are used, the test interval can be extended if a successful test was carried out directly before the safety area is enabled). The following tests must be carried out:
  - Selection of the STO function at the drive by the safety technology master
  - Query of the drive's acknowledgment of safety by the safety technology master
  - Deselection of the STO function at the drive by the safety technology master
  - Query of the drive's acknowledgment of normal operation by the safety technology master

☞ When setting up a safety zone of several drives with STO function, you must ensure that each drive can be individually tested and that the feedback can be evaluated. This can be ensured by the following measures:

- In the case of collective STO selection of the drives, the acknowledgments of each drive must be separately transmitted to the safety technology master and must be evaluated. The test can be carried out for all drives in parallel.
- In the case of collective acknowledgment of safety (series connection or parallel connection of the acknowledgment outputs), the selection of the drives must take place separately. Each drive must be tested individually, one after the other.

The collective STO selection and collective acknowledgment of safety (series connection or parallel connection of the acknowledgment outputs) is not allowed for SIL 3/PL e applications!

Safe Motion

For the safety technology option "Safe Motion", there are the following requirements to the control unit:

- The control unit must know the operation modes (normal operation / special mode), as well as their safety functions.
- It is the responsibility of the control unit that the drive is interpolated within the given time within the limits given by the safety function.
- For this purpose, the control unit must be able to recognize the selection of a safety function so that it can react at any time to the switching to the safe operation (e.g., read "P-0-3215, Selected safety technology operating status" from the drive). For online monitoring of the safety technology states, the binary status signals provided by "P-0-3213, Safety technology operating status" can be read by the control unit.
- The transition to "Safe stop 1", "Safe stop 1 (NOT-HALT)" and "Safe stop 2" can alternatively be controlled by the drive or the control unit (parameterized via "P-0-3210, Safety technology configuration").
  - In the case of transition, controlled by the control unit, to the safety technology operating states "Safe stop 1 (Emergency stop)" and special mode "safe standstill" with the safety function "Safe stop 1", the control unit has to remove drive enable.
  - In the case of transitions controlled by the drive, the drive removes drive enable.
- The transition to safe standstill in the case of error takes place according to the settings in the parameters "P-0-0117, Activation of NC reaction on error" and "P-0-0119, Best possible deceleration".

☞ The control unit must react to the selection of a safety function with the corresponding command value input!

9 Acceptance Test

See "Commissioning the Optional Safety Technology Module "Safe Motion" (S2)", "Step 10: Acceptance test" on page 240.

10 Error Messages and Error Elimination

10.1 Firmware Code

The parameter "P-0-3200, Safety technology firmware code" contains the designation of the safety technology firmware version.

10.2 Errors

The error handling of safety technology is covered by the error handling of the standard drive.

In the case of error, the drive is decelerated in the best possible or quickest possible way and then goes to safety related standstill.

☞ In the case of a feedback error (encoder error), the safety technology can no longer guarantee dual-channel safety. It is then impossible, for example, to detect a coasting spindle. In this case, the safety door may only be unlocked manually after an additional visual check by the operators. The door has to be unlocked at the drive that signals the encoder error. This drive then acknowledges safety and the master can open the safety door.

The parameter "P-0-3218, C3700 Manually unlocking the safety door" allows manually unlocking the safety door in the case of a feedback error.

☞ For causes of errors and troubleshooting, please see the documentation "Troubleshooting Guide".

10.3 Errors in Operation Mode "Normal Operation"

☞ Detection of errors in **inactive safety functions** causes a warning in normal operation. In **active safety functions**, detection of an error causes an error of category F31xx or F7xxx.

For causes of errors and troubleshooting, please see the documentation "Troubleshooting Guide".

10.4 Status Messages

The parameter "P-0-3213, Safety technology operating status" makes available binary status signals for online monitoring of the safety technology states. By means of this status word, the individual status signals can be optionally programmed to existing real-time bits of the master communication or hardware I/Os or I/O extensions.

The parameter "P-0-3215, Selected safety technology operating status" makes available the selected safety technology mode of the individual monitoring channels in coded form.

The parameter "P-0-3216, Active safety technology signals" shows the current states of the safety technology signals of the individual channels.

The parameter "P-0-3217, I/O status channel 2 (optional safety technology module)" shows the current states of the inputs/outputs of the optional safety technology module.

11 Troubleshooting information

11.1 Introduction

For the purpose of diagnosis (messages of error, warning, operating status) and service (firmware and hardware replacement), it is necessary that you make yourself familiar, by means of the Functional Description of the firmware, with some functions/elements:

- MultiMediaCard,
- Control panel (standard and comfort version) and
- Parameter handling

The paragraphs below above all explain the points relevant to integrated safety technology in detailed form.

The paragraphs are divided into:

- Overview of diagnostic system (e.g. logbook parameters and parameters containing information on the hardware configuration) ("Diagnostic System")
- Diagnostic messages which can be read from the display of the control panel ("Diagnostic Messages of Integrated Safety Technology")
- Diagnostic possibilities specifically extended for integrated safety technology ("Extended Diagnostic Possibilities")

11.2 Diagnostic system

11.2.1 General Information

The general diagnostic system of IndraDrive is explained in detail in the Functional Description of the firmware where you can read more about it, if required (see also index entry "Diagnostic system").

In this chapter we only list the parameters which are used in conjunction with the diagnostic system:

- S-0-0095, Diagnostic message
- S-0-0375, List of diagnostic numbers
- S-0-0390, Diagnostic message number
- P-0-0009, Error number
- P-0-0478, Logbook event
- P-0-0479, Logbook time stamp
- P-0-3219, Extended safety technology diagnosis

☞ For integrated safety technology, an extended diagnostic function is provided in the form of a safety technology error code (cf. "P-0-3219, Extended safety technology diagnosis" which should be read in the case of error. The error code supports quick and easy error diagnosis (see also index entry "Extended diagnostic possibilities").

Axis or Device Configuration

A drive controller consists of several components (power section, control section, firmware,...); each of them has its own identifier in the form of a parameter (see also Functional Description of firmware "Device Configuration").

Identifiers useful for the purpose of diagnosis and service are stored in the following parameters:

- S-0-0140, Controller type
- S-0-0141, Motor type
- S-0-0142, Application type
- P-0-1518, Module code of control section
- P-0-1519, Module code of power section
- P-0-1520, Control section type
- S-0-0030, Manufacturer version
- P-0-3200, Safety technology firmware code

"P-0-3200, Safety technology firmware code" contains the designation of the safety technology firmware version which is required for operating the optional safety technology module "S2"!

11.2.2 Diagnostic Messages of Integrated Safety Technology

Overview

We distinguish the following operating states of integrated safety technology:

- In **normal operation**, the triggering of a monitoring function in **inactive safety functions** causes a warning of category E31xx. In **active safety functions**, detection of an error causes an error of category F31xx or F7xxx.
- In **special mode**, the triggering of a monitoring function causes an error of category F3xxx or F7xxx.

Apart from the error and warning messages, the operating states of integrated safety technology are displayed in individual parameters (status messages).

Safety Technology Errors (F7xxx, F3xxx)

General Information

Errors in the integrated safety technology (F3xxx, F7xxx) are basically handled like "normal" drive errors (F2xxx, F4xxx,...).

But as regards the error reaction and above all the required measures for eliminating an error, specific measures are required for integrated safety technology.

For the respective causes of errors and troubleshooting, please see the documentation Troubleshooting Guide.

Behavior in Case of Safety Technology Errors

NC-controlled stopping is not possible in case of safety technology errors (F7xxx) ("P-0-0117, Activation of control unit reaction on error" is ineffective).

The behavior of the drive (error reaction) in case of safety technology errors was extended and can be set as of firmware MPx03V20.

Up to MPx-03V18

Up to the firmware MPx-03V18, the drive is shut down as quickly as possible in case of safety technology errors (F7xxx), i.e., independently of the settings in "P-0-0119, Best possible deceleration"; the drive is brought to a standstill by a velocity command value reset (see also MPx02 and MPx03 Functional Descriptions, index entry "Error reaction").

As of Firmware MPx-03V20

As of firmware MPx-03V20, the error reaction in case of safety technology errors (F7xxx) can be parameterized via the configuration bit "reaction to F7 error" in "P-0-3210, Safety technology configuration"; the error reaction "velocity command value reset" is activated by default but can be deactivated so that the drive immediately goes torque-free when an F7 error occurs.

☞ The F7 error reaction "torque disable" should only be used when forced deceleration by a velocity command value reset generally causes problems, e.g. in case of mechanically coupled axes.

The machine manufacturer is responsible for the F7 error reaction "torque disable" and his risk analysis has to show this responsibility.

As of Firmware MPx-05

As of firmware MPx-05, "P-0-3210, Safety technology configuration" and "P-0-0119, Best possible deceleration" can be used to configure the error reaction "Velocity command value reset while maintaining the emergency halt deceleration (S-0-0429)".

At the end of each F7 error reaction, the drive goes torque-free and the output stage is locked via two channels after the time entered in "P-0-3220, Tolerance time transition from normal operation" or "P-0-3225, Tolerance time transition from safe operation" is over.

Commissioning Steps

After a safety technology error (F7xxx) has occurred, the drive can only be put into operation again when:

1. The actual cause of the error was recognized and removed (e.g. incorrect parameterization of velocity thresholds or time windows).

💡 When using the optional module "safety technology I/O" (S1) (up to MPx06) or "Safe Motion" (S2) (as of MPx07), you can, in addition to the error message, obtain detailed information with regard to the cause of the error or the error location. For this purpose, evaluate parameter "P-0-3219, Diagnostic safety technology message".

Up to MPx06: See "Extended Diagnosis (P-0-3219)".

As of MPx07: See "Extended Diagnosis (P-0-3219) as of MPx07".

2. The error message was cleared by the error clearing command (cf. "S-0-0099, C0500 Reset class 1 diagnostics").
3. The drive is in the operating mode again and power was switched on again ("Ab").
4. Drive enable was switched on again (0-1 edge).

☞ In case safety technology errors are occurring repeatedly, contact our service department as operating the drive then is no longer allowed.

Special Case: Encoder Error

In the case of an encoder error, the integrated safety technology can no longer guarantee dual-channel safety; a coasting spindle, for example, cannot be recognized. In this case, the safety door may only be unlocked manually after an additional visual check by the operators. The door has to be unlocked at the drive that signals the encoder error. This drive then acknowledges safety and the master can open the safety door.

☞ The parameter "P-0-3218, C3700 Manually unlocking the safety door" allows manually unlocking the safety door in the case of an encoder error.

Safety Technology Warnings in Operation Mode "Normal Operation"

Warnings in the integrated safety technology (E3xxx) are basically handled like "normal" drive warnings (E2xxx, E4xxx). However, you have to observe the following points:

- With activated safety technology, warnings of category E3xxx only occur in normal operation.
- When a safe operation is selected, the cause of the warning results in an error being triggered.

☞ For the respective causes of warnings and troubleshooting, please see the documentation "Troubleshooting Guide".

Status Information of Integrated Safety Technology

For the purpose of diagnosis, the following status information is made available for integrated safety technology:

- The parameter "P-0-3213, Safety technology operating status" makes available binary status signals for online monitoring of the safety technology states. By means of this status word, the individual status signals can be optionally programmed to existing real-time bits of the master communication or hardware I/Os or I/O extensions.
- The parameter "P-0-3215, Selected safety technology operating status" makes available the selected safety technology mode in coded form.
- The parameter "P-0-3216, Active safety technology signals" shows the current states of the safety technology signals of the individual channels.
- The parameter "P-0-3217, I/O status channel 2 (optional safety technology module)" shows the current states of the inputs/outputs of the optional safety technology module.

11.3 Extended Diagnostic Possibilities

11.3.1 General Information

Apart from the diagnostic standard functions, the drive system Rexroth IndraDrive with integrated safety technology provides extended diagnostic possibilities specifically implemented for integrated safety technology:

- Change Status of the Safety Technology Memory
- Tracing Back the Change History
- Extended Safety Technology Diagnosis

11.3.2 Change Status of the Safety Technology Memory

Every change of the safety technology memory can be assigned to an unequivocal change status.

Within the scope of the safety technology acceptance test, the change status has to be documented together with the password.

- The value of the parameter "P-0-3201, Change counter of safety technology memory" is incremented each time the safety technology memory is changed; this also applies to the command "S-0-0262, C07_x Load defaults procedure command".

- The value of the parameter "P-0-3202, Operating hours at last change of memory" indicates the point of time the safety technology memory was changed the last time. It is part of the safety technology memory.

11.3.3 Tracing Back the Change History

In case you are obliged to produce supporting documents, you can reproduce the last states of the safety technology memory by calling the content of the parameter "P-0-3203, Memory image of safety technology memory". The content of the parameter is a hexadecimal list. By means of an external program, it is possible to trace back the old states.

11.3.4 Extended Safety Technology Diagnosis

In conjunction with integrated safety technology, the parameter "P-0-3219, Extended safety technology diagnosis" was introduced to provide an extended possibility of diagnosis in case safety technology errors (F3xxx, F7xxx) or safety technology warnings (E3xxx) occur.

Extended Safety Technology Diagnosis in P-0-3219

An error or a warning which is generated by one of the two safety technology channels is processed by the error handling of the standard drive. In addition, an error code for the corresponding channel, which provides detailed error description, is entered in "P-0-3219, Extended safety technology diagnosis".

The procedure is as follows:

1. Read diagnostic message number in the case of error.
2. Read error code entered in "P-0-3219, Extended safety technology diagnosis".
3. Select corresponding list by means of diagnostic message number.
4. By means of error code, see cause and remedy of error.

☞ For a list of the error codes of "P-0-3219, Extended safety technology diagnosis" for MPx07, see the documentation "Diagnostic Messages" under the index entry "Extended diagnosis (P-0-3219) as of MPx07".

11.4 Replacing drive components

11.4.1 General information

☞ When replacing drive components, observe the safety instructions in the chapter "Safety instructions for electric drives and controls"!

11.4.2 Replacing the motor

⚠ WARNING **Lethal electric shock by live parts with more than 50 V!**

The supply unit may only be replaced by qualified personnel which have been trained to perform the work on or with electrical devices.

☞ The motor should be replaced by a motor of identical type. Only by doing this is it ensured that all parameter settings can remain unchanged; in addition, it is not required in this case to repeat the acceptance test within the scope of the function "Integrated safety technology".

1. If necessary, write down last absolute value
2. Open main switch
3. Make sure main switch cannot be switched on again
4. Disconnect plug-in connectors

☞ When replacing the motor, cover the open mating sites of power lines with protective caps if sprinkling with cooling liquid/lubricant or pollution may occur (allowed pollution degree according to EN50178: 2).

5. Replace motor

☞ To mechanically replace the AC servo motor, observe the instructions of the machine manufacturer.

6. Connect plug-in connectors
7. **WARNING!** Risk of accident caused by unwanted axis motion! Servo axes with indirect distance measuring system via the motor encoder will lose their position data reference when the motor is replaced!

   This position data reference to the machine coordinate system must therefore be reestablished after replacement.

11.4.3 Replacing the Optional Encoder

⚠ WARNING **Lethal electric shock by live parts with more than 50 V!**

The supply unit may only be replaced by qualified personnel which have been trained to perform the work on or with electrical devices.

☞ The encoder may only be replaced by an encoder of identical type. Only by doing this is it ensured that all parameter settings can remain unchanged; in addition, it is not required in this case to repeat the acceptance test within the scope of the integrated safety technology.

1. If necessary, write down last absolute value
2. Open main switch
3. Make sure main switch cannot be switched on again
4. Disconnect plug-in connectors

5.

☞ To mechanically replace the optional encoder, observe the mounting instructions of the encoder manufacturer.

If the optional encoder is used as safety technology encoder, it must be ensured that the replacement encoder complies with the requirements of safety technology! (See chapter "Required Motors and Measuring Systems".)

Replace encoder

6. Connect plug-in connectors
7. **WARNING!** Risk of accident caused by unwanted axis motion! Axes with absolute measuring system will loose the position data reference when the encoder is replaced!

   This position data reference to the machine coordinate system must therefore be reestablished after replacement.

11.4.4 Replacing the supply unit

☞ Replacing the supply unit might require a lifting device due to its size and weight.

⚠ WARNING **Lethal electric shock from live parts with more than 50 V!**

The replacement may only be carried out by qualified personnel which have been trained to perform the work at or with electric devices.

⚠ WARNING **Lethal electric shock by live parts with more than 50 V!**

Before working on live parts: De-energize installation and secure power switch against unintentional or unauthorized re-energization.

Wait at least **30 minutes** after switching off the supply voltages to allow **discharging.**

Check whether voltage has fallen below 50 V before touching live parts!

☞ Prior to the replacement, check by means of the type plates whether these devices are of the same types. Only replace devices of the same types.

Proceed as follows for the replacement:

1. De-energize installation and secure it against being switched on again by unauthorized staff or in an accidental way.
2. Using an appropriate measuring device, check whether installation has been de-energized. If necessary, wait for devices to discharge.
3. Make sure that motors have come to a safe standstill.
4. Secure vertical axes against motion.
5. Remove all electrical connections at defective device.
6. Release mounting screws and remove device from control cabinet (use lifting device, if necessary).

7. Mount replacement device in control cabinet (use lifting device, if necessary).
8. Connect replacement device according to connection diagram of machine manufacturer.
9. If you secured vertical axes mechanically before replacing the device, remove these securing devices at this point.
10. By reading error memories of connected drive controllers make sure that device defect has not been caused by drive controllers.

The replacement has been completed. The installation can be put into operation again.

☞ Within the scope of the "Integrated safety technology" function, it is not required to repeat the acceptance test.

11.4.5 Replacing the Controller

Overview

A controller of the IndraDrive range consists of the components power section and control section (incl. firmware). The control section can be configured with additional components (encoder interface, optional safety technology module,...). In the case of a defect, it is basically possible to replace one of the two components (control section or power section). As control section and power section are firmly connected and one of the two components may only be replaced by Rexroth service engineers or especially trained users, the paragraphs below describe how to replace the complete controller as regards safety technology. The mounting and dismounting of the entire drive controller is described in the Project Planning Manual for the power section.

☞ Only applies to Rexroth service engineers or especially trained users. The replacement of a defective power section does not require any specific handling due to integrated safety technology; i.e. it is not necessary to repeat safety technology commissioning and acceptance test.

When a controller is replaced for which the control section has been configured with the option "Safe Torque Off" (L2), this does not require any specific measures, i.e. the additional measures only apply to the use of option "Safe Motion" (S2)!

☞ No firmware version upgrade is to be undertaken when replacing the controller, as it is otherwise necessary to repeat the safety technology acceptance test!

When replacing a controller with activated safety technology, observe that **safety technology is not active** for **controllers in their condition as supplied**:

- The status of "P-0-3207, Safety technology password level" is zero and
- "INDRASAVE" has been inputted into "P-0-3206, Safety technology password".

☞ A controller supplied for replacement, which has already been operational, must be returned to its delivery state (see document "Integrated Safety Technology", keyword "Deactivating safety technology").

The figure below illustrates the basic individual steps required.

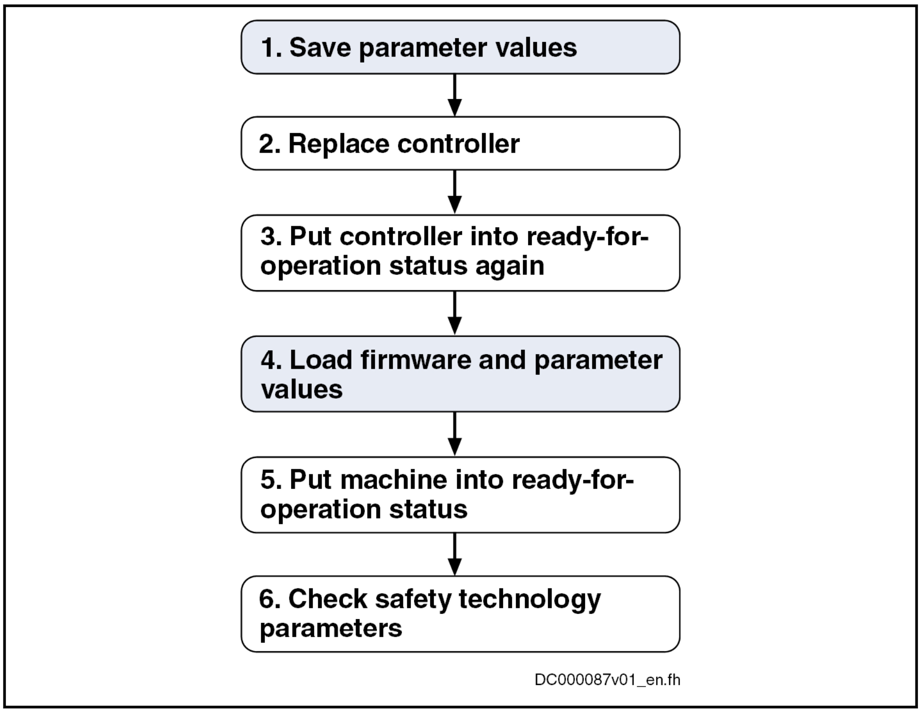

1. Save parameter values
2. Replace controller
3. Put controller into ready-for-operation status again
4. Load firmware and parameter values
5. Put machine into ready-for-operation status
6. Check safety technology parameters
DC000087v01_en.fh

Fig. 11-1: General sequence for controller replacement

Controller Replacement Without Stationarily Plugged-in MMC

1. Saving parameter values

   Before dismantling the defective device, save the drive parameter values, if possible.

   When the controller is to be replaced by means of the MMC, make sure before starting the replacement that the MMC folder "Firmware" contains the firmware required for the drive (e.g. FWA-INDRV*-MPH-07V02-D5.IBF).

☞ If backing up the parameter values before replacing the device is impossible due to a total breakdown of the device, only the parameter values backed up after initial commissioning can be loaded when the parameter values are loaded later on (see "Loading Parameter Values in Case of Total Breakdown of Device")!

1. Switch drive off and on again

2. Switch to Parameter mode (PM or P2)

Parameter values of the defective device are saved via the control panel with with the MMC temporarily plugged in ("hot plug").

