Panasonic

No. SX-DSV03514

TECHNICAL REFERENCE

– Integrated Safety Part –

MODEL

Product Name : AC Servo Driver

Product No. : MINAS A6 Multi series

Issued on
May. 29, 2020
Revised on
Oct. 1, 2020

Industrial Device Solution Business Unit, Industrial Device Business Division,
Industrial Solutions Company, Panasonic Corporation

7-1-1 Morofuku, Daito-City, Osaka 574-0044, Japan
Phone : +81-72-871-1212
Fax : +81-72-870-3151

English specification is published by Industrial Device Solution Business Unit, Panasonic Corporation.
Translation into European local languages is provided only for the convenience of users and it is not officially proofread.
Industrial Device Solution Business Unit, Panasonic Corporation is not liable for any disadvantages caused by utilizing only translated version of specification.
Only the English specification is effective.

Industrial Device Solution Business Unit, Industrial Device Business Division,
Industrial Solutions Company, Panasonic Corporation

Revisions

Date	Page	Rev.	Description	Signed
May. 29, 2020	-	1.0	NEWLY ISSUED	S. Nakano
July. 29, 2020	3-6	1.1	Added descriptions to Safety-related specifications	S. Sakaguchi
Oct. 1, 2020	Cover Cover 1.7 2.1.5 3.2.2 3.3 4 5.3.1.3 9.1	1.2	Changed document title Fixed disclaimer Renamed paragraph Corrected the wording of the document Renamed paragraph Renamed 2nd Encoder name Renamed paragraph Revised description Revised notes	T.Fukuda

Note: The page number (Page) is the current page number at the time of revision.

Integration Guide for Safety Part of MINAS A6 Multi Series

Valid as of

Firmware Version: V 1.00, Rev 0.05

◆ NOTE

- **If the user manual is missing, contact the manufacturer immediately!**
- **Keep the manual at hand at all times!**
- **Ensure that the manual is complete**
- **Only obtain this manual from the original publisher**

Subject to technical change

The contents of our documentation have been collated with greatest care and correspond to our current information.

However, we would like to point out that this document cannot always be updated contemporaneously with the technical development of our products.

Information and specifications can be changed at any time. Please learn more about the current version.

Table of contents

1

General Information

1.1 Identification

Safety part of MINAS A6 Multi Series

Item	Description
Firmware Version	The Firmware Version is specified by the serial number and QR Code on the device identification plate.
Hardware Version	The Hardware Version is specified by the serial number and QR Code on the device identification plate.

1.2 Use of this documentation

- This documentation is part of the product and contains important information about the integration of the servo-driver module, its use and service. Programming and parametrization are described in the online help of the software PANATERM for Safety.
- This documentation is intended for all persons involved in the integration and installation planning as well as those who carry out assembly, installation, use and service of the product
- This documentation must be made available in readable condition to all such persons.
- Please ensure that those responsible for design, integration, application and use, as well as those who work with the device under their own responsibility, have fully read and understood this documentation.
- In case of lack of clarity or further required information, contact Panasonic Corporation.
- All copying, modification, dissemination and all other exploitation, including that of excerpts, is forbidden without the express permission of Panasonic Corporation.

1.3 Structure of the safety instructions

1.3.1 Meaning of signal words

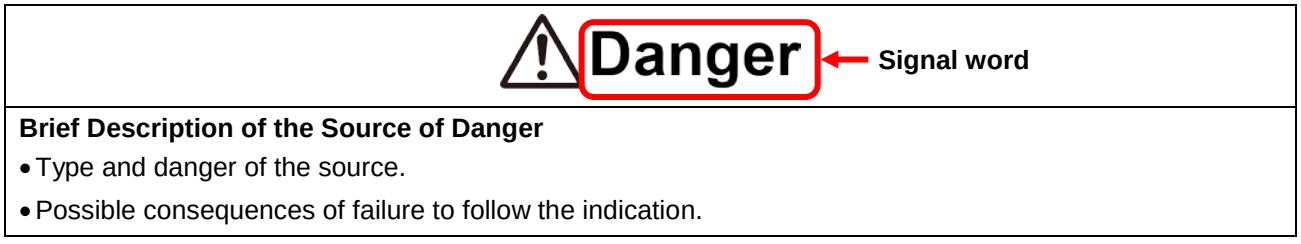
The following symbols and signal words are used in the following documentation: The combination of an icon and a signal word classifies each respective safety instruction. The symbol can vary according to the type of danger.

Symbol	Signal word	Explanation	
	Danger	Death	This signal word must be used where death or irreversible bodily harm can occur as a result of failure to follow this warning.
	Warning	Injury + Property damage	This signal word indicates bodily harm and property damage, including high risks of bodily harm, accidents and health effects.
	Caution		This signal word indicates a danger of property damage. In addition, there is a small risk of injury.
	Beware	Property damagje	This signal word warns of functional interruptions and damage to the driver module or its environment.
	Note	No damage	This signal word indicates useful information and tips that can make use and operation easier.

1.3.2 Safety information

The safety information applies not only to a specific action but to multiple actions within a topic. The icons used indicate either a general or specific danger.

Here you can see the formal structure of a safety indication:



1.4 Defect claims

Compliance with the following documentation is the prerequisite for interruption-free usage and the fulfilment of any potential defect claims. Therefore, read this documentation before you begin planning integration and/or working with the connected devices!

Ensure that the documentation is made available in a readable condition to all those involved in integration and installation planning, as well as to those who carry out assembly, installation, use and service of the product and those who work on the devices under their own responsibility.

1.5 Disclaimer