☞ If the MMC does not remain stationarily (permanently) plugged in the device, it may be temporarily plugged into the switched-on device at the end of the booting phase and removed again ("hot plug" and "hot unplug" respectively).

3. Go to the Service menu.

⇒By simultaneously pressing "Esc" and "Enter" for at least 8 seconds, it is possible to call up extended displays; subsequently pressing the "Up" key (twice) activates the Service menu.

Select the "Device replace" submenu using the arrow keys and activate it with "Enter".

⇒The active parameter values [according to "S-0-0192, IDN list of backup operation data" and "P-0-0195, IDN list of retain data (replacement of devices)"] and the PLC retain data is copied from the controller-internal memory to an MMC temporarily plugged into the controller.

Activate "save Data?" command

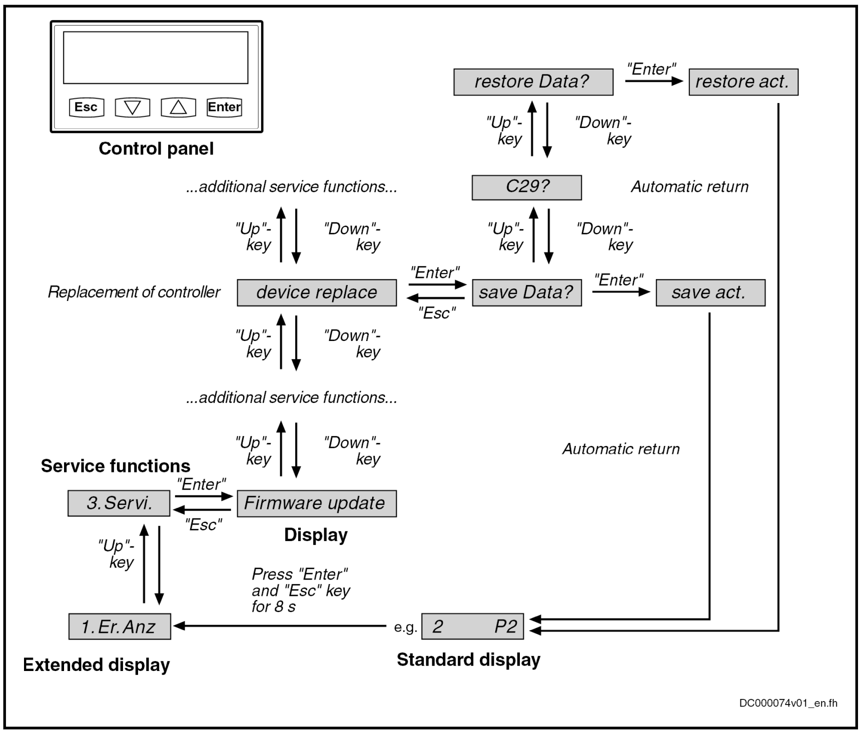


Fig. 11-2: Activating "save Data?" and "restore Data?" commands when replacing the controller using the control panel

2. Replace controller

   WARNING! Lethal electric shock by live parts with more than 50 V! Make sure drive controller is completely de-energized. Wait at least 30 minutes after switching off the supply voltages to allow discharging. To shorten the waiting time until voltage has fallen below 50 V, you can use a discharging device (see chapter "Appendix").

   1. Open main switch
   2. Make sure main switch cannot be switched on again
   3. Remove touch guard
   4. Check whether the voltage has dropped below 50 V before touching the live parts!
   5. Disconnect connecting lines from the drive controller
   6. Unscrew bolts on top and bottom of housing
   7. Take drive controller out of the drive system
   8. Fit new drive controller
   9. Connect new drive controller as specified in the machine circuit diagram
   10. Mount touch guard

3. Put controller into ready-for-operation status again

Put machine into ready-for-operation status again according to machine manufacturer's instructions.

4. **Load firmware and parameter values via MMC**

If firmware and drive parameters are to be transmitted via MMC to the replacement controller, ensure that the MMC folder "Firmware" contains the firmware required for the drive and the MMC folder "Parameters" contains the parameters backed up before replacing the device.

1. Disconnect replacement controller from the control voltage.

2. Put MMC into the replacement controller.

3. Supply device with control voltage again.

4. Depending on the "previous configuration" of the replacement device, the message "Firmware update?" can appear during the booting phase. Acknowledge this message by pressing "Enter" (on the control panel). By doing this, firmware is loaded from the plugged-in MMC into the controller.

☞ If the message "Firmware update?" does not appear, the firmware update must be started via the display.

"3. Service" → "Firmware update" → "FWA update"

5. Then one of the messages below might be displayed:

- "Load new param.?"
- "Load Par from MMC?"

⇒ Acknowledge this message by pressing "Enter" on the control panel. The drive parameters are now loaded from the MMC to the volatile memory of the device; the message "Load new safety?" may possibly appear.

⇒ Acknowledge this message by pressing "Enter" on the control panel. Safety technology parameters are now loaded from the MMC to the memory of the optional safety technology module.

6. Switch to Parameter mode (PM or P2).

The step below depends on the utilized firmware version:

7. Go to the Service menu.

⇒By simultaneously pressing "Esc" and "Enter" for at least 8 seconds, it is possible to call up extended displays; subsequently pressing the "Up" key (twice) activates the Service menu.

Select the "Device replace" submenu using the arrow keys and activate it with "Enter".

⇒Store PLC retain data and parameters from the MMC to the internal, non-volatile memory of the controller via the control panel by activating the command "Restore data?" (storing according to parameters "S-0-0192, IDN list of backup operation data" and "P-0-0195, IDN list of retain data (replacement of devices)". After parameter loading processes have been completed, the drive waits for further actions from the control master.

☞ If safety technology is to be activated in the replacement device (in accordance with the replaced device), the drive must be switched to operating mode (OM) or communication phase (P4) after loading the safety technology parameters before it is switched off!

8. Switch controller off.

9. Remove MMC from the device.

10. Switch controller on again.

11. The message "Load new param.?" can then be displayed. Acknowledge this message by pressing "Enter" (on the control panel). The drive parameters are now loaded from the non-volatile memory ("Flash") to the volatile memory (RAM) of the device. From now on, device behaves like device without MMC plugged.

5. **Put machine into ready-for-operation status**

   1. Put machine into ready-for-operation status again according to machine manufacturer's instructions.

   2. Check functions of the drive

6. **Check safety technology parameters**

   Finally when the safety technology is activated, it is necessary to check whether the right safety technology parameters have been loaded for the drive. To do so, check the data in "P-0-3205, Safety technology device identifier" (machine types unit, drive for .. axis/spindle) and compile a protocol with the following contents and add it to safety-relevant documentation for the machine:

   - Drive controller replaced on (date)
   - Change counter of safety technology memory (P-0-3201) is at (value)
   - Operating hours at last change of memory (P-0-3202) is at (value)
   - Serial number of control section (see type plate on the device)
   - Serial number of power unit (see type plate on the device)
   - (Date), (name), (signature)

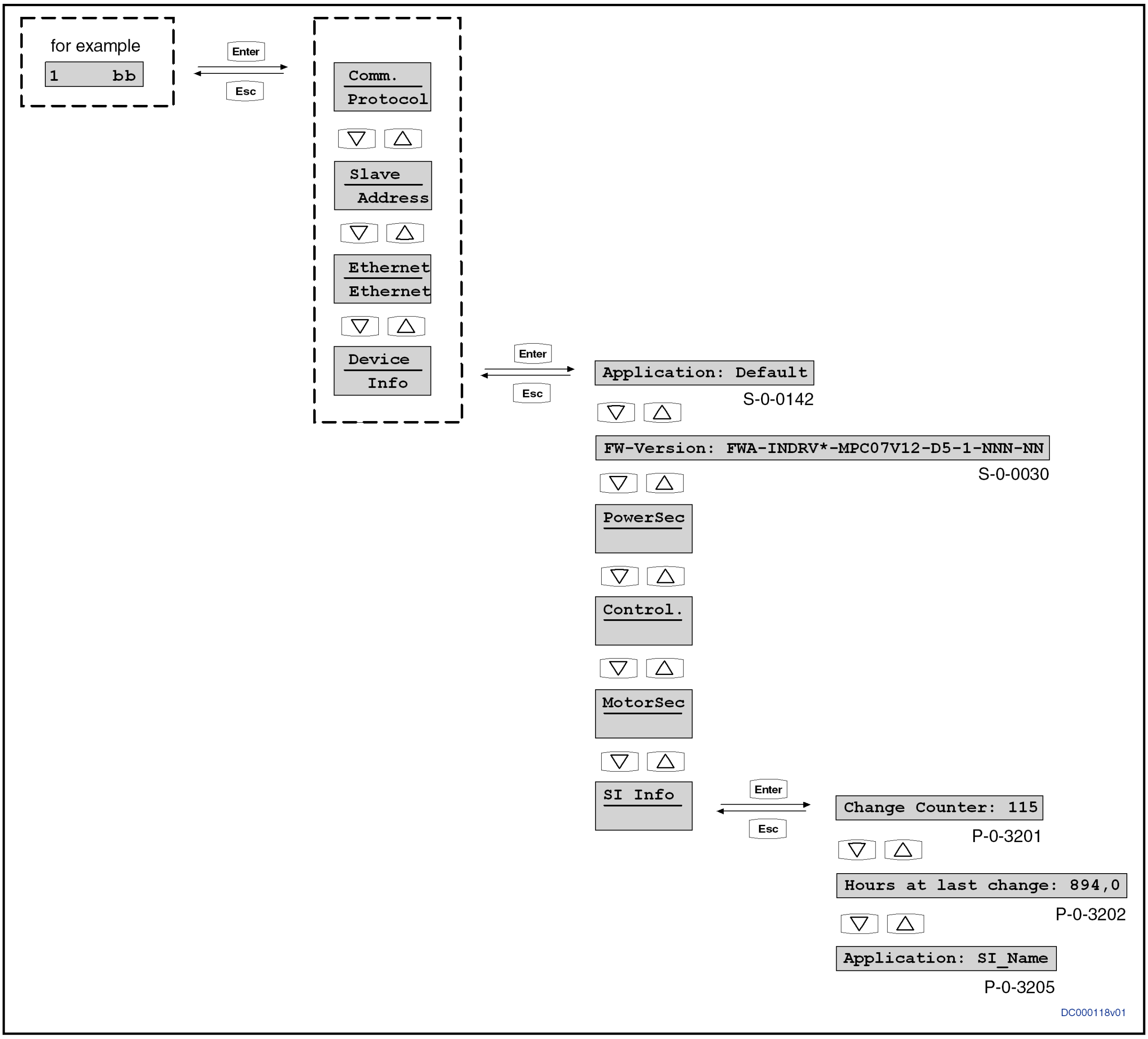


Fig. 11-3: Calling up safety technology characteristic data via the control panel

Controller Replacement With Stationarily Plugged-in MMC

1. Saving parameter values

   If the firmware characteristic IndraMotion MLD with firmware type code:

   - FWA-INDRV*-MPH-08VRS-D5-1-***-ML
   - FWA-INDRV*-MPC-08VRS-D5-1-***-ML

   is activated and the controller to be replaced is configured in one of the following optional modules, the retain data of the drive PLC must be stored on the MMC before dismantling the defective device.

   - Module Digital I/O (control section type code: CSH01.**-**-***-***-MD1-**-S-NN-FW)
   - Module Digital I/O and SSI encoder interface (control section type code: CSH01.**-**-***-***-MD2-**-S-NN-FW)

☞ If backing up the PLC retain data before replacing the device is impossible due to a total breakdown of the device, the parameter values and retain data backed up after initial commissioning must be loaded when the parameter values are loaded later on (see "Loading Parameter Values in Case of Total Breakdown of Device")!

1. Switch drive off and on again

2. Switch to Parameter mode (PM or P2).

3. Switch drive to the Service menu using the display

⇒By simultaneously pressing "Esc" and "Enter" for at least 8 seconds, it is possible to call up extended displays; subsequently pressing the "Up" key (twice) activates the Service menu.

4. Select the "device replace" submenu using the arrow keys and activate it with "Enter".

5. Activate "save Data?" command

⇒The active PLC retain data is copied from the controller-internal memory to an MMC temporarily plugged into the controller.

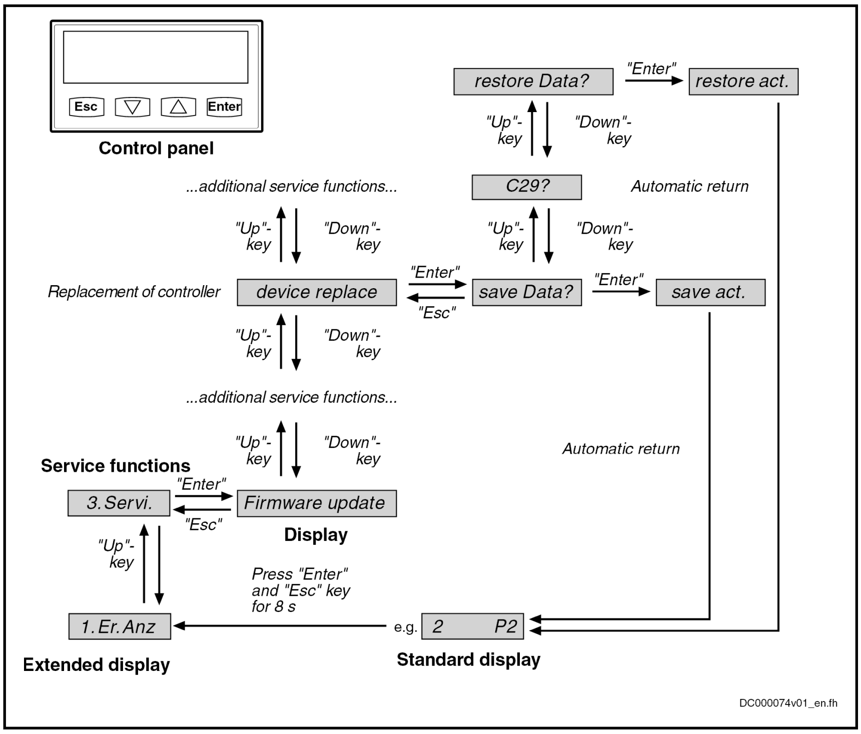


Fig. 11-4: Activating "save Data?" and "restore Data?" commands when replacing the controller using the control panel

6. Disconnect controller from control voltage (this automatically saves parameter values).

7. Remove MMC from the controller.

2. Replace controller

WARNING! Lethal electric shock by live parts with more than 50 V! Make sure drive controller is completely de-energized. Wait at least **30 minutes** after switching off the supply voltages to allow discharging. To shorten the waiting time until voltage has fallen below 50 V, you can use a discharging device (see chapter "Appendix").

1. Open main switch

   2. Make sure main switch cannot be switched on again
   3. Make sure the drive controller is completely de-energized
   4. Remove touch guard and separate connecting lines from drive controller
   5. Unscrew bolts on top and bottom of housing
   6. Take drive controller out of the drive system
   7. Fit new drive controller
   8. Connect new drive controller as specified in the machine circuit diagram
   9. Mount touch guard

3. **Put controller into ready-for-operation status again**

   Put machine into ready-for-operation status again according to machine manufacturer's instructions.

4. **Load firmware and parameter values via MMC**

   If firmware and drive parameters are to be transmitted via MMC to the replacement controller, ensure that the MMC folder "Firmware" contains the firmware required for the drive and the MMC folder "Parameters" contains the parameters backed up before replacing the device.

   1. Disconnect replacement controller from the control voltage.

   2. Put MMC into the replacement controller.

   3. Supply device with control voltage again.

   4. Depending on the "previous configuration" of the replacement device, the message "Firmware update?" can appear during the booting phase. Acknowledge this message by pressing "Enter" (on the control panel). By doing this, firmware is loaded from the plugged-in MMC into the controller.

☞ If the message "Firmware Update?" does not appear, the firmware update must be started via the display.

"3. Service" → "Firmware update" → "FWA update"

   5. Then one of the messages below might be displayed:

   - "Load new param.?"
   - "activate new MMC?"

   ⇒ Acknowledge this message by pressing "Enter" on the control panel. The drive parameters are now loaded from the MMC to the volatile memory of the device; the message "Load new safety?" may possibly appear.

   ⇒ Acknowledge this message by pressing "Enter" on the control panel. Safety technology parameters are now loaded from the MMC to the memory of the optional safety technology module.

   After parameter loading process has been completed, the drive waits for further actions from the control master.

☞ If safety technology is to be activated in the replacement device (in accordance with the replaced device), the drive must be switched to operating mode (OM) or communication phase (P4) after loading the safety technology parameters before it is switched off!

5. **Put machine into ready-for-operation status**

   1. Put machine into ready-for-operation status again according to machine manufacturer's instructions.

   2. Check functions of the drive

6. **Check safety technology parameters**

   Finally when the safety technology is activated, it is necessary to check whether the right safety technology parameters have been loaded for the drive. To do so, check the data in "P-0-3205, Safety technology device identifier" (machine types unit, drive for .. axis/spindle) and compile a protocol with the following contents and add it to safety-relevant documentation for the machine:

   - Drive controller replaced on (date)
   - Change counter of safety technology memory (P-0-3201) is at (value)
   - Operating hours at last change of memory (P-0-3202) is at (value)
   - Serial number of control section (see type plate on the device)
   - Serial number of power unit (see type plate on the device)
   - (Date), (name), (signature)

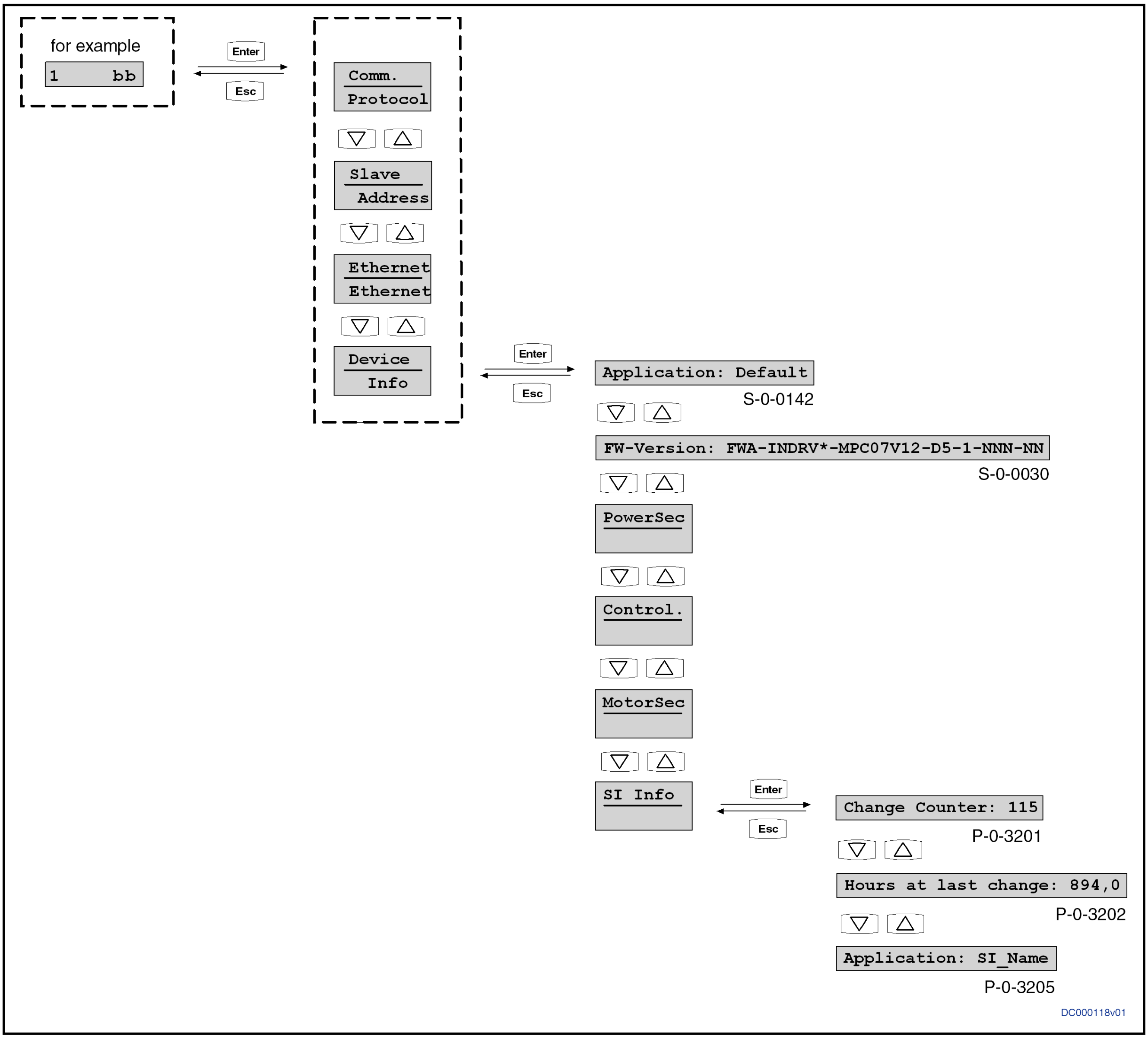


Fig. 11-5: Calling up safety technology characteristic data via the control panel

Controller Replacement Without MMC

☞ The execution of a controller replacement without MMC only makes sense if the controller is equipped with a BASIC single-axis control section.

If the controller is equipped with another control section, it cannot be ensured that after the replacement of the device all parameterized device functions are available again when carrying out the process described below. Therefore, for such controllers, replacement is only recommended with MMC.

1. Saving parameter values

   Before dismantling the defective device, save the drive parameter values, if possible.

☞ If backing up the parameter values before replacing the device is impossible due to a total breakdown of the device, only the parameter values backed up after initial commissioning can be loaded when the parameter values are loaded later on (see "Loading Parameter Values in Case of Total Breakdown of Device")!

1. Switch drive off and on again

2. Switch to Parameter mode (PM or P2)

3. Saving the parameter values of the defective device can take place via the commissioning tool "IndraWorks Ds/D/MLD" or the control master:

- Commissioning tool "IndraWorks Ds/D/MLD":

  By selecting the respective menu item, the parameter values according to the list parameters S-0-0192 and P-0-0195 are stored on an external data carrier (hard disk, floppy disk or the like) [serial communication with the controller or via SYSDA/sercos interface].

- Control master

  The parameter values according to the list parameters S-0-0192 and P-0-0195 are stored on a master-side data carrier by the control master.

2. **Replace controller**

   WARNING! Lethal electric shock by live parts with more than 50 V! Make sure drive controller is completely de-energized. Wait at least **30 minutes** after switching off the supply voltages to allow discharging. To shorten the waiting time until voltage has fallen below 50 V, you can use a discharging device (see chapter "Appendix").

   1. Open main switch
   2. Make sure main switch cannot be switched on again
   3. Make sure the drive controller is completely de-energized
   4. Remove touch guard and separate connecting lines from drive controller
   5. Unscrew bolts on top and bottom of housing
   6. Take drive controller out of the drive system
   7. Fit new drive controller
   8. Connect new drive controller as specified in the machine circuit diagram
   9. Mount touch guard

3. **Put controller into ready-for-operation status again**

   Put machine into ready-for-operation status again according to machine manufacturer's instructions.

4. **Load firmware and parameter values**

   When firmware and drive parameters are to be transmitted to the replaced controller, the required firmware and a parameter backup of the respective axis must be available.

   1. Supply controller with control voltage

   2. Depending on the "previous configuration" of the replacement device, one of the following messages can appear during the booting phase:

   - "F2120 MMC: defective or missing, replace"

⇒ Acknowledge this message by pressing "Esc" on the control panel.

- "Load new param.?"

  ⇒ Acknowledge this message by pressing "Enter" on the control panel,

3. By selecting the respective menu item in "IndraWorks Ds/D/MLD", the firmware stored on an external data carrier (hard disk, floppy disk or similar) is loaded to the controller (serial communication with the controller).

4. Loading the parameter values can take place via the commissioning tool "IndraWorks Ds/D/MLD" or the control master:

- Commissioning tool "IndraWorks Ds/D/MLD"

  By selecting the respective menu item, the parameter values stored on an external data carrier (hard disk, floppy disk or the like), immediately before the device was replaced, according to list parameters S-0-0192 and P-0-0195 are loaded to the controller (serial communication with the controller or via SYSDA/sercos interface). With safety technology available, further actions are required (see "Replacing the controller without stationarily plugged-in MMC").

- Control master

  The axis-specific parameter values saved before having replaced the device can also be loaded via the control master. The parameter values saved immediately before the replacement of the device on a master-side data carrier (according to list parameters S-0-0192 and P-0-0195) are loaded to the controller by the control master. With safety technology available, further actions are required (see "Replacing the controller without stationarily plugged-in MMC").

5. **Put machine into ready-for-operation status**

   1. Put machine into ready-for-operation status again according to machine manufacturer's instructions.

   2. Check functions of the drive

Possible Problems During Controller Replacement

The paragraphs below give a brief description of critical problems and their recommended handling.

Loading parameter values in the event of total breakdown of the device

If it was no longer possible to save the parameter values according to the list parameters S-0-0192 and P-0-0195 immediately before replacing the device (total breakdown of device), the parameter values backed up following initial commissioning are to be loaded.

☞ With drives with absolute value encoder and modulo format, the position data reference has to be established again after having loaded the parameter values saved after initial commissioning, even if the actual position values are signaled to be valid via the parameter "S-0-0403, Position feedback value status"!

NOTICE **The parameter values saved after initial commissioning are not generally suited for reestablishing the operability of the drive after replacement of devices!**

⇒ Check actual position values and active target position before drive enable!

11.4.6 Replacing the Cables

⚠ WARNING **Lethal electric shock by live parts with more than 50 V!**

Power connectors of the cables may only be separated or connected if the installation has been de-energized.

☞ Observe the following points before replacing cables:

- Observe the instructions of the machine manufacturer.
- When using ready-made Rexroth cables, only replace defective cables by cables of identical type.
- If you do not use ready-made Rexroth cables, check to ensure that the new cables match the connection diagram of the machine manufacturer; cable cross section and shielding must match, too!

When the mentioned points are observed, it is not required to repeat the acceptance test within the scope of the function "Integrated safety technology".

- Open main switch
- Make sure main switch cannot be switched on again
- Disconnect connections

☞ When replacing cables, cover the open ends of power lines with protective caps if sprinkling with cooling liquid/lubricant or pollution may occur (allowed pollution degree according to EN50178: 2).

- Replace cables

NOTICE **Property damage caused by bad power connectors!**

Only separate or connect clean and dry power connectors.

- Re-establish connections

11.4.7 Replacing components of safety technology

Replacing the Control Module

When the control module is replaced, it is not necessary to repeat safety technology commissioning and acceptance test.

☞ The same type of control module has to be used after replacement.

Replacing the Redundant Holding Brake

When the redundant holding brake is replaced, it is not necessary to repeat safety technology commissioning and acceptance test.

⚠ DANGER **Dangerous movements! Danger to life, risk of injury, serious injury or property damage!**

While the redundant holding brake is replaced, secure the axis by a blocking device or by moving the axis to a safe end position.

☞ The same type of brake has be used after replacement.

11.4.8 Firmware replacement

General notes on how to replace the firmware

Basic principles

Explanation of terms

For firmware replacement, we distinguish the following cases:

- Release update

  An old firmware release contained in the device (e.g., MPH08**V06**) is replaced by a new firmware release (e.g., MPH08**V08**).

  ⚠ CAUTION **The parameters of the firmware MPx08-V04 are not compatible with those of the firmware MPx08-V02.**

  The parameters of the firmware MPx08-V06 are not compatible with those of the firmware MPx08-V04.

  For the firmware replacement therefore proceed as for a firmware version upgrade.

- Version upgrade

  The old firmware version (e.g., MPH**07**V08) in the device is replaced by a new firmware version (e.g., MPH**08**V12).

☞ The paragraphs below describe the recommended options of firmware replacement by higher releases ("update") or versions ("upgrade"). The same conditions and sequences of actions apply to firmware replacement by older releases or older firmware versions.

Firmware for IndraDrive is replaced using the following hardware and software:

- MultiMediaCard (MMC)
- PC with "IndraWorks Ds/D/MLD" software

☞ The "IndraWorks Ds/D/MLD" commissioning software can be ordered from one of our sales and service facilities. The scope of supply of "IndraWorks Ds/D/MLD" contains a documentation which describes the operation of the program.

Preparations and conditions for firmware replacement

Preparing the firmware replacement

Make the following preparations for firmware replacement:

1. Drive controller must be on (24 V supply).
2. Be absolutely sure to save parameter values before any firmware version upgrade (for release update this is recommended), as otherwise complete (re-)commissioning of the drive is required.

   See Functional Description of firmware "Loading, storing and saving parameters"

General notes on how to proceed

Observe the following points when carrying out the firmware replacement:

- Do not switch off the 24V control voltage while replacing the firmware.
- For devices with MultiEthernet interface (ET option), the firmware has to be replaced using an MMC.

☞ After the firmware was replaced, devices with MultiEthernet interface have to be switched off and back on again to carry out the update of the MultiEthernet firmware. Only then is it allowed to remove the MMC.

☞ When the firmware is replaced in conjunction with the option "Safe Torque Off" (L2), this does not require any specific measures, i.e. the additional measures described below only apply to the use of option "S2"!

Firmware release update

General information

When firmware in a drive controller is replaced by firmware of a **new release**, this is called firmware release update (e.g., FWA-INDRV*-MPH-08**V04**-D5 replaced by FWA-INDRV*-MPH-08**V06**-D5).

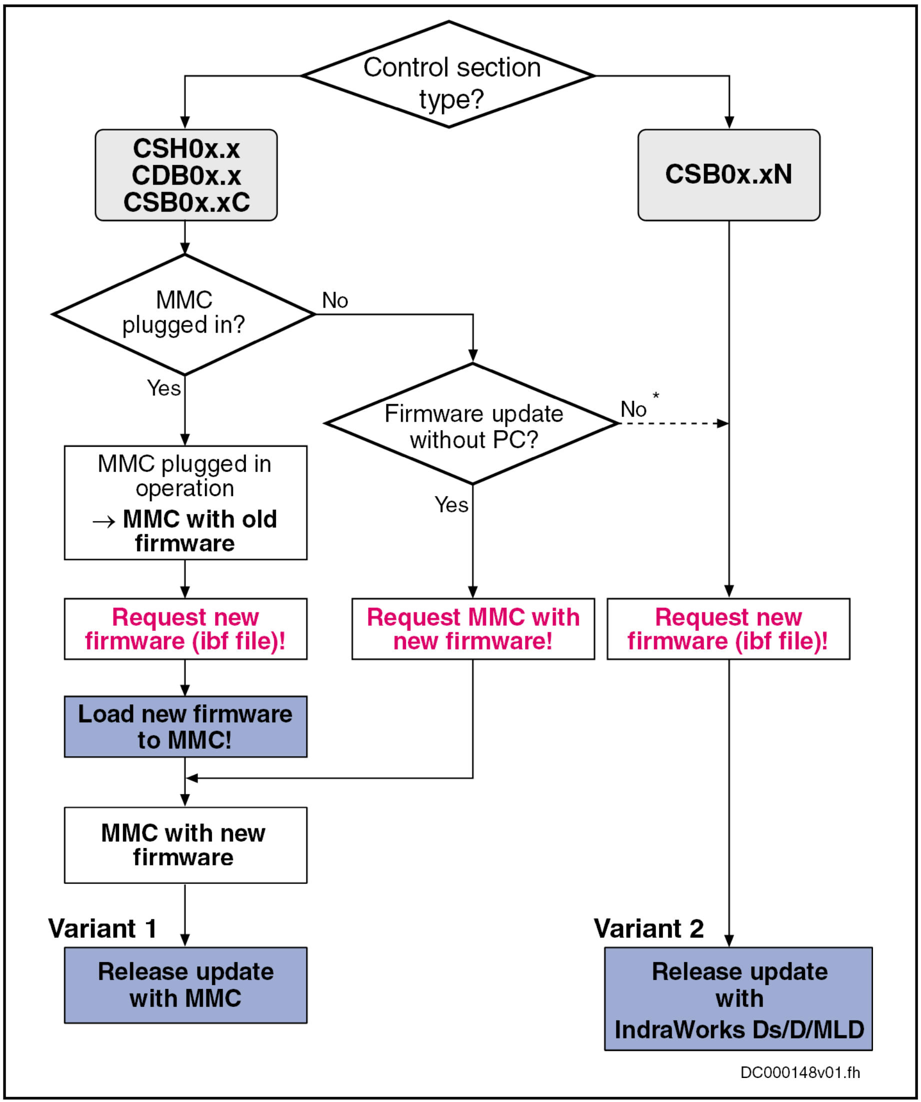
⚠ CAUTION

The parameters of the firmware MPx08-V04 are not compatible with those of the firmware MPx08-V02.

The parameters of the firmware MPx08-V06 are not compatible with those of the firmware MPx08-V04.

For the firmware replacement therefore proceed as for a firmware version upgrade.

The described sequences of the firmware release update depend on the configuration of the control section and the hardware (MMC or PC) used for update. The basically recommended sequence of the firmware release update is illustrated in the diagram below:



*	Only possible for devices without ET option
CSH0x.x	ADVANCED single-axis control section
CDB0x.x	BASIC double-axis control section
CSB0x.xC	BASIC single-axis control section (configurable)
CSB0x.xN	BASIC single-axis control section (not configurable)
Active memory	"Programming module" operation of MMC (see P-0-4065)

Fig. 11-6: Schematic sequence of firmware release update

☞ The actions to be taken which are marked with dark background in this figure are described in the paragraphs below.

Loading new firmware to MMC

Requirements

The following requirements must have been fulfilled for loading firmware to the MMC of the drive:

- New firmware available (ibf file)
- PC with MMC reader
- MMC with old firmware in drive

Loading firmware to MMC

The following steps are required for loading the firmware to the MMC:

1. Switch drive off and remove MMC.
2. Plug MMC into MMC reader and open "Firmware" folder on MMC.
3. Delete old firmware (e.g., FWA-INDRV_-MPH-08**V02**-D5.ibf).
4. Copy new firmware (e.g., FWA-INDRV_-MPH-08**V04**-D5.ibf) to "Firmware" folder.

☞ Only one firmware file may be stored in the folder "Firmware" on the MMC. With several firmware files, the message "MMC not correct" appears on the display of the drive after the booting process.

5. Remove MMC from MMC reader after writing process has been completed.

Option 1: Release update with MMC

Selection criterion

Carrying out the firmware release update with MMC makes sense when the controller has **not** been equipped with a BASIC single-axis control section of the CSB0x.xN type.

Firmware update with MMC

The optional MultiMediaCard (MMC) allows transmitting drive firmware to the drive controller in a quick and uncomplicated way.

☞ As the MMC is a storage medium that can be simply written (for example via a PC), it is recommended that the MMC content be checked before downloading the firmware. Make sure that the MMC really contains the appropriate firmware type.

An MMC with the current release of the required firmware can be ordered from one of our sales and service facilities.

Carrying out the firmware release update with MMC requires the following steps:

1. **Load firmware**

   ⇒ Switch drive off.

   ⇒ Plug MMC with new firmware into corresponding slot at controller.

   ⇒ Restart drive with MMC plugged.

   After drive has booted up, the following message appears:

   - "Firmware update?"

   ⇒ Acknowledge this message by pressing "Enter" key of control panel. By doing this, firmware is loaded from plugged MMC to controller.

   One of the following messages will be displayed, depending on the operating status of the drive:

   - "Load Param from MMC" or "Load new param?"
   - "Activate new MMC?"

- "F2120 MMC: Defective or missing, replace"

> ☞ For control sections with an optional MultiEthernet card (option: ET), the "Load Param from MMC", "Load new param?" and "activate new MMC?" checks have to be aborted with ESC via the display. Only after this action is the firmware for the MultiEthernet option installed.

⇒ Switch off drive, remove MMC (if drive was operated without MMC plugged) and restart drive!

2. **Put machine into ready-for-operation state**

   ⇒ Put machine into ready-for-operation state again according to machine manufacturer's instructions!

   ⇒ Check functions of drive!

3. **Check safety technology parameters** (only when safety technology has been activated in the drive)

   In the case of a release update, the safety technology parameters are retained. With safety technology activated, the following steps are additionally required:

   ⇒ Check whether correct safety technology parameter settings for drive are still available.

   To do this, check the following points:

   - Data in parameter "P-0-3205, Safety technology device identifier"
   - Status of safety technology using parameter "P-0-3207, Safety technology password level" (in the case of active and locked safety technology, level is 2)
   - Change counter of safety technology memory (parameter "P-0-3201, Change counter of safety technology memory")
   - Operating hours at last change of memory (parameter "P-0-3202, Operating hours at last change of memory")

⚠ CAUTION **If the integrated safety technology is used and a firmware release update is carried out for firmware versions older than MPx02-V20, it is necessary to repeat the safety technology acceptance test.**

After firmware release update, the safety technology acceptance test must be carried out again!

Option 2: Release update with "IndraWorks Ds/D/MLD"

Selection criterion

The following requirements should have been fulfilled in order that carrying out the firmware release update with "IndraWorks Ds/D/MLD" makes sense:

- Controller is operated without MMC

  - or -

- Controller has been equipped with BASIC single-axis control section of the CSB0x.xN type.

Firmware update with "IndraWorks Ds/D/MLD"

Carrying out the firmware release update with "IndraWorks Ds/D/MLD" requires the following steps:

1. **Load firmware**

⇒ Start "IndraWorks".

⇒ Load project for corresponding axis or create new project. To do this, address axis via a serial connection.

⇒ Switch project "online".

⇒ Select/highlight controller and call "Firmware management" in context menu.

A new window opens and firmware currently available in drive is displayed on its right side. On left side of window, firmware available in current firmware directory is displayed.

⇒ Select new firmware (*.ibf file) and start firmware download using "Download" button.

Firmware download runs automatically and all required firmware components are loaded to drive.

☞ IndraWorks automatically goes to the offline mode. You will be asked whether a backup of the parameters is to be made. Refuse this with "No".

⇒ After firmware download has been completed, close "Firmware management" window.

2. **Put machine into ready-for-operation state**

   ⇒ Put machine into ready-for-operation state again according to machine manufacturer's instructions!

   ⇒ Check functions of drive!

3. **Check safety technology parameters** (only when safety technology has been activated in the drive)

   In the case of a firmware release update, the safety technology parameters are retained. With safety technology activated, the following steps are additionally required:

   ⇒ Check whether correct safety technology parameter settings for drive are still available.

   To do this, check the following points:

- Data in parameter "P-0-3205, Safety technology device identifier"
- Status of safety technology using parameter "P-0-3207, Safety technology password level" (in the case of active and locked safety technology, level is 2)
- Change counter of safety technology memory (parameter "P-0-3201, Change counter of safety technology memory")
- Operating hours at last change of memory (parameter "P-0-3202, Operating hours at last change of memory")

Firmware version upgrade

General information

When firmware in a drive controller is replaced by firmware of a **more recent version**, this is called firmware version upgrade (e.g., FWA-INDRV*-MPH-**07**V10-D5 replaced by FWA-INDRV*-MPH-**08**V06-D5).

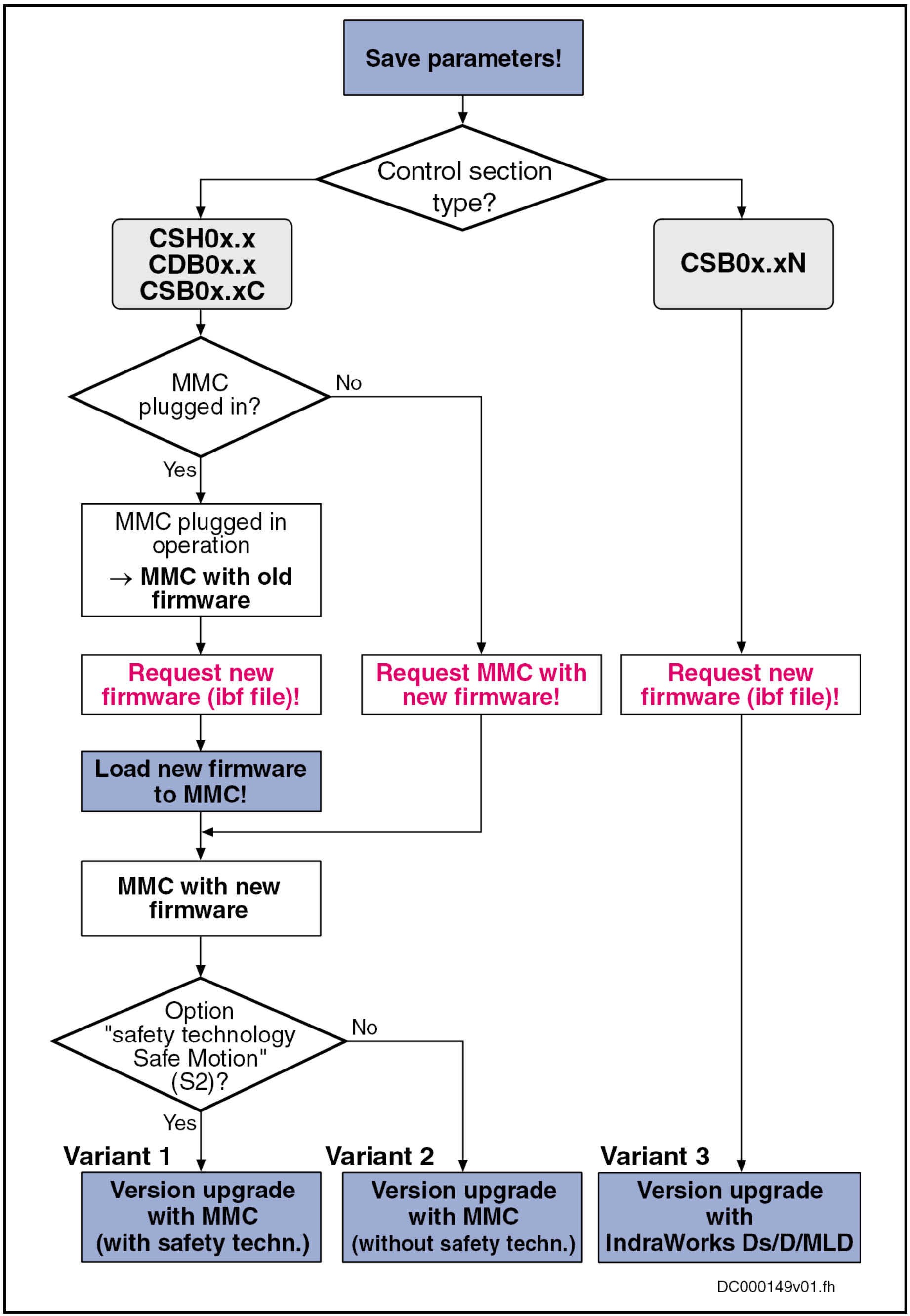
☞ **Before** the firmware version upgrade is carried out, all parameters have to be saved (e.g., with "IndraWorks").

After the firmware replacement, the parameters have to be restored.

⚠ DANGER **Dangerous movements possible! Danger to life, risk of injury, serious injury or property damage!**

In order to ensure correct functioning and to prevent personal damage, a complete acceptance test must be carried out after a firmware version upgrade for drive controllers with the optional module for safety technology (S2).

The described sequences of the firmware version upgrade depend on the configuration of the control section and the firmware used. The basically recommended sequence of the firmware version upgrade is illustrated in the scheme below:


Save parameters!
Control section type?
CSH0x.x
CDB0x.x
CSB0x.xC
CSB0x.xN
MMC plugged in?
No
Yes
MMC plugged in operation
→ MMC with old firmware
Request new firmware (ibf file)!
Request MMC with new firmware!
Request new firmware (ibf file)!
Load new firmware to MMC!
MMC with new firmware
Option "safety technology Safe Motion" (S2)?
No
Yes
Variant 1
Version upgrade with MMC (with safety techn.)
Variant 2
Version upgrade with MMC (without safety techn.)
Variant 3
Version upgrade with IndraWorks Ds/D/MLD
DC000149v01.fh

CSH0x.x	ADVANCED single-axis control section
CDB0x.x	BASIC double-axis control section
CSB0x.xC	BASIC single-axis control section (configurable)
CSB0x.xN	BASIC single-axis control section (not configurable)
Active memory	"Programming module" operation of MMC (see P-0-4065)

Fig. 11-7: Schematic sequence of firmware version upgrade

☞ The actions to be taken which are marked with dark background in this figure are described in the paragraphs below.

Saving parameter values

Before the firmware upgrade, all application-specific parameter values have to be saved on a data carrier. The parameter backup can be carried out by means of:

- **Commissioning software "IndraWorks Ds/D/MLD"**

  → Saving parameter values on external data carrier

- or -

- **Control master**

  → Saving parameter values on master-side data carrier

☞ Saving the parameters on the MMC available in the drive is without effect, as this backup will be deleted during the firmware upgrade!

Loading new firmware to MMC

Requirements

The following requirements must have been fulfilled for loading firmware to the MMC of the drive:

- New firmware available (ibf file)
- PC with MMC reader
- MMC with old firmware in drive

Loading firmware to MMC

The following steps are required for loading the firmware to the MMC:

1. Switch drive off and remove MMC.
2. Plug MMC into MMC reader and open "Firmware" folder on MMC.
3. Delete old firmware (e.g., FWA-INDRV*-MPH-07V10-D5.ibf).
4. Copy new firmware (e.g., FWA-INDRV*-MPH-08V02-D5.ibf) to "Firmware" folder.

   Note: Only one firmware file may be stored in the folder "Firmware" on the MMC. With several firmware files, the message "MMC not correct" appears on the display of the drive after the booting process.
5. Remove MMC from MMC reader after writing process has been completed.

Option 1: Version upgrade with MMC (with safety technology)

Selection criterion

The following requirements should have been fulfilled in order that carrying out the firmware version upgrade with MMC makes sense (with safety technology):

- Controller has **not** been equipped with BASIC single-axis control section.
- Optional slot for safety technology has been equipped with the optional module "Safe Motion" (S2).
- The current parameterization of the axis was saved.

Firmware upgrade with MMC (with safety technology)

Carrying out the firmware version upgrade with MMC requires the following steps (with safety technology):

1. **Load firmware**

   ⇒ Switch drive off.

   ⇒ Plug MMC with new firmware into corresponding slot at controller.

   ⇒ Restart drive with MMC plugged.

   After drive has booted up, the following message appears:

   - "Firmware update?"

   ⇒ Acknowledge this message by pressing "Enter" key of control panel. By doing this, firmware is loaded from plugged MMC to controller.

One of the following messages will be displayed, depending on the operating status of the drive:

- "Load Param from MMC" or "Load new param?"
- "Activate new MMC?"
- "F2120 MMC: Defective or missing, replace"
- "F2009 PL Load parameter default values"

☞ For control sections with an optional MultiEthernet card (option: ET), the "Load Param from MMC", "Load new param?" and "activate new MMC?" checks have to be aborted with ESC via the display. Only after this action is the firmware for the MultiEthernet option installed.

⇒ Switch off drive, remove MMC (if drive was operated without MMC plugged) and restart drive!

2. **Put drive into ready-for-operation state**

   ⇒ Clear all present error messages and start execution of "C07_2 Load defaults procedure command (load defaults procedure for safety technology)"!

   ⇒ As the number of parameters to be buffered has changed, "C07_1 Load defaults parameter command (loading basic parameters)" has to be activated subsequently. All buffered parameters are thereby set to their default values.

3. **Load parameter values**

   ⇒ Load parameter file which was saved!

   ⇒ Switch off drive and restart it or execute reboot command to activate parameter setting.

4. **Entire commissioning of integrated safety technology**

   ⇒ Switch drive to operating mode (communication phase 4).

   ⇒ Clear any error message that is present.

   ⇒ Activate command "synchronize and store safety technology IDN " (C3000 Synchronize and store safety technology IDN).

   ⇒ Activate safety technology by inputting safety technology password (P-0-3206, Safety technology password).

   ⇒ Carry out parameter verification and new acceptance test.

   ℹ See sections "Activating the safety technology" and "Acceptance test" in the documentation "Integrated Safety Technology According to IEC61508" (DOK-INDRV*-SI2-**VRS**-AW**-EN-P; mat. no. R911327664)

⚠ DANGER **Dangerous movements possible! Danger to life, risk of injury, serious injury or property damage!**

In order to ensure correct functioning and to prevent personal damage, a complete acceptance test must be carried out after a firmware version upgrade for drive controllers with the optional module for safety technology (S2).

⇒ Make safety technology parameter backup, compile acceptance test protocol and add it to safety-relevant documentation of machine.

5. **Put machine into ready-for-operation state**

   ⇒ Put machine into ready-for-operation state again according to machine manufacturer's instructions!

   ⇒ Check functions of drive!

Option 2: Version upgrade with MMC (without safety technology)

Selection criterion

The following requirements should have been fulfilled in order that carrying out the firmware version upgrade with MMC makes sense (without safety technology):

- Controller has **not** been equipped with BASIC single-axis control section of the CSB0x.xN type.
- Optional slot for safety technology has **not** been equipped with the optional module "Safe Motion" (S2).
- The current parameterization of the axis was saved.

Firmware upgrade with MMC (without safety technology)

Carrying out the firmware version upgrade with MMC requires the following steps (without safety technology):

1. **Load firmware**

   ⇒ Switch drive off.

   ⇒ Plug MMC with new firmware into corresponding slot at controller.

   ⇒ Restart drive with MMC plugged.

   After drive has booted up, the following message appears:

   - "Firmware update?"

   ⇒ Acknowledge this message by pressing "Enter" key of control panel. By doing this, firmware is loaded from plugged MMC to controller.

   One of the following messages will be displayed, depending on the operating status of the drive:

   - "Load Param from MMC" or "Load new param.?"
   - "Activate new MMC?"
   - "F2120 MMC: Defective or missing, replace"

☞ For control sections with an optional MultiEthernet card (option: ET), the "Load Param from MMC", "Load new param?" and "activate new MMC?" checks have to be aborted with ESC via the display. Only after this action is the firmware for the MultiEthernet option installed.

   ⇒ Switch off drive, remove MMC (if drive was operated without MMC plugged) and restart drive!

2. **Put drive into ready-for-operation state**

   ⇒ As the number of parameters to be buffered has changed, "PL" appears on display (in case errors are present, remove them first). If the "Esc" key is pressed now, all buffered parameters are set to their default values. During this time, message "C07 Load default parameters" appears on the display. If errors are present, they first have to be removed and the command C07_1 must then be manually activated!

3. **Load parameter values**

   ⇒ Load parameter file which was saved!

⇒ Switch off drive and restart it or execute reboot command to activate parameter setting.

4. **Put machine into ready-for-operation state**

   ⇒ Put machine into ready-for-operation state again according to machine manufacturer's instructions!

   ⇒ Check functions of drive!

Option 3: Version upgrade with "IndraWorks Ds/D/MLD"

Selection criterion

The following requirements should have been fulfilled in order that carrying out the firmware version upgrade with "IndraWorks Ds/D/MLD" makes sense:

- Controller has been equipped with BASIC single-axis control section.
- The current parameterization of the axis was saved.

Firmware upgrade with "IndraWorks Ds/D/MLD"

Carrying out the firmware version upgrade with "IndraWorks Ds/D/MLD" requires the following steps:

1. **Load firmware**

   ⇒ Call "IndraWorks".

   ⇒ Load project for corresponding axis or create new project. To do this, address axis via a serial connection.

   ⇒ Switch project "online".

   ⇒ Select/highlight controller and call "Firmware management" in context menu.

   A new window opens and firmware currently available in drive is displayed on its right side. On left side of window, firmware available in current firmware directory is displayed.

   ⇒ Highlight new firmware (*.ibf file) on left side and start firmware download using "Download" button.

   Firmware download runs automatically and all required firmware components are loaded to drive.

   ⇒ After firmware download has been completed, close "Firmware management" window.

2. **Put drive into ready-for-operation state**

   ⇒ Switch project "offline" and then switch it back "online".

   After project has been switched online, a message signals that "IndraWorks" could not establish communication to drive via serial interface, as drive-internal settings for serial communication were reset.

   ⇒ Reconfigure communication using "Search for devices" button.

   ⇒ As firmware in drive no longer complies with version stored in project, a corresponding message is displayed. To adjust firmware version in project, first select "Repair" option and then the "Delete existing drive from project" and "Add new drive to project" options.

   ⇒ As the number of parameters to be buffered has changed, "PL" appears on display (in case errors are present, remove them first). If the "Esc" key is pressed now, all buffered parameters are set to their default values. During this time, message "C07 Load default parameters" appears on the display.

   If errors are present, they first have to be removed and the command C07_1 must then be manually started!

3. **Load parameter values**

   ⇒ Load parameter file which was saved!

4. **Put machine into ready-for-operation state**

   ⇒ Put machine into ready-for-operation state again according to machine manufacturer's instructions!

   ⇒ Check functions of drive!

Possible problems during firmware replacement

Problematic situations

Firmware replacement is carried out incompletely, if one of the following situations occurs during the sequence of firmware replacement:

- 24V supply of control section is switched off
- Connection to drive is interrupted (e.g., defective interface cable)
- Software crashes

The drive controller then possibly is no longer operable, because the firmware contained in the components is no longer compatible.

If no valid firmware is available in the control section in this case, the loader is started. The drive display signals "LOADER". The loader only allows the firmware of the control section to be updated. Optional modules, such as "Safe Motion" (S2) or "cross communication" (CCD), cannot be programmed in this state. This has to be done, after successful firmware replacement in the control section, in a second run according to the descriptions of the firmware replacement variants.

In this situation, replacement of the control section firmware is only supported by "IndraWorks".

☞ Upon successful firmware replacement in the control section, a restart has to be carried out. Then all available components have to be updated, too.

Requirements for loading the firmware

The following requirements must have been fulfilled for loading firmware to the drive:

- Serial connection to drive available
- Drive display signals "LOADER"

Firmware replacement in control section in the case of error

The following steps are required for loading the firmware to the control section in the case of error:

1. Call "IndraWorks Ds/D/MLD".
2. In menu, call firmware management under "Tools → Drive → Firmware management".
3. Select device and COM interface.

   A new window opens and firmware available in current firmware directory is displayed on its left side.
4. Highlight new firmware (*.ibf file) on left side and start firmware download via "Download" button.

   Firmware download runs automatically and all required firmware components are loaded to drive.
5. After firmware download has been completed, close "Firmware management" window.
6. Restart drive!

If the drive has not been equipped with any optional modules, such as "Safe Motion" (S2) or "cross communication" (CCD), continue following the instructions for release update or version upgrade! Otherwise, carry out the release update or version upgrade again to program the optional modules.

F8129 displayed after firmware replacement

If the error F8129 (Incorrect optional module firmware) is displayed after every booting process of the device after the firmware has been replaced, the firmware was not loaded correctly to one of the optional modules. This can occur if:

- The firmware was loaded via IndraWorks, but the device does not support the complete firmware replacement via IndraWorks
- The firmware had been loaded via MMC, but the MMC card was removed too early

In both cases, repeat the firmware replacement using an MMC. In doing so, make sure to carry out the complete firmware replacement. The procedure is described in detail in the previous chapters.

12 Decommissioning Drive Components

Before the drive or a component is decommissioned, an impact and hazard analysis must be prepared. This analysis must assess how the decommissioning affects the safety of the installation.

Furthermore, the impact and hazard analysis must contain a risk assessment of the process of decommissioning.

On the basis of this impact and hazard analysis, decommission the drive or component (see also IEC 61508-1:2010, 7.17).

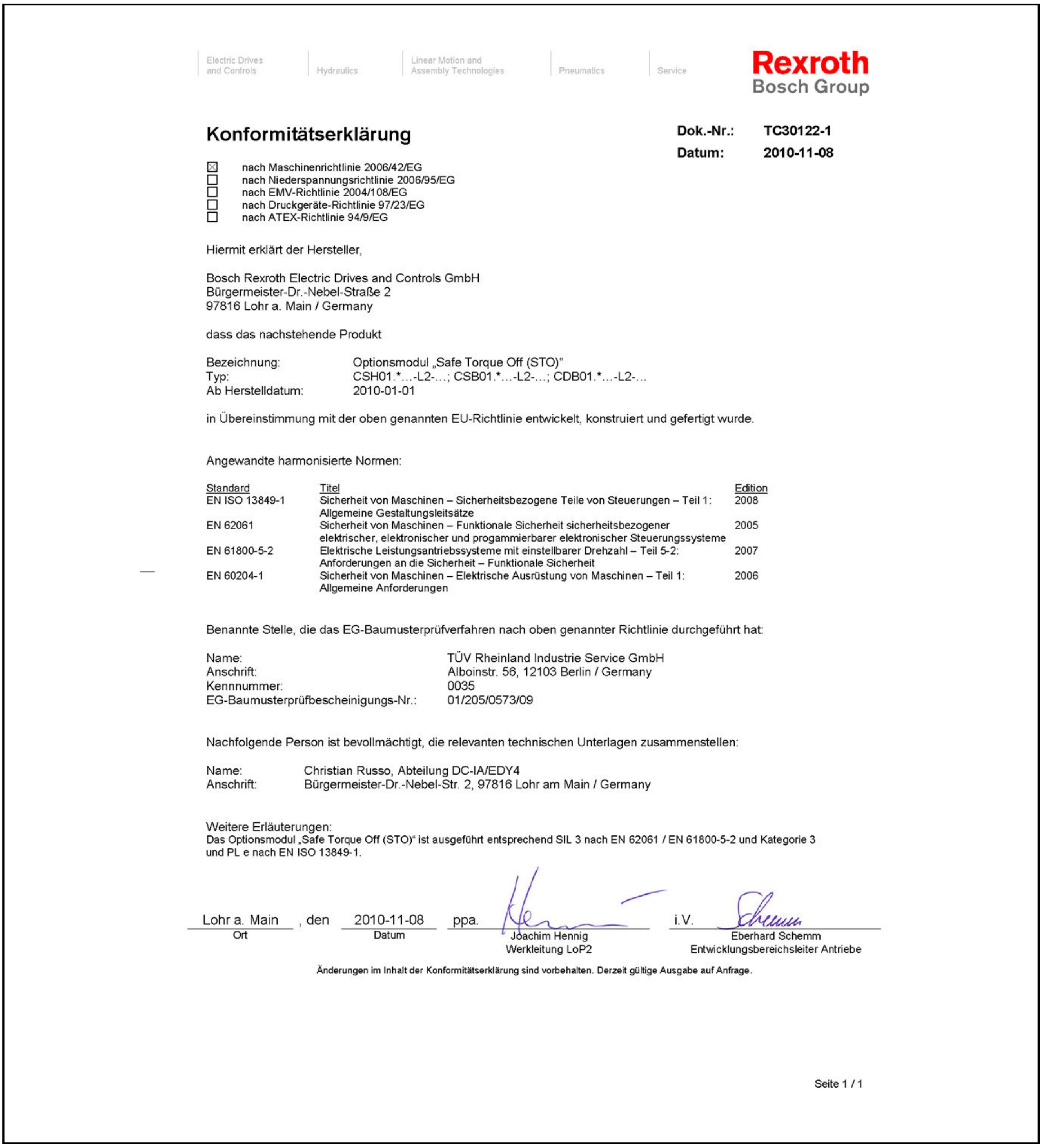
13 Declarations of Conformity

The safety technology was certified by TÜV Rheinland®; the NRTL listing by TÜV Rheinland of North America is in preparation.

The drive controller complies with the protection goals of the Low-Voltage Directive 2006/95/EC.

We declare conformity with the Machinery Directive for the optional safety technology module "L2 - Safe Torque Off".

Declarations of Conformity



Electric Drives and Controls | Hydraulics | Linear Motion and Assembly Technologies | Pneumatics | Service

Rexroth
Bosch Group

Konformitätserklärung

Dok.-Nr.: TC30122-1
Datum: 2010-11-08

☒ nach Maschinenrichtlinie 2006/42/EG
☐ nach Niederspannungsrichtlinie 2006/95/EG
☐ nach EMV-Richtlinie 2004/108/EG
☐ nach Druckgeräte-Richtlinie 97/23/EG
☐ nach ATEX-Richtlinie 94/9/EG

Hiermit erklärt der Hersteller,

Bosch Rexroth Electric Drives and Controls GmbH
Bürgermeister-Dr.-Nebel-Straße 2
97816 Lohr a. Main / Germany

dass das nachstehende Produkt

Bezeichnung: Optionsmodul „Safe Torque Off (STO)“
Typ: CSH01.*…-L2-…; CSB01.*…-L2-…; CDB01.*…-L2-…
Ab Herstelldatum: 2010-01-01

in Übereinstimmung mit der oben genannten EU-Richtlinie entwickelt, konstruiert und gefertigt wurde.

Angewandte harmonisierte Normen:

Standard	Titel	Edition
EN ISO 13849-1	Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze	2008
EN 62061	Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und progammierbarer elektronischer Steuerungssysteme	2005
EN 61800-5-2	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit	2007
EN 60204-1	Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen	2006

Benannte Stelle, die das EG-Baumusterprüfverfahren nach oben genannter Richtlinie durchgeführt hat:

Name: TÜV Rheinland Industrie Service GmbH
Anschrift: Alboinstr. 56, 12103 Berlin / Germany
Kennnummer: 0035
EG-Baumusterprüfbescheinigungs-Nr.: 01/205/0573/09

Nachfolgende Person ist bevollmächtigt, die relevanten technischen Unterlagen zusammenstellen:

Name: Christian Russo, Abteilung DC-IA/EDY4
Anschrift: Bürgermeister-Dr.-Nebel-Str. 2, 97816 Lohr am Main / Germany

Weitere Erläuterungen:
Das Optionsmodul „Safe Torque Off (STO)“ ist ausgeführt entsprechend SIL 3 nach EN 62061 / EN 61800-5-2 und Kategorie 3 und PL e nach EN ISO 13849-1.

Lohr a. Main , den 2010-11-08 ppa. i.V.
Ort Datum

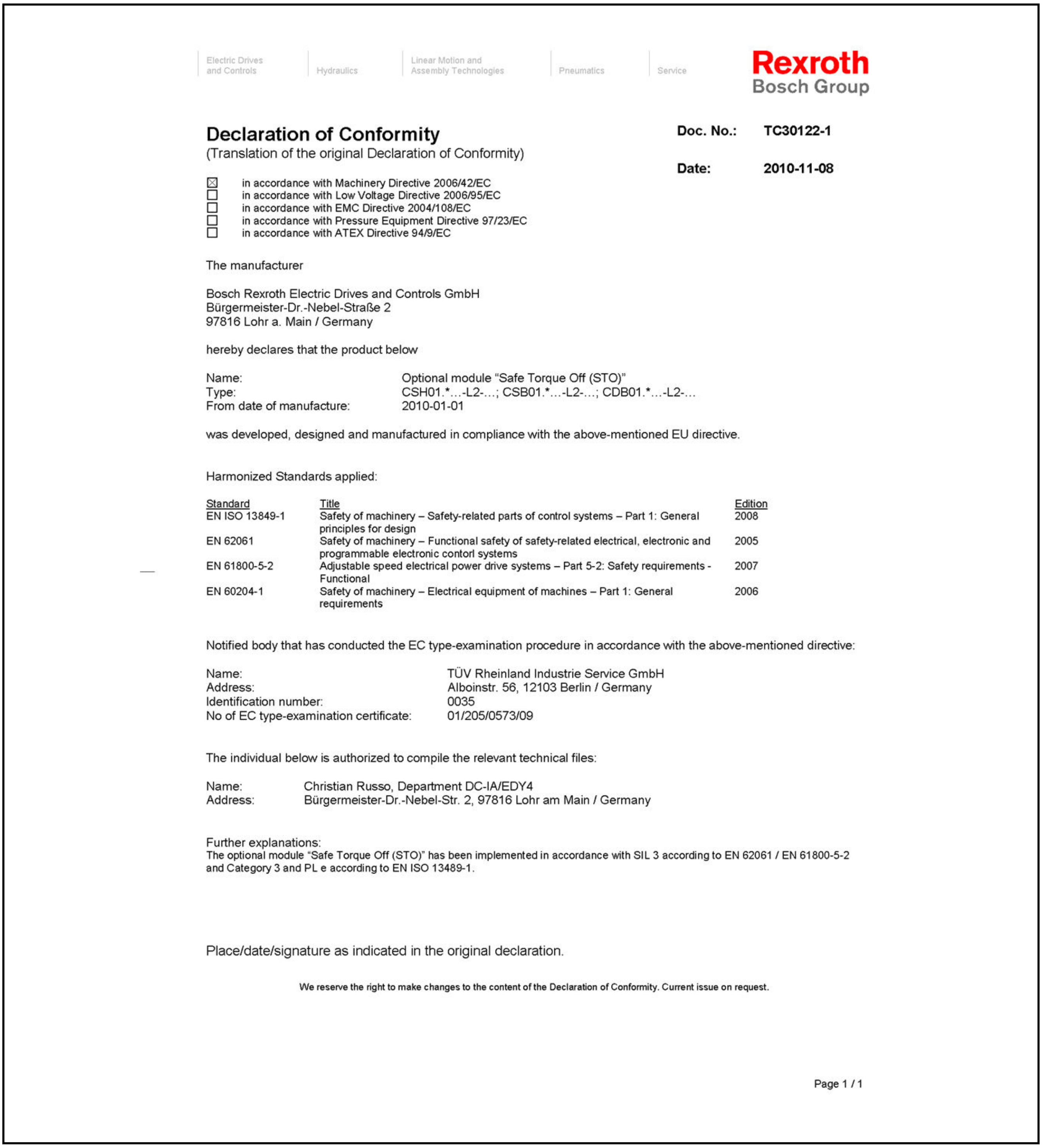
Joachim Hennig
Werkleitung LoP2

Eberhard Schemm
Entwicklungsbereichsleiter Antriebe

Änderungen im Inhalt der Konformitätserklärung sind vorbehalten. Derzeit gültige Ausgabe auf Anfrage.

Seite 1 / 1

Fig. 13-1: Declaration of Conformity for the Optional Safety Technology Module "L2 - Safe Torque Off"



Electric Drives and Controls | Hydraulics | Linear Motion and Assembly Technologies | Pneumatics | Service

Rexroth
Bosch Group

Declaration of Conformity
(Translation of the original Declaration of Conformity)

Doc. No.: **TC30122-1**

Date: **2010-11-08**

☒ in accordance with Machinery Directive 2006/42/EC
☐ in accordance with Low Voltage Directive 2006/95/EC
☐ in accordance with EMC Directive 2004/108/EC
☐ in accordance with Pressure Equipment Directive 97/23/EC
☐ in accordance with ATEX Directive 94/9/EC

The manufacturer

Bosch Rexroth Electric Drives and Controls GmbH
Bürgermeister-Dr.-Nebel-Straße 2
97816 Lohr a. Main / Germany

hereby declares that the product below

Name:	Optional module “Safe Torque Off (STO)”
Type:	CSH01.*…-L2-…; CSB01.*…-L2-…; CDB01.*…-L2-…
From date of manufacture:	2010-01-01

was developed, designed and manufactured in compliance with the above-mentioned EU directive.

Harmonized Standards applied:

Standard	Title	Edition
EN ISO 13849-1	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design	2008
EN 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic contorl systems	2005
EN 61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements - Functional	2007
EN 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	2006

Notified body that has conducted the EC type-examination procedure in accordance with the above-mentioned directive:

Name:	TÜV Rheinland Industrie Service GmbH
Address:	Alboinstr. 56, 12103 Berlin / Germany
Identification number:	0035
No of EC type-examination certificate:	01/205/0573/09

The individual below is authorized to compile the relevant technical files:

Name:	Christian Russo, Department DC-IA/EDY4
Address:	Bürgermeister-Dr.-Nebel-Str. 2, 97816 Lohr am Main / Germany

Further explanations:
The optional module “Safe Torque Off (STO)” has been implemented in accordance with SIL 3 according to EN 62061 / EN 61800-5-2 and Category 3 and PL e according to EN ISO 13489-1.

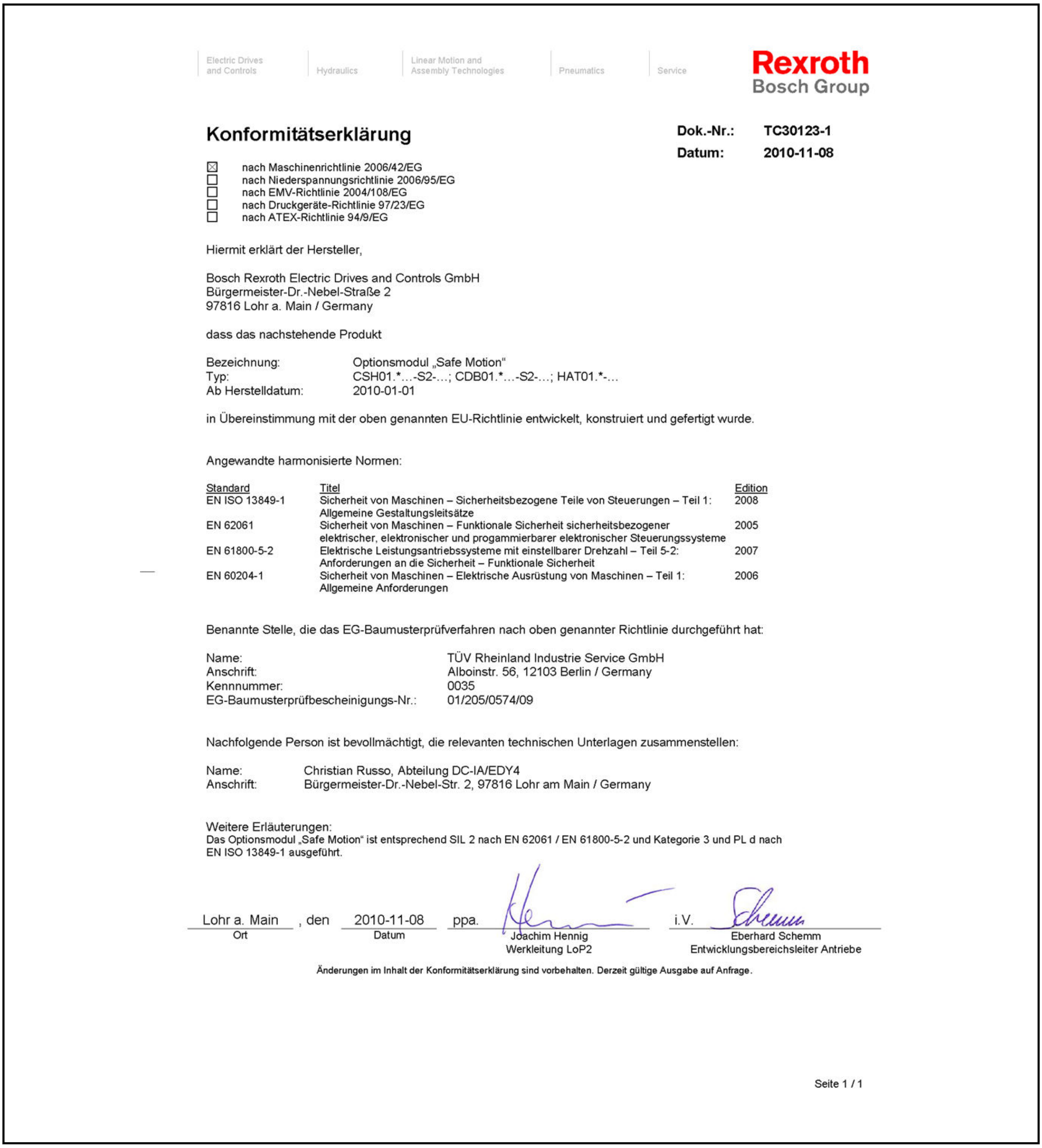
Place/date/signature as indicated in the original declaration.

We reserve the right to make changes to the content of the Declaration of Conformity. Current issue on request.

Page 1 / 1

Fig. 13-2: Translation of the Original Declaration of Conformity for the Optional Safety Technology Module "L2 - Safe Torque Off"

We declare conformity with the Machinery Directive for the optional safety technology module "S2 - Safe Motion".



Electric Drives and Controls | Hydraulics | Linear Motion and Assembly Technologies | Pneumatics | Service

Rexroth
Bosch Group

Konformitätserklärung

Dok.-Nr.: **TC30123-1**
Datum: **2010-11-08**

☒ nach Maschinenrichtlinie 2006/42/EG
☐ nach Niederspannungsrichtlinie 2006/95/EG
☐ nach EMV-Richtlinie 2004/108/EG
☐ nach Druckgeräte-Richtlinie 97/23/EG
☐ nach ATEX-Richtlinie 94/9/EG

Hiermit erklärt der Hersteller,

Bosch Rexroth Electric Drives and Controls GmbH
Bürgermeister-Dr.-Nebel-Straße 2
97816 Lohr a. Main / Germany

dass das nachstehende Produkt

Bezeichnung: Optionsmodul „Safe Motion"
Typ: CSH01.*…-S2-…; CDB01.*…-S2-…; HAT01.*-…
Ab Herstelldatum: 2010-01-01

in Übereinstimmung mit der oben genannten EU-Richtlinie entwickelt, konstruiert und gefertigt wurde.

Angewandte harmonisierte Normen:

Standard	Titel	Edition
EN ISO 13849-1	Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze	2008
EN 62061	Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und progammierbarer elektronischer Steuerungssysteme	2005
EN 61800-5-2	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit	2007
EN 60204-1	Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen	2006

Benannte Stelle, die das EG-Baumusterprüfverfahren nach oben genannter Richtlinie durchgeführt hat:

Name: TÜV Rheinland Industrie Service GmbH
Anschrift: Alboinstr. 56, 12103 Berlin / Germany
Kennnummer: 0035
EG-Baumusterprüfbescheinigungs-Nr.: 01/205/0574/09

Nachfolgende Person ist bevollmächtigt, die relevanten technischen Unterlagen zusammenstellen:

Name: Christian Russo, Abteilung DC-IA/EDY4
Anschrift: Bürgermeister-Dr.-Nebel-Str. 2, 97816 Lohr am Main / Germany

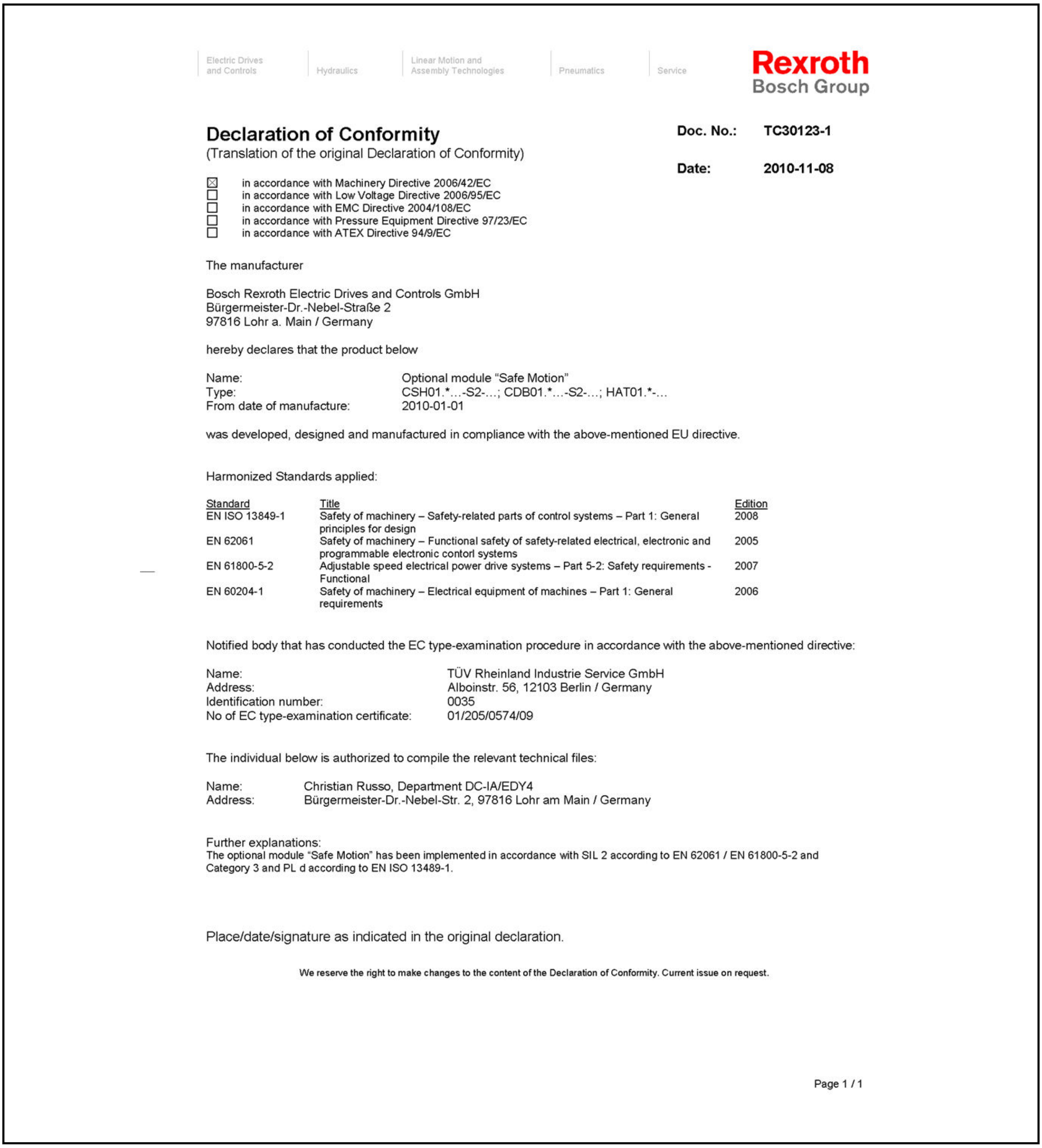
Weitere Erläuterungen:
Das Optionsmodul „Safe Motion" ist entsprechend SIL 2 nach EN 62061 / EN 61800-5-2 und Kategorie 3 und PL d nach EN ISO 13849-1 ausgeführt.

Lohr a. Main , den 2010-11-08 ppa. i.V.
Ort Datum Joachim Hennig Eberhard Schemm
Werkleitung LoP2 Entwicklungsbereichsleiter Antriebe

Änderungen im Inhalt der Konformitätserklärung sind vorbehalten. Derzeit gültige Ausgabe auf Anfrage.

Seite 1 / 1

Fig. 13-3: Declaration of Conformity for the Optional Safety Technology Module "S2 - Safe Motion"



Electric Drives and Controls | Hydraulics | Linear Motion and Assembly Technologies | Pneumatics | Service

Rexroth
Bosch Group

Declaration of Conformity

(Translation of the original Declaration of Conformity)

Doc. No.: **TC30123-1**

Date: **2010-11-08**

☒ in accordance with Machinery Directive 2006/42/EC
☐ in accordance with Low Voltage Directive 2006/95/EC
☐ in accordance with EMC Directive 2004/108/EC
☐ in accordance with Pressure Equipment Directive 97/23/EC
☐ in accordance with ATEX Directive 94/9/EC

The manufacturer

Bosch Rexroth Electric Drives and Controls GmbH
Bürgermeister-Dr.-Nebel-Straße 2
97816 Lohr a. Main / Germany

hereby declares that the product below

Name:	Optional module “Safe Motion”
Type:	CSH01.*…-S2-…; CDB01.*…-S2-…; HAT01.*-…
From date of manufacture:	2010-01-01

was developed, designed and manufactured in compliance with the above-mentioned EU directive.

Harmonized Standards applied:

Standard	Title	Edition
EN ISO 13849-1	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design	2008
EN 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic contorl systems	2005
EN 61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements - Functional	2007
EN 60204-1	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	2006

Notified body that has conducted the EC type-examination procedure in accordance with the above-mentioned directive:

Name:	TÜV Rheinland Industrie Service GmbH
Address:	Alboinstr. 56, 12103 Berlin / Germany
Identification number:	0035
No of EC type-examination certificate:	01/205/0574/09

The individual below is authorized to compile the relevant technical files:

Name:	Christian Russo, Department DC-IA/EDY4
Address:	Bürgermeister-Dr.-Nebel-Str. 2, 97816 Lohr am Main / Germany

Further explanations:
The optional module “Safe Motion” has been implemented in accordance with SIL 2 according to EN 62061 / EN 61800-5-2 and Category 3 and PL d according to EN ISO 13489-1.

Place/date/signature as indicated in the original declaration.

We reserve the right to make changes to the content of the Declaration of Conformity. Current issue on request.

Page 1 / 1

Fig. 13-4: Translation of the Original Declaration of Conformity for the Optional Safety Technology Module "S2 - Safe Motion"

14 Service and support

Our worldwide service network provides an optimized and efficient support. Our experts offer you advice and assistance should you have any queries. You can contact us **24/7**.

Service Germany

Our technology-oriented Competence Center in Lohr, Germany, is responsible for all your service-related queries for electric drive and controls.

Contact the **Service Hotline** and **Service Helpdesk** under:

Phone:	**+49 9352 40 5060**
Fax:	**+49 9352 18 4941**
E-mail:	service.svc@boschrexroth.de
Internet:	http://www.boschrexroth.com/

Additional information on service, repair (e.g. delivery addresses) and training can be found on our internet sites.

Service worldwide

Outside Germany, please contact your local service office first. For hotline numbers, refer to the sales office addresses on the internet.

Preparing information

To be able to help you more quickly and efficiently, please have the following information ready:

- Detailed description of malfunction and circumstances
- Type plate specifications of the affected products, in particular type codes and serial numbers
- Your contact data (phone and fax number as well as your e-mail address)

15 Appendix

15.1 Optional safety technology modules

15.1.1 S2 - Safe Motion

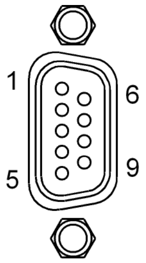
Description S2

The optional module allows different application-related safety functions, such as

- Safe stop 1 (Emergency stop)
- Safe stop 1
- Safe stop 2
- Safe maximum speed
- Safely-limited speed
- Safely-limited increment
- Safe direction
- Safely-monitored position
- Safely-limited position
- Safely-limited position, positive
- Safely-limited position, negative
- Safe homing procedure
- Safe braking and holding system
- Safely-monitored deceleration
- Safe communication
- Safe door locking
- Safe diagnostic outputs
- Safe inputs/outputs
- Safe parking axis
- Single-axis acknowledgment
- Safe stop 1 (braked)
- Safe stop 1 (braked Emergency stop)

☞ It is only possible to use the option in conjunction with an encoder (at slot X4 or X4.1 and X4.2).

X41, connection point safety technology S2

View	Identification	Function	
	X41	Safety technology S2	
D-Sub, 9-pin, female	**Unit**	**Min.**	**Max.**
Connection cable Stranded wire	mm^2	0.25	0.5

Tab. 15-1: Function, pin assignment, properties

Function		Signal	Connection	Nominal data	Technical data
Input/output forced dynamization	Digital input	IO30	1	24 V / 3 mA	Digital inputs type A (standard) [2)]
	Digital output			24 V / 0.5 A	Digital outputs [3)]
Input/output acknowledgment	Digital input	IO20	2	24 V / 3 mA	Digital inputs type A (standard) [2)]
	Digital output			24 V / 0.5 A	Digital outputs [3)]
Input/output / relay contact diagn. message / door locking	Digital input	IO10n	3	24 V / 3 mA	Digital inputs type A (standard) [2)]
	Digital output			24 V / 0.5 A	Digital outputs [3)]
	N/O contact			DC 24 V / 1A	Relay contact type 3 [4)]
Digital inputs	Operation mode selection	I1n	4	24 V / 3 mA	Digital inputs type A (standard) [2)]
		I2n	5		
		I3n	6		
		I4n	7		

Function		Signal	Connection	Nominal data	Technical data
Power supply of **isolated** inputs and outputs [1]		+24V	8	DC 24 V	DC 19.2 … 30 V Min. 0.1 A Max. 1.6 A (depending on load of outputs)
		0 VE	9		

[1] The maximum current consumption depends on the required current at the outputs IO10n, IO20 and IO30 (3 × 0.5 A + 0.1 A = 1.6 A).

2) See index entry "Digital inputs → Technical data"

3) See index entry "Digital outputs → Technical data"

4) See index entry "Relay contact → Type 3"

Tab. 15-2: Pin assignment

Accessories

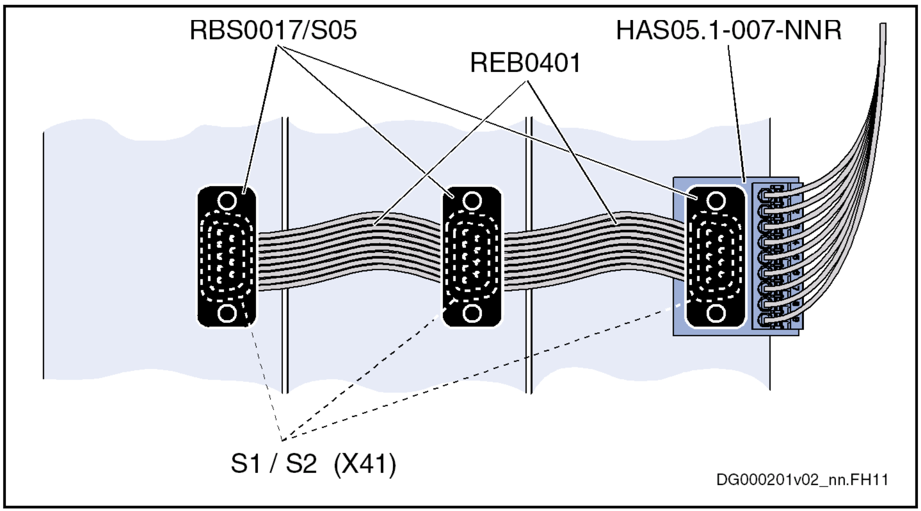
For the connection X41, there is the accessory "**HAS05.1-007**, adapter from D-Sub to terminal connector" .

For the connections of involved X41 via ribbon cable, there are the accessories

- **RBS0017/S05**, D-Sub connector for ribbon cable
- **REB0401**, ribbon cable

Wiring Example With HAS05.1-007-NNR

HAS05.1-007-NNR is the preferred adapter for the bus connection of several optional modules S1 or S2.



RBS0017/S05 D-Sub connector with connection for ribbon cable
REB0401 Ribbon cable

Fig. 15-1: HAS05.1-007-NNR

At CSH01.1C control sections, the adapter HAS05.1-007-NNL can only be used at the left end of the bus connection, when option 3 has not been equipped.

Note on Commissioning

If you wire the connection X41 via ribbon cable, you must deactivate the "safe feedback for channel 2" for the slave axes.

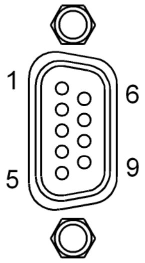
See also Parameter Description "P-0-3210, Safety technology configuration".

15.1.2 L2 - Safe Torque Off

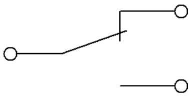
Description

The optional module is used for the safety function "Safe torque off".

X41, connection point "Safe Torque Off" L2

View	Identification	Function	
	X41	"Safe Torque Off" L2	
D-Sub, 9-pin, female	**Unit**	**min.**	**max.**
Connection cable Stranded wire	mm^2	0.25	0.5

Tab. 15-3: Function, pin assignment, properties

Function		Signal	Connection	Nominal data	Technical data
Inverted acknowledgment		STO Q2	6	DC 24 V / 1 A	Relay contact type 3 [1]
Supply for acknowledgment potential		STO Q	4		
Acknowledgment		STO Q1	5		
Control signal "Safe Torque Off" assignment A		STO A	1	24 V / 3 mA	Digital inputs type A (standard) [2]
Inverted control signal "Safe Torque Off"		STO n	2		
Control signal "Safe Torque Off" assignment B		STO B	3		
Reference voltages of the isolated inputs "STO A", "STO B", "STO n"		+24V	8	DC 24 V	DC 19.2 … 30 V Min. 0.1 A
		0VE	9		
n. c.			7		

[1] See index entry "Relay contact → Type 3"

[2] See index entry "Digital inputs → Technical data"

Tab. 15-4: Pin assignment

Function

STO	STO n	State	STO Q1	STO Q2
1	0	"Safe torque off" active	= STO Q	Open
0	1	"Safe torque off" not active	Open	= STO Q

STO	STO n	State	STO Q1	STO Q2
0	0	Selection error "Safe torque off"	Open	= STO Q
1	1			

Tab. 15-5: Function

Connection accessories

The bus wiring is **not** suited for multiple "L2" options.

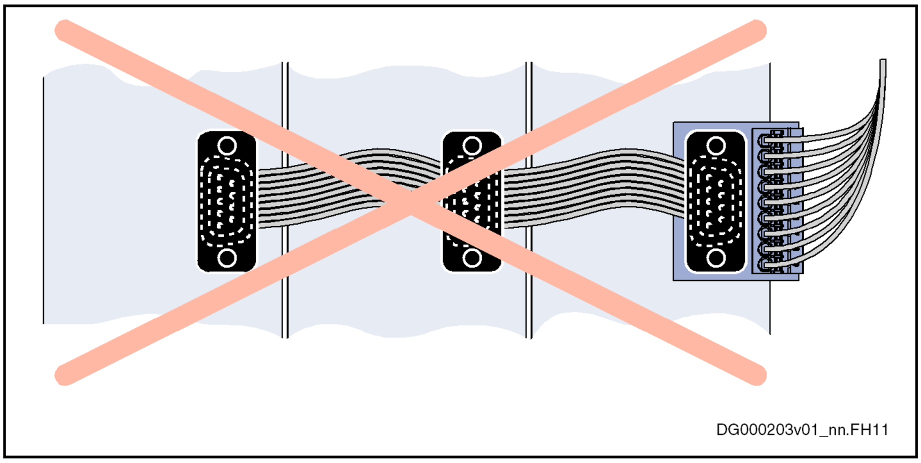


Fig. 15-2: No bus wiring for multiple L2 options

For wiring with single cores, use the ready-made cable **RKS0001** (D-Sub connector for single wire ends) or the adapter **HAS05.1-007-NNR** .

Commissioning information

Via the ribbon cable, the signals of all involved connection points X41 are connected in parallel. Differentiated evaluation is impossible with N/O contacts (STO Q, STO Q1) connected in parallel.

Feedback for all N/C contacts (STO Q, STO Q2) connected in parallel is allowed via one channel, if the "supply for acknowledgment potential" (STO Q) signal has been designed in dynamized form.

15.2 Technical data of the digital inputs/outputs and relay contacts

15.2.1 Digital Inputs Type A (Standard)

The digital inputs correspond to IEC 61131.

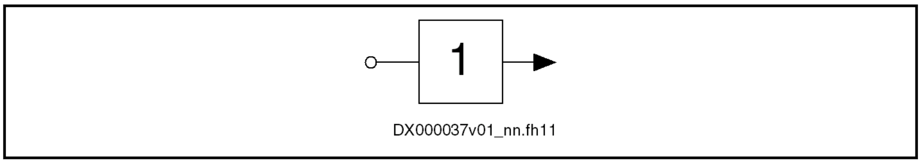


Fig. 15-3: Symbol

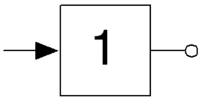
Data	Unit	Min.	Typ.	Max.
Allowed input voltage	V	-3		30
On	V	15		
Off	V			5

Data	Unit	Min.	Typ.	Max.
Input current	mA	2		5
Input resistance	kΩ	Non-linear; varies depending on input voltage		
Sampling frequency	kHz	Depending on firmware		
Control delay	µs	20		100 + 1 cycle time of position control

Tab. 15-6: *Digital Inputs Type A*

15.2.2 Digital Outputs

The digital outputs correspond to IEC 61131.



DX000038v01_nn.fh11

Fig. 15-4: Symbol

Data	Unit	Min.	Typ.	Max.
Output voltage ON	V	U_{ext} - 0.5	24	U_{ext}
Output voltage OFF	V			2,1
Output current OFF	mA			0,05
Allowed output current per output	mA			500
Allowed output current total or per group	mA			1000
Update interval	ns	Depending on firmware		
Short circuit protection		Present		
Overload protection		Present		
Allowed energy content of connected inductive loads, e.g. relay coils; only allowed as single pulse	mJ			400

Tab. 15-7: *Digital Outputs*

☞ The digital outputs have been realized with high-side switches. This means that these outputs can actively supply current, but not sink it.

☞ The energy absorption capacity of the outputs is used to limit voltage peaks caused when inductive loads are switched off.

Limit voltage peaks by using free-wheeling diodes directly at the relay coil.

15.2.3 Relay Contact Type 3

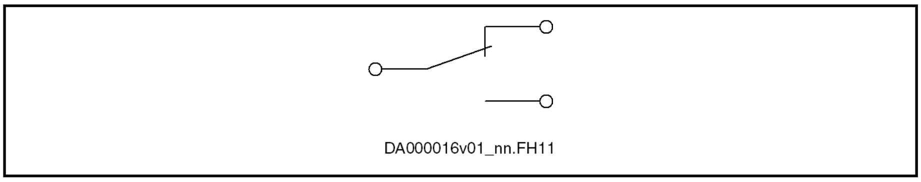


Fig. 15-5: Relay Contact

Data	Unit	Min.	Typ.	Max.
Current carrying capacity	A			DC 1
Voltage load capacity	V			DC 30
Minimum load of the contacts	mA	10		
Contact resistance at minimum current	mΩ			1000
Switching actions at maximum electric load[1]			1×10^6	
Number of mechanical switching cycles			1×10^7	
Pick up delay	ms			10
Drop out delay	ms			10

[1] Only the number of mechanical switching cycles is relevant to the relays of the optional safety technology modules

Tab. 15-8: Relay Contacts Type 3

15.3 HAT01 - Control Module for Holding Brake

15.3.1 Brief Description, Usage and Design

Brief Description The control module HAT01 belongs to the Rexroth IndraDrive product range and is used for the "Safe braking and holding system".

HAT01 control modules are mounted on a top-hat rail in the control cabinet.

Usage The types are used as follows:

Type	Usage
HAT01.1-002-NNN-NN	To control an electrically releasing, redundant holding brake.

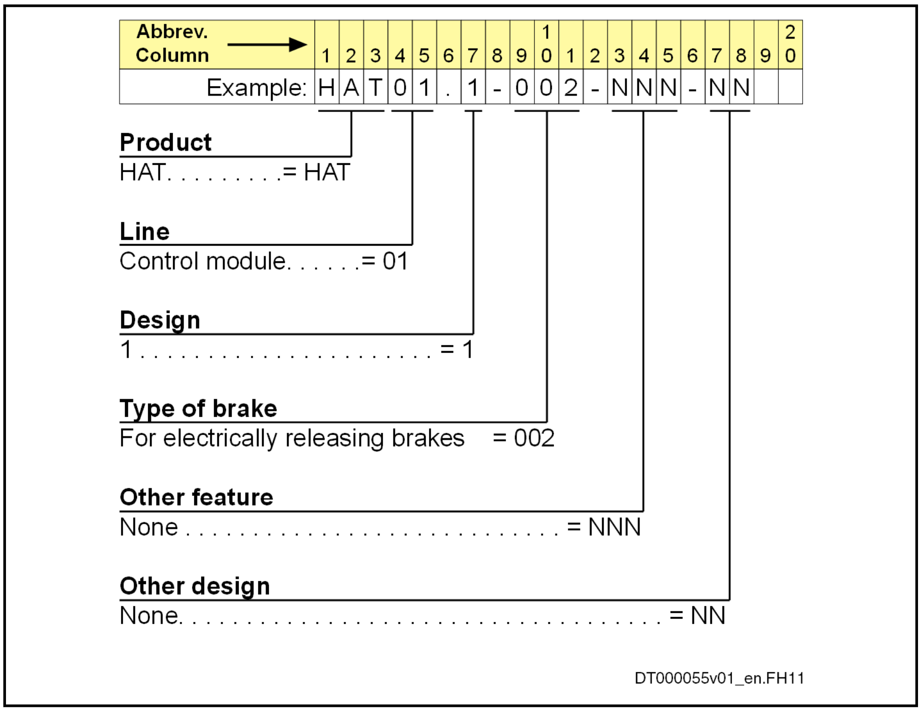
Tab. 15-9: Usage

15.3.2 Type Code and Identification

Type Code

☞ The figure illustrates the basic structure of the type code. Our sales representative will help you with the current status of available versions.

Appendix



Abbrev. Column →	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20
Example:	H	A	T	0	1	.	1	-	0	0	2	-	N	N	N	-	N	N		

Product
HAT. . . . .= HAT

Line
Control module. . . . . .= 01

Design
1 . . . . = 1

Type of brake
For electrically releasing brakes = 002

Other feature
None . . . . = NNN

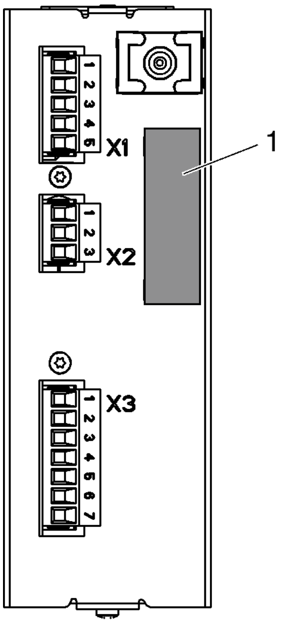
Other design
None. . . . . = NN

DT000055v01_en.FH11

Fig. 15-6: Type Code

Identification

Type Plate Arrangement

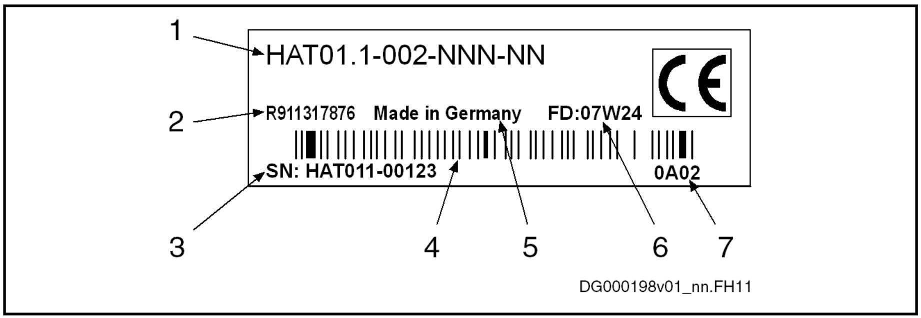


DG000197v01_nn.FH11

1 Type plate

Fig. 15-7: Type Plate Arrangement

Type Plate



1	Device type
2	Part number
3	Serial number
4	Bar code
5	Country of manufacture
6	Production week, 07W24 meaning year 2007, week 24
7	Hardware index

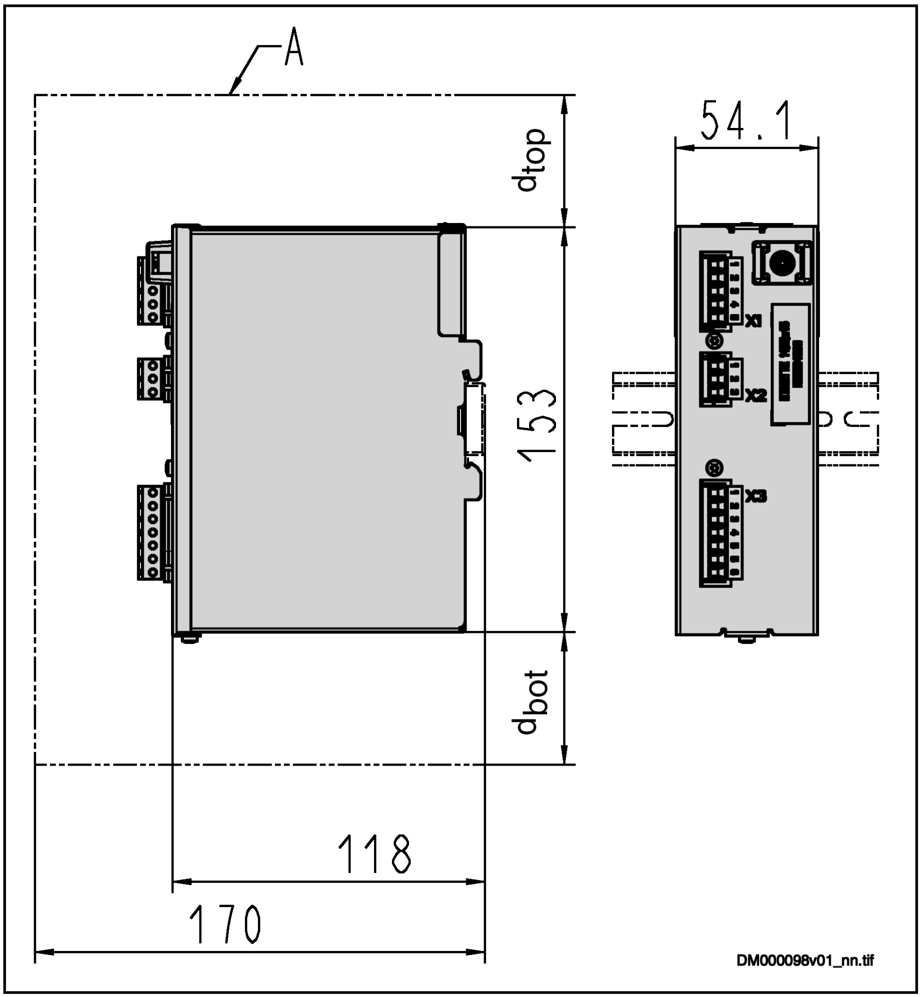
Fig. 15-8: Type Plate

15.3.3 Scope of Supply

The scope of supply of the control module HAT01 contains:

- Connectors X1, X2, X3

15.3.4 Dimensions



All dimensions in mm

A Minimum mounting clearance

d_{top}, d_{bot} See table "Technical Data"

Fig. 15-9: Dimensions

15.3.5 Technical Data

Technical Data

Description	Symbol	Unit	HAT01.1-002-NNN-NN
Weight	m	kg	0,6
Degree of protection			IP20
Allowed mounting position			Vertical
Minimum distance from the top of the device[5]	d_{top}	mm	50
Minimum distance from the bottom of the device[6]	d_{bot}	mm	50
Minimum distance on the side of the device	d_{hor}	mm	-
Allowed ambient temperature range	T_{a_work}	°C	0 … 55
Cooling type[3]			n

Description	Symbol	Unit	HAT01.1-002-NNN-NN
Listing according to UL standard (UL)			UL 508C
UL files (UL)			E134201
Control voltage supply			
Rated control voltage input (UL)[1)]	U_{N3}	V	Brake cable length < 50 m: 24 ±5% Brake cable length > 50 m: 26 ±5%
Maximum allowed voltage for 1 ms[2)]	U_{N3_max}	V	33
Rated power consumption control voltage input at U_{N3} (UL)	P_{N3}	W	1,5
Inrush current at 24V supply	I_{EIN3}	A	35
Pulse width of I_{EIN3}	$t_{EIN3Lade}$	ms	4
Input capacitance	C_{N3}	mF	3,6
Power dissipation	P_{Diss}	W	Max. 7.5 (brake controlled)
Output current	I_{Br}	A	See "X2, Output to Brake"

1) Observe supply voltage for holding brake
2) See following note regarding overvoltage
3) n: Natural convection; f: Forced cooling
5) 6) 7) See fig. "Air Intake and Air Outlet at Device"

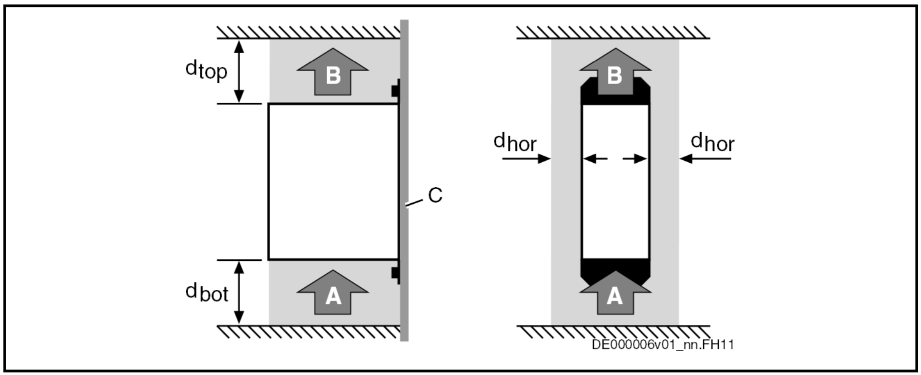
Tab. 15-10: HAT01 - Technical Data

☞ **Overvoltage** of more than 33V has to be discharged by means of the appropriate electrical equipment of the machine or installation.

This includes:

- 24V power supply units that reduce incoming overvoltages to the allowed value.
- Overvoltage limiters at the control cabinet input that limit existing overvoltage to the allowed value. This, too, applies to long 24V lines that have been run in parallel to power cables and mains cables and can absorb overvoltages by inductive or capacitive coupling.

Distances

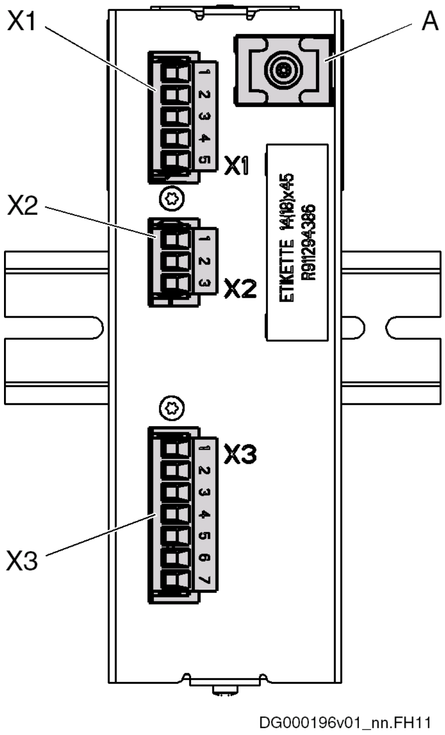


A	Air intake
B	Air outlet
C	Mounting surface in control cabinet
d_{top}	Distance top
d_{bot}	Distance bottom
d_{hor}	Distance horizontal

Fig. 15-10: Air intake and air outlet at device

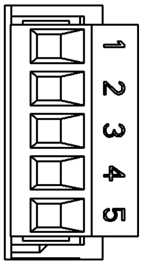
15.3.6 Connection Points

Front View

Front view	Connection point	Description
 X1 A 1 2 3 4 5 X1 X2 1 2 3 X2 ETIKETTE 141(8)x45 R911294386 X3 1 2 3 4 5 6 7 X3 DG000196v01_nn.FH11	X1	24 V power supply (24V, 0V)
	X2	Output to brake
	X3	Signal exchange with control section; connection with ready-made cable **RKS0007**
	A	Strain relief: Fix connection cable with cable tie

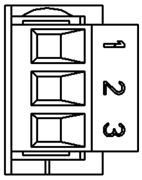
Tab. 15-11: Connection Points

X1, 24 V Power Supply

Pin assignment	Connection	Signal name	Function
 DA000230v01_nn.FH11	X1.1	+24V	Power supply and "looping through"
	X1.2	+24V	
	X1.3	0V	Reference potential for power supply and "looping through"
	X1.4	0V	
	X1.5	-	Housing potential
Screw connection at connector	**Unit**	**Min.**	**Max.**
Tightening torque	Nm	0,5	0,6
Connection cable stranded wire	mm^2	1,0	2,5
Connection cable	AWG	18	14
Power consumption	W	See P_{N3}	
Voltage load capacity	V	See U_{N3}	
Current carrying capacity "looping through" from +24V to +24V, 0V to 0V	A		6 (max. 1 other HAT01 for operation with HMD01)
Polarity reversal protection	-	Within the allowed voltage range by internal protective diode	

Tab. 15-12: Function, Pin Assignment, Properties

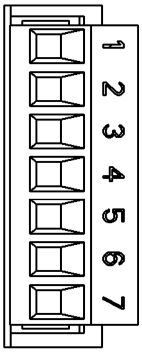
X2, Output to Brake

Pin assignment	Connection	Signal name	Function
 DA000231v01_nn.FH11	X2.1	Br+	Connection to positive pole of holding brake
	X2.2	Br-	Connection to negative pole of holding brake
	X2.3	-	Housing potential HAT01 (connection for cable shield)
Screw connection at connector	**Unit**	**Min.**	**Max.**
Tightening torque	Nm	0,5	0,6
Connection cable stranded wire	mm^2	1,0	2,5
Connection cable	AWG	18	14
Output current I_{Br_cont}	A		6
Output current I_{Br_max}; $t \leq 1$ s; $I_{AV} \leq I_{Br\_cont}$	A		7,5

Output voltage U_{Br}	V	U_{N3} - 0.5 V	U_{N3}
Output protection	-	Short-circuit proof and overload-proof within the allowed voltage range	

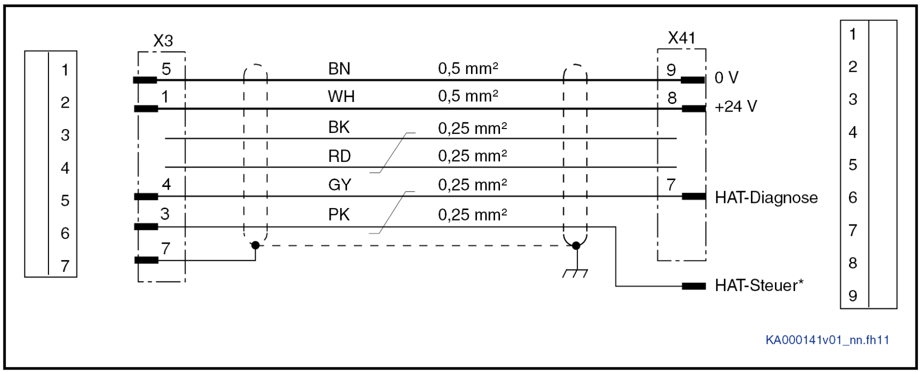
Tab. 15-13: Function, Pin Assignment, Properties

X3, Signal Exchange with Control Section

Pin assignment	Connection	Signal name	Function
 DA000234v01_nn.FH11	X3.1	+24V	Power supply of isolated inputs/outputs X3.3 and X3.4 with 24 V / 0.1 A
	X3.2	+24V	
	X3.3	HAT-Steuer	Input for brake control via U_{Br} (X2)
	X3.4	HAT-Diagnose	Output HAT-Diagnose
	X3.5	0V	Reference potential for power supply at X3.1
	X3.6	0V	
	X3.7	-	Connection for cable shield
Screw connection at connector	**Unit**	**Min.**	**Max.**
Tightening torque	Nm	0,5	0,6
Connection cable stranded wire	mm^2	1,0	2,5
Connection cable	AWG	18	14
Allowed cable length	m		3
Input X3.3 controls output Br+/Br- (X2) (dynamized input)		250 Hz ±20%, duty cycle ~50% → "H" level at output Br (X2) "H" level → "L" level at output Br (X2) "L" level → Error state: "L" level at output Br (X2)	
Output voltage at X3.4 shows status of controlled brake	V	Brake applied: 150 Hz ±20% Brake released: "H", (max. X3.1 - 0.5 V) Brake faulty: "L"	
Ready-made connection cable	-	RKS0007	

Tab. 15-14: Function, Pin Assignment, Properties

Interconnection Diagram RKS0007



* Connection between HAT01 (X3) and control section (X41 [HAT-Diagnose], X32 [HAT-Steuer])

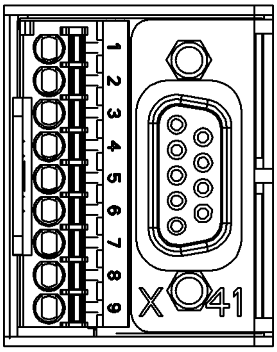
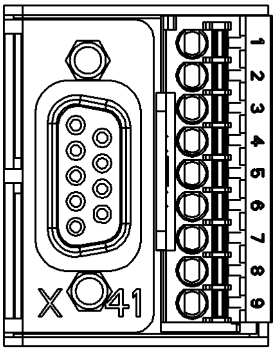
Fig. 15-11: Interconnection Diagram RKS0007

15.4 HAS05.1-007, Adapter From D-Sub to Terminal Connector

15.4.1 Use

The adapter **HAS05.1-007** exists in the following types of design:

- **NNL:** Mounting direction left (outgoing direction spring terminal left)
- **NNR:** Mounting direction right (outgoing direction spring terminal right)

HAS05.1-007-	
NNL	NNR
 DA000233v01_nn.FH11	 DA000220v01_nn.FH11

Tab. 15-15: Types of Design

Assignment

The accessory HAS05.1-007 can be used at the following control sections:

HAS05.1-007-NNL	HAS05.1-007-NNR
CSH01.1C at X41 (Condition: Option 3 not equipped)	CSH01.1C at X41
CDB01.1C at X41.1 (option ST1)	CSH01.2C at X41 CSH01.3C at X41
	CDB01.1C at X41.2 (option ST2)

Tab. 15-16: Assignment HAS05.1-007

At **CDB01** control sections, you can use both types of design together. However, there is the following restriction:

When using the type of design NNL at HMD01.1N-W0012 or HMD01.1N-W0020 drive controllers of a width of 50 mm, you cannot use the adapter of type of design NNR at the neighboring control section on the left-hand side.

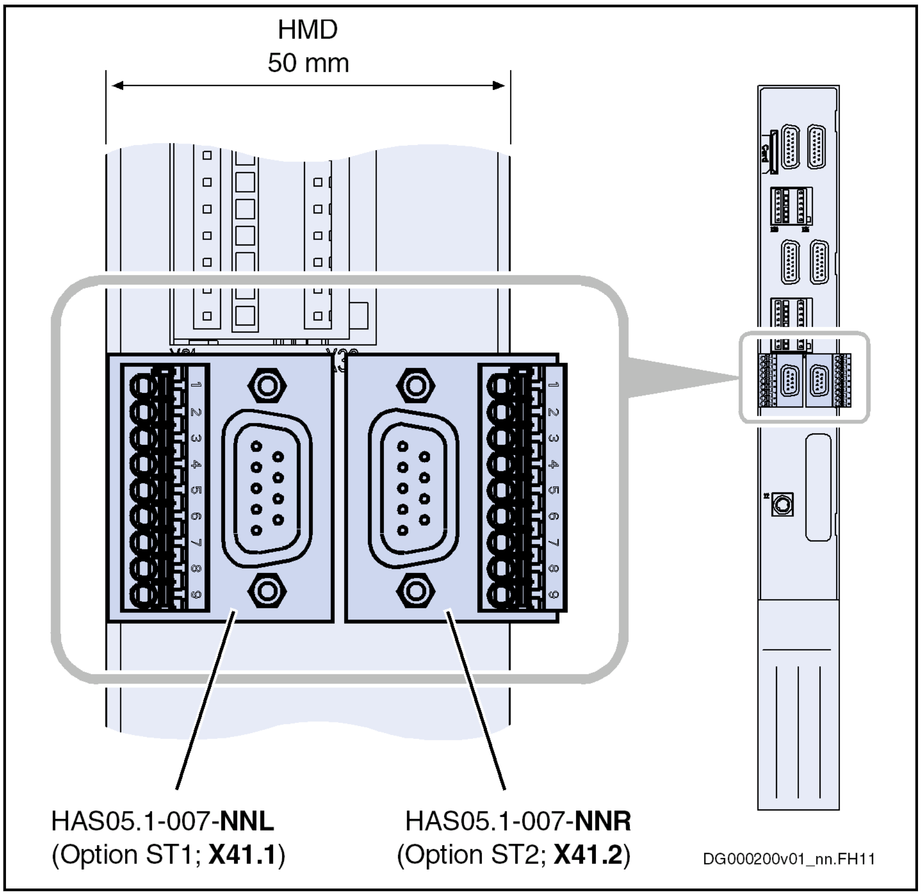


Fig. 15-12: HAS05.1-007-NNL and -NNR at HMD Drive Controller of a Width of 50 mm

Function

Universal adapter for safety technology

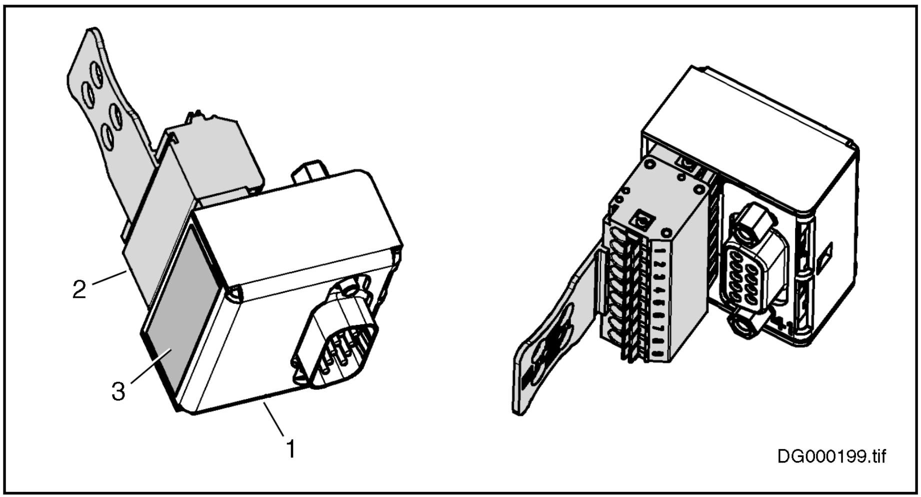
Usage:

1. Converter of D-Sub connection to terminal connection for an axis
2. Connection of additional component HAT01 to the optional module S1 or S2
3. Converter of D-Sub connection to terminal connection for bus connection of optional modules S1 or S2 of the axes of one zone (see figure "Wiring Example With HAS05.1-007-NNR" on page 305)

Identification, Parts

The accessory has a type plate for identification.

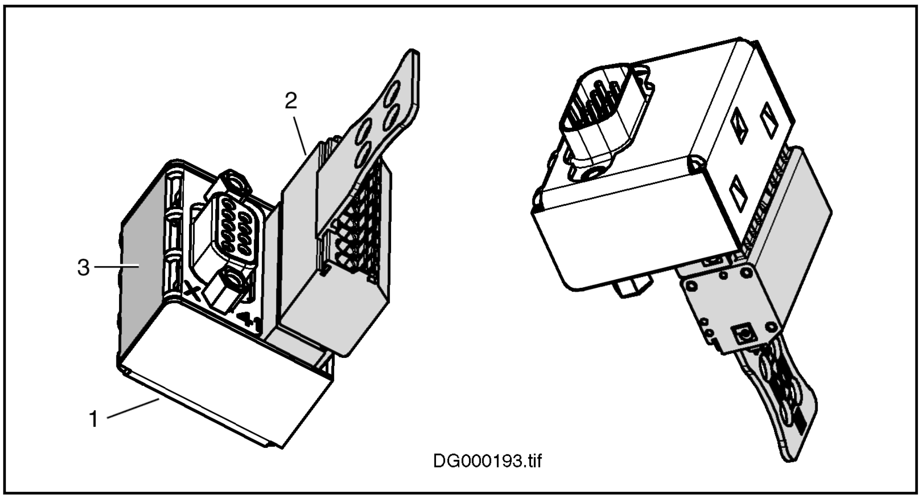
HAS05.1-007-NNL



1	Adapter
2	Connector (spring terminal)
3	Type plate

Fig. 15-13: HAS05.1-007-NNL

HAS05.1-007-NNR



1	Adapter
2	Connector (spring terminal)
3	Type plate

Fig. 15-14: HAS05.1-007-NNR

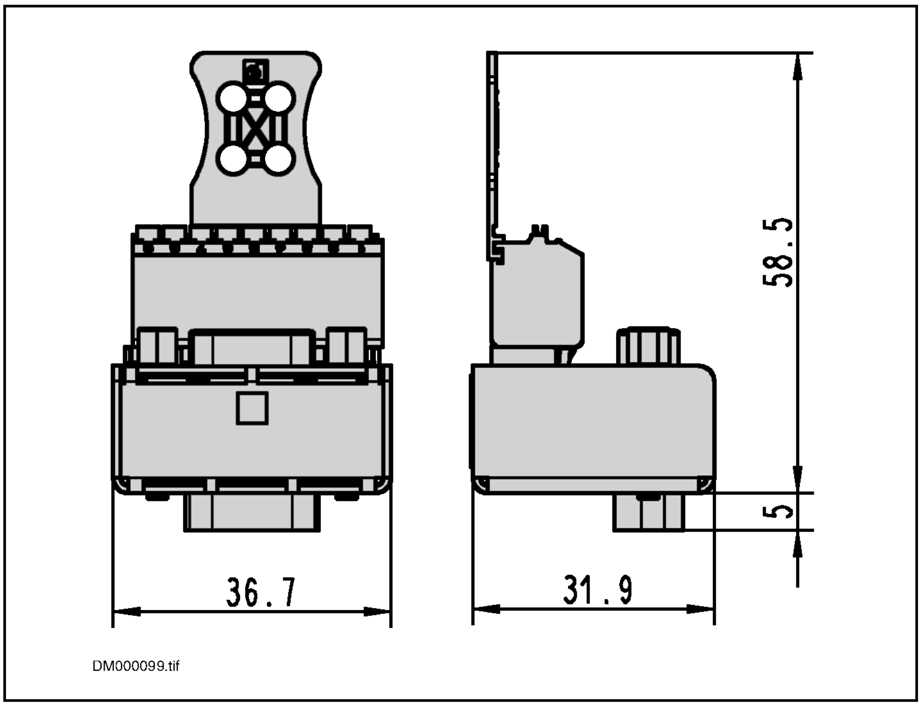
The adapter is plugged in the connection point X41 (resp. X41.1 or X41.2 for double-axis devices) of the control section and secured with screws (screw tightening torque: 0.5 Nm).

15.4.2 Technical Data

Mounting Dimensions

The accessory requires the following mounting clearance at the drive controller.

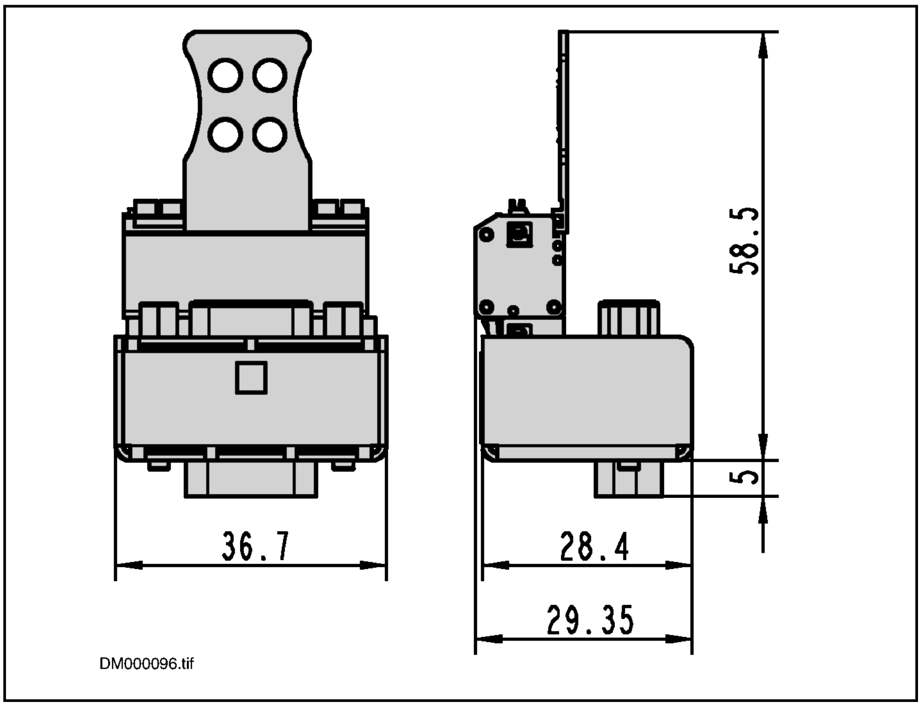
HAS05.1-007-NNL



Data in mm

Fig. 15-15: Mounting Dimensions HAS05.1-007-NNL

HAS05.1-007-NNR

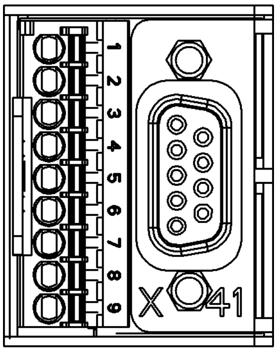
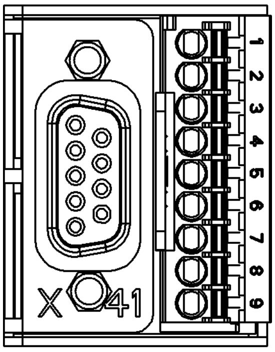


Data in mm

Fig. 15-16: Mounting Dimensions HAS05.1-007-NNR

☞ Observe the minimum bending radiuses of the lines used. This requires additional mounting clearance at the front of the drive controller.

Connection Point X41

View	Connection (terminal)	Signal name	Function
HAS05.1-007-**NNL** Spring terminal / D-Sub female connector  DA000233v01_nn.FH11 HAS05.1-007-**NNR** D-Sub female connector / spring terminal  DA000220v01_nn.FH11	1	X41.1	The adapter brings the connections of X41 to the connections 1-9 of a spring terminal and a D-Sub female connector. 🕮 Description of connection point X41: See Project Planning Manual "Rexroth IndraDrive Control Sections", section "Optional Modules for Control Sections, Safety Technology".
	2	X41.2	
	3	X41.3	
	4	X41.4	
	5	X41.5	
	6	X41.6	
	7	X41.7	
	8	X41.8	
	9	X41.9	

Spring terminal (connector)	Unit	Min.	Max.
Cable cross section stranded wire	mm^2	0,5	1,5
Cable cross section	AWG	20	16
Coding	At both types of design, the connection point 5 has been coded, i.e. provided with a coding section. The spring terminal was already assembled accordingly at the factory.		

Electrical Data	Description of connection point X41: See Project Planning Manual "Rexroth IndraDrive Control Sections", section "Optional Modules for Control Sections, Safety Technology".
• Mating connector for D-Sub female connector • Ribbon cable	• **RBS0017/S05** → D-Sub connector, 9-pin (Screw tightening torque: 0.5 Nm) • **REB0401** → Ribbon cable, 9-pin, can be ordered in steps of 0.1 m For professional assembly of the ribbon cable in the D-Sub connector, use the following Tyco tools: • Pistol-Grip tool (part number 734155-1) • Matrix for D-Sub connector (part number 734148-1)

Tab. 15-17: Function, Pin Assignment

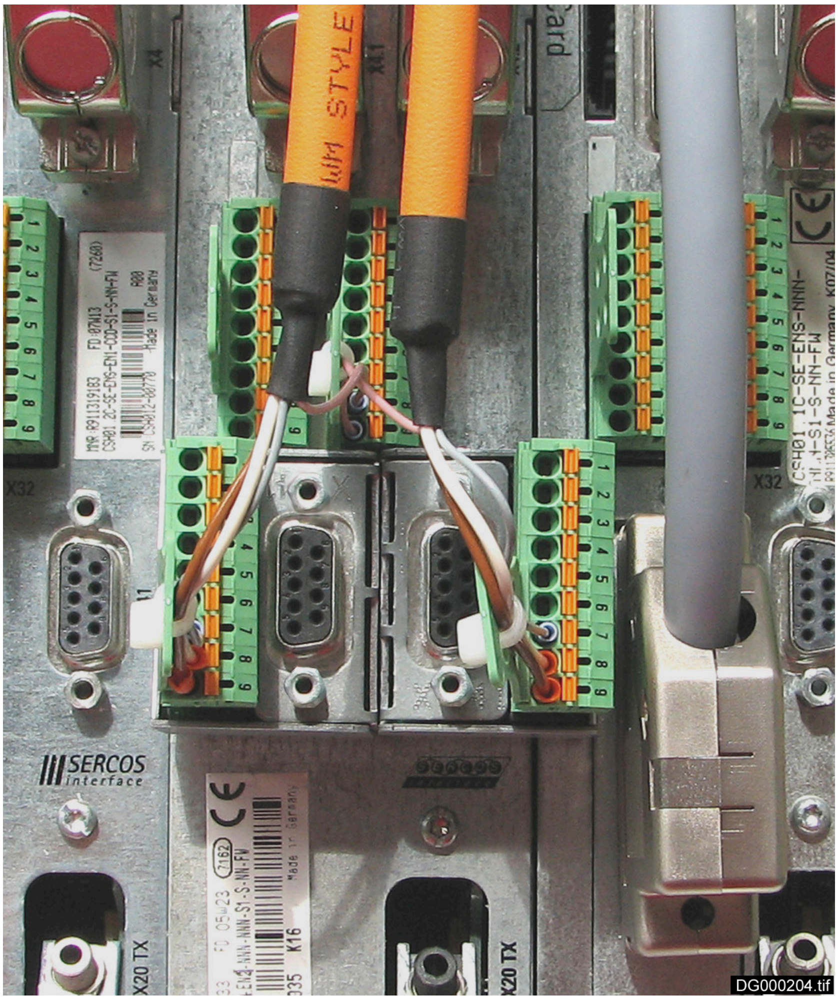
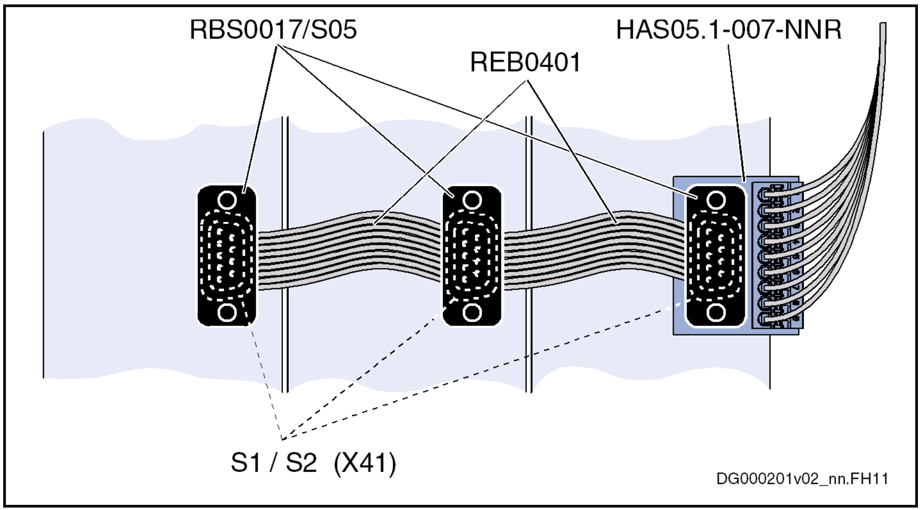


Fig. 15-17: HAS05.1-007-NNL and HAS05.1-007-NNR at CDB Control Section

Wiring Example With HAS05.1-007-NNR

HAS05.1-007-NNR is the preferred adapter for the bus connection of several optional modules S1 or S2.



RBS0017/S05	D-Sub connector with connection for ribbon cable
REB0401	Ribbon cable

Fig. 15-18: HAS05.1-007-NNR

At CSH01.1C control sections, the adapter HAS05.1-007-NNL can only be used at the left end of the bus connection, when option 3 has not been equipped.

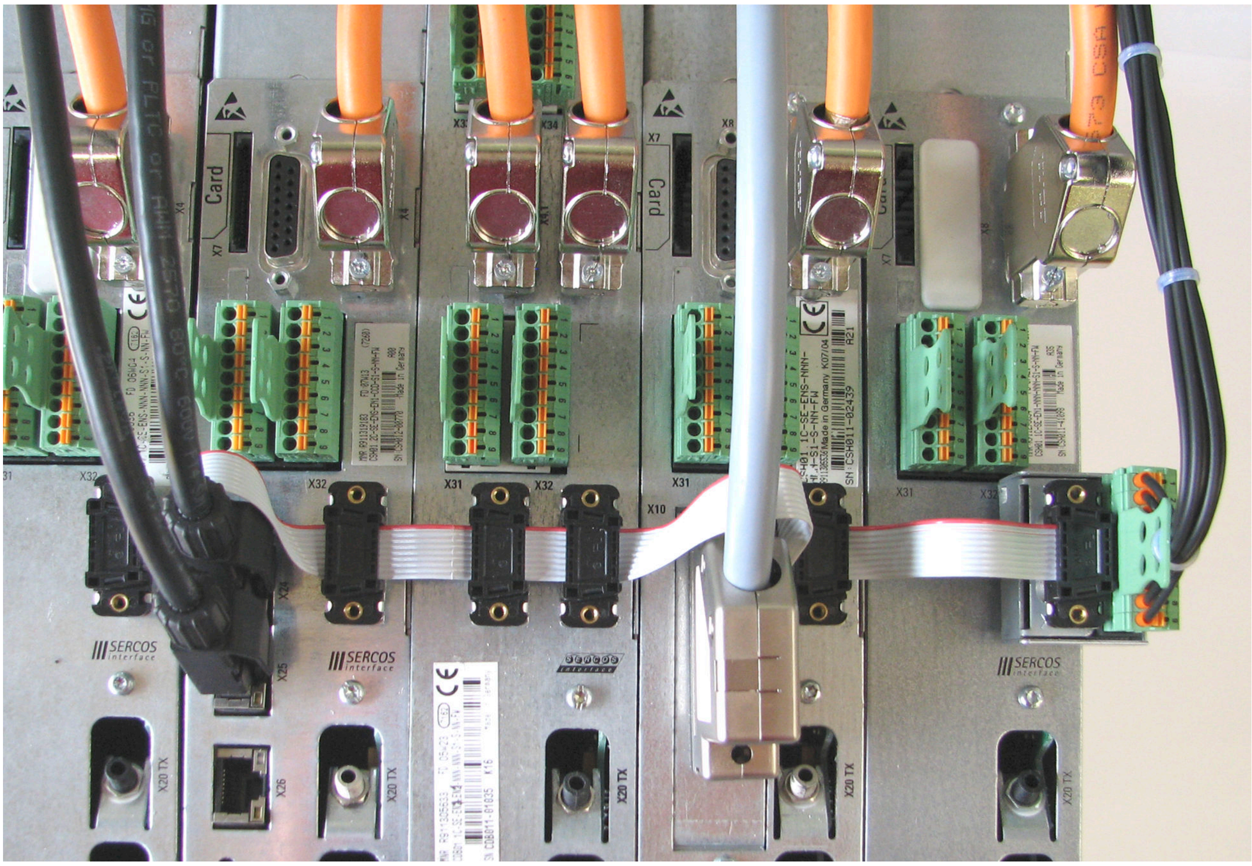


Fig. 15-19: HAS05.1-007-NNR, RBS0017/S05 and REB0401 for Bus Connection of Optional Modules S1 or S2 of the Axes of One Zone

Glossary

Accessories

The accessories are assigned to the corresponding device in order to support its functioning. For example, the basic accessories belong to each drive controller and supply unit to fasten them and connect them electrically.

Additional components

Additional components complement supply units, converters and inverters. Typical additional components are mains chokes, mains filters and braking resistors, for example.

Application software

Software specifically implemented in the machine by the manufacturer for the application; it usually contains logic sequences, limit values and expressions for controlling the corresponding inputs, outputs, calculations and decisions to comply with the necessary requirements of SRP/CS.

Appropriate use of a machine

Use of a machine in compliance with the information made available in the user information.

Basic control section circuit board

The basic control section circuit board is the main part of the control section. It has its own interfaces and, in the case of configurable control sections, additional optional slots for optional modules.

Cable

A cable is a combination of several strands which is kept together by the cable jacket. A typical type of cable is the cable for the motor connection.

Category

Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability (EN ISO 13849-1).

Closed-loop (CL)

Closed-loop describes the closed-loop-controlled operation of motors, for example with field-oriented control. This operation is possible both in sensorless form and with encoder and is distinguished with regard to its applications.

Sensorless, i.e. without additional encoder, for velocity control, for example by means of observer.

With encoder, i.e. with additional encoder, for velocity and position control of synchronous motors and asynchronous motors in field-oriented operation.

Combination

Combination refers to a combination of components which is formed via a common DC bus or common mains connection; components such as mains choke, mains transformer and mains filter are used in common.

Common DC bus

Voltage source backed up with powerful capacitors to supply drive controllers with power voltage. Common means that the DC bus connections of the involved devices are interconnected.

Configuration

Configuration describes a specific combination of optional modules to form a configured control section which is ideally suited for the intended application.

Control panel

The control panel is the complete unit for operation; it contains input and output elements, such as a key panel and a display.

Control section

The control section is a separate component which is plugged into the power section. The control section is the "brain" of the drive controller.

Converter, frequency converter

Drive controller which generates three-phase alternating voltage with variable amplitude and frequency from the mains voltage with fixed amplitude and frequency in order to set the speed of three-phase a.c. motors, for example. Contains the fundamental stages mains rectifier, DC bus and inverter.

Cross data comparison

For cross data comparison, the safety-relevant parameters and processes are checked in 2 independent systems (e.g. µC). If a discrepancy is detected, the system is shut down.

Dangerous failure

Failure having the potential to put the SRP/CS in a hazardous state or a malfunction.

NOTE 1: Whether this potential can be detected or not depends on the architecture of the system; a redundant system decreases the probability that a hazardous hardware failure causes a hazardous failure of the overall system.

NOTE 2: According to IEC 61508-4:1998, term 3.6.7.

Deactivation

"Stopping process" is the decrease of motion until standstill is reached. The procedure starts when the signal for stopping process is triggered and ends when the motion has come to a standstill.

Demand mode

[Demand mode (r_d); occurrence per time unit of demands on a safety-related reaction of an SRP/CS.

Diagnostic coverage (DC)

Measure for the effectiveness of the diagnosis, which can be determined as the relation of the failure rate of detected dangerous failures and the failure rate of the total of dangerous failures.

NOTE 1: The diagnostic coverage can apply to the entirety or to parts of the safety-related system. For example, there might be a diagnostic coverage for the sensors and/or the logic system and/or the actuators.

NOTE 2: According to IEC 61508-4:1998, term 3.8.6.

Display

The display is part of the control panel for visual output of information.

Drive controller

Device with which a motor can be operated. Umbrella term for converter or inverter.

Drive system

The drive system comprises all components from mains supply to motor shaft. It consists of the components supply unit, power section with control section incl. firmware, as well as motor and required additional components and corresponding system connections.

Dynamization

Optional module "Safe Motion" (S2): Dynamization is to detect static error states, so-called "sleeping errors", during safety function selection and in the safety-relevant circuits. Dynamization takes place, in certain time intervals, automatically in the background without having an effect on the safety function.

Electric drive system

An electric drive system comprises all components from mains supply to motor shaft; this includes, for example, electric motor(s), motor encoder(s), supply units and drive controllers, as well as auxiliary and additional components, such as mains filter, mains choke and the corresponding lines and cables.

Embedded software (firmware, system software)

Software which is supplied by the control unit manufacturer as part of the system and which the user of the machine cannot modify.

NOTE: Embedded software is usually written in FVL.

EMERGENCY HALT (stopping process in case of an emergency)

An emergency operation which is destined to stop a process or motion that has become dangerous.

EMERGENCY HALT device

Manually operated control device which is used to trigger an EMERGENCY HALT function.

EMERGENCY ON (switch-on in case of an emergency)

An emergency operation which is destined to switch on the supply with electric energy to a part of an installation that is required for emergency situations.

Emergency operation

An emergency operation includes individually or in combination:

- EMERGENCY HALT (stopping process in case of an emergency)
- EMERGENCY START (start in case of an emergency)
- EMERGENCY STOP (switch-off in case of an emergency)
- EMERGENCY ON (switch-on in case of an emergency)

EMERGENCY START (start in case of an emergency)

An emergency operation which is destined to start a process or motion in order to remove or prevent a dangerous situation.

EMERGENCY STOP (switch-off in case of an emergency)

An emergency operation which is destined to switch off the supply with electric energy to an entire installation or part of an installation, wherever there is a risk of electric shock or another risk of electric origin.

EMERGENCY STOP device

Manually operated control device which causes the electric energy supply to an entire installation or part of an installation to be switched off, wherever there is a risk of electric shock or another risk of electric origin.

Enabling control

"Enabling control" is to be understood as an "enabling control device" according to EN 60204-1:2006, chapter 10.9.

The enabling control is an additional manually actuated control device with 2 or preferably 3 positions and automatic reset. It is used in connection with a start control (hold-to-run pushbutton) that requires continuous actuation in order to enable motion.

Equipment grounding conductor

The equipment grounding conductor establishes the conductive connection from the connection point of the equipment grounding conductor of the component to the equipment grounding system.

Equipment grounding conductor connection point

The connection point of the equipment grounding conductor is the connection point at which the equipment grounding conductor is fixed to the component; the connection point is identified with the ⏚ icon.

Equipment grounding system

The equipment grounding system is the entire equipment by which the equipment grounding conductors of components are connected to the equipment grounding conductor of the mains. In the majority of cases, an earth-circuit connector belongs to the equipment grounding system.

Failure

Termination of the ability of an item to perform a required function [IEC 60050-191:1990, 04-01].

NOTE 1: After failure, the item has a fault.

NOTE 2: "Failure" is an event, as distinguished from "fault", which is a status.

NOTE 3: The concept as defined does not apply to items consisting of software only.

NOTE 4: Failures which only concern the availability of the process to be controlled are not within the field of application of this part of ISO 13849.

Fault

State of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources (IEC 60050-191:1990, 05-01).

NOTE 1: A fault is often the result of a failure of the item itself, but may exist without prior failure.

NOTE 2: In this part of ISO 13849, the term "fault" means random fault.

FIT

"FIT" is the abbreviation of the unit "Failure in Time ". It describes the failure rate of technical components, in particular of electronic parts. "FIT" specifies the number of parts which fail in 10^9 hours.

Forced dynamization

Optional module "Safe Torque Off" (L2): Forced dynamization is to detect static error states, so-called "sleeping errors", during safety function selection and in the interrupting circuits. Both the control section in standard design and the optional safety technology module "L2" have their own interrupting circuits. Forced dynamization takes place by the machine operator selecting the safety function "Safe torque off" and must be carried out in certain time intervals.

Full variability language (FVL)

Type of language having the ability to cover and implement a big range of functions (EXAMPLE C, C++, Assembler).

NOTE 1: According to IEC 61511-1:2003, term 3.2.80.1.3.

NOTE 2: Typical example of systems using FVL: Embedded systems.

NOTE 3: In the field of machines, FVL is used in embedded software and occasionally in application software.

Guard (EN ISO 12100-1)

A guard is the part of a machine that is used as a kind of physical barrier to provide protection for people. Depending on its design, the guard can be a casing, cover, shield, door, enclosing guard, etc.

Hazardous situation

The hazardous situation is a 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 [ISO 12100-1:2003, 3.9].

Hold-to-run control

The hold-to-run control is a control device that requires continuous actuation of the control element in order to enable motion. The hold-to-run pushbutton is a control device with automatic reset.

Hybrid cable

In the hybrid cable, both electrical signals are transmitted on copper wires and optical signals are transmitted on fiber optic cables.

Integrated safety technology

"Integrated safety technology" includes the hardware and software features that allow making available safety-relevant drive functions. A maximum of safety for persons and machines can therefore be made available.

MPx06 and below: The integrated safety technology is state-of-the-art for safety-relevant control units of Category 3 according to EN 954-1 in the field of high-dynamic drives.

MPx07 and above: The integrated safety technology is state-of-the-art for safety-relevant control units of Category 3 PL d according to EN ISO 13849-1 and SIL 2 according to EN 62061 (Safe Motion) or Category 3 PL d/e according to EN ISO 13849-1 and SIL 2/SIL 3 according to EN 62061 (Safe Torque Off) in the field of high-dynamic drives.

Interlocking guard with guard locking (EN ISO 12100-1)

The interlocking guard with guard locking ensures that:

- The hazardous machine functions "covered" by the guard cannot operate until the guard is closed and locked and

- The guard remains closed and locked, even if a halt command was triggered, until the risk of injury due to the hazardous machine functions has disappeared and

- The hazardous machine functions, when the guard is closed and locked, can operate, but the closure and locking of the guard do not by themselves start the hazardous machine functions

Interrupting circuit

An interrupting circuit is the point of access that can be used for switching the drive or installation off. In the case of drive controllers, the interrupting circuit is used, for example, for switching off the output stage.

NOTE: Switching off in a safe way requires 2 interrupting circuits.

Inverter

Device which generates three-phase alternating voltage with variable amplitude and frequency from the DC bus direct voltage.

Key panel

The key panel is part of the control panel. For example, converters can be controlled via the keys of the key panel.

Limited variability language (LVL)

Type of language having the ability to combine predefined, application-specific library functions to implement the specification of the safety requirements.

NOTE 1: According to IEC 61511-1:2003, term 3.2.80.1.2.

NOTE 2: Typical examples of LVL (ladder diagram, function block diagram) are given in IEC 61131-3.

NOTE 3: Typical example of a system using the LVL: PLC.

Line

A line consists of an electric conductor and its insulation. Sheathed lines are also called cables.

Machine control

System which reacts to input signals of parts of the machine, of the user, external control devices or any combination of these, and generates output signals so that the machine acts in the intended way.

NOTE: The machine control can use any technology or combination of different technologies (e.g. electric/electronic, hydraulic, pneumatic, mechanical).

Master communication

Master communication is the specific communication between hierarchical communication levels. By means of master communication, command variables (e.g., command values) are transmitted from a higher-level control unit to receivers, and actual values, for example, are transmitted back to the control unit.

Mean time to failure

[Mean time to failure ($MTTF_d$)]; expected value of the mean time to failure.

NOTE: According to IEC 62061:2005, term 3.2.34.

Mission Time

"Mission Time" is the specified cumulative operating time of the PDS(SR) during its entire service life.

Mode selector

The mode selector determines the operation mode relevant for safe operation, like for example:

- Normal operation (productive operation, automatic operation etc.) and

- Special mode (manual mode, tool or workpiece change and cleaning process)

The selected type of control has to be on a higher level than all other control functions - except for the one for the emergency control device. The mode selector can be replaced by other means of selection which allow only certain groups of operators to carry out certain machine functions (e.g., access code for certain numerical control functions etc.). Each position of the mode selector may only correspond to one control or operation mode [see Machinery Directive 98/37/EC or 2006/42/EC (as of 2009-12-29)].

Monitoring

Safety function which ensures that a protective measure is initiated when the ability of a component or element to fulfill its function is reduced, or the operating conditions are modified in such a way that the value of the risk reduction is reduced.

Open-loop (OL)

Open-loop describes the open-loop-controlled operation of asynchronous motors at frequency converters in V/Hz [U/f] operation without an encoder at the motor. This is the simplest operation of asynchronous motors.

Operating stop

Operating stop is the state in which the mechanical component is kept at rest and the motor is supplied with energy, i.e. it is under torque or under force.

Optional module

By means of optional modules, the configurable control sections are equipped with various functions. For example, there are optional modules for master communications, encoder evaluations, I/O extensions, safety technologies, control panels and storage media.

Optional slot

Slot into which an optional module can be plugged. Only configurable control sections have optional slots.

Performance Level (PL)

Discrete level which specifies the ability of safety-related parts of a control system to carry out a safety function under predictable conditions.

Power section

The power section is a separate component which contains all the important power elements of the drive controller.

Programmable electronic system (PES)

System for control, protection or monitoring, depending on its function based on one or more programmable electronic devices, including all elements of the system, such as power supplies, sensors and other input devices, actuators and other output devices.

NOTE: According to IEC 61508-4:1998, term 3.3.2.

Proof Test

The "Proof Test" (also called "periodical test") is a periodic test performed to detect failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition.

NOTE: According to IEC 61508-4:1998, term 3.8.5.

Protective measure

Measure intended to achieve risk reduction [EXAMPLE 1 Implemented by the designer: Inherently safe design, safeguarding and complementary protective measures, information for use. EXAMPLE 2 Implemented by the user: By organization (safe working procedures, supervision, permit-to-work systems), provision and use of additional safeguards (use of personal protective equipment; training)].

NOTE: According to ISO 12100-1:2003, term 3.18.

Reasonably foreseeable misuse

Use of a machine in a way not intended by the designer, but which may result from readily predictable human behavior.

Required performance level

[Required performance level (PL_r)]; performance level (PL) applied to achieve the required risk minimization for each safety function.

Residual risk

Residual risk is the risk remaining after protective measures have been taken (according to ISO 12100-1:2003, 3.12).

Risk

Combination of the probability of occurrence of harm and the severity of that harm (ISO 12100-1:2003, 3.11).

Risk analysis

The risk analysis is the combination of the specification of the limits of the machine, hazard identification and risk estimation (ISO 12100-1:2003, 3.14).

Risk assessment

Overall process comprising a risk analysis and a risk evaluation (ISO 12100-1:2003, 3.13).

Risk evaluation

Judgement, on the basis of risk analysis, of whether the risk reduction objectives have been achieved (ISO 12100-1:2003, 3.16).

Safe

"Safe" in connection with drive functions (e.g., "Safe stop 1", "Safely-limited speed", etc.) means that the behavior of the control unit parts in the case of error complies with the requirements according to

EN ISO 13849-1 Category 3 PL d and IEC 61508 SIL 2 (optional module "Safe Motion") or EN ISO 13849-1 Category 3 PL d/PL e and IEC 61508 SIL 2/SIL 3 (optional module "Safe Torque Off"). An error does not cause safety to be lost. Errors must be detected in time and the drive goes to a safe state.

Safely-limited increment

The limited increment is a change in position; it starts in standstill, a specified distance/angle is traveled and it ends in standstill.

Safely-limited speed

Using the measure "Safely-limited speed" implies that a person can in time escape the danger caused by hazardous movements. In general, this can be supposed if the resulting speed does not exceed 15 m/min in the case of hazardous movements without the danger of bruising and cutting, and 2 m/min in the case of hazardous movements with the danger of bruising and cutting.

In accordance with the Machinery Directive [98/37/EC or 2006/42/EC (as of 2009-12-29)], the machine manufacturer has to carry out a risk analysis and afterwards a risk assessment. With these data, the values for reduced speeds have to be determined.

Safe maximum speed

With the function "Safe maximum speed", the speed value is monitored with regard to a maximum allowed limit value.

Safe stop 1 (Emergency stop)

The safety function "Safe stop 1 (Emergency stop)" corresponds to the safety function "Safe stop 1", but is not disabled by activating an enabling control.

Safe Torque Off

The energy supply to the motor is safely interrupted with the safety function "Safe torque off". The motor cannot generate any torque/any force and therefore no dangerous movements.

Safety function

Function of a machine; the failure of the function can result in an immediate increase of the risk(s).

Safety Integrity Level (SIL)

Discrete level (one of three possible levels) to determine the requirements for safety integrity of the safety-related control functions, which is assigned to the safety-related electric control system (SRECS); Safety Integrity Level 3 is the highest and Safety Integrity Level 1 is the lowest of the Safety Integrity Levels (IEC EN 62061:2005, 3.2.23).

Safety-limited position

The "Safely-limited position" is the absolute position at which a motion must have come to standstill.

SRP/CS

Parts of a machine control, which are to provide safety functions, are called "safety-related parts of a control system" (SRP/CS). These parts can consist of hardware and software and be a separate or integral component of the machine control. In addition to the safety functions it makes available, an SRP/CS can also provide operating functions (e.g., two-hand control device for starting a process).

State machine

A state machine is a model of behavior composed of states, transitions between those states and actions.

Stop

"Stop" is the status in which the mechanical component is at rest and the motor is no longer supplied with energy, i.e. it is torque-free or force-free.

Stop categories according to EN 60204-1

- Category 0: Stopping process by immediately switching off power supply to the drives.

- Category 1: Controlled stopping process; power supply to the drives is maintained in order to achieve stopping process. Power is only cut off when standstill has been reached.

- Category 2: Controlled stopping process; power supply to the drives is maintained.

Supply unit

Device which provides power supply to drive controllers. For disconnection from the supply mains, it often contains a mains contactor or makes available the signals required to control the mains contactor.

Test rate

[Test rate (r_t)]; occurrence of the automatic tests to detect errors in an SRP/CS, reciprocal value of the diagnosis test interval.

Third-party supply unit

Supply units which do not belong to the "Rexroth IndraDrive" product range.

Time To Repair

[Time To Repair (r_r)]; reciprocal value of the time span between the detection of a dangerous failure, either by an online test or an apparent malfunction of the system, and restart after system/component replacement.

NOTE: The time to repair does not include the time span required for error detection.

V/Hz [U/f] operation

Operation in which the drive controller generates variable voltage and frequency in order to set the speed of three-phase a.c. motors, for example.

Index

Index

Notes

The Drive & Control Company

Rexroth
Bosch Group

Bosch Rexroth AG
Electric Drives and Controls
P.O. Box 13 57
97803 Lohr, Germany
Bgm.-Dr.-Nebel-Str. 2
97816 Lohr, Germany
Phone +49 9352 18 0
Fax +49 9352 18 8400
www.boschrexroth.com/electrics

R911327664

DOK-INDRV*-SI2-**VRS**-FK04-EN-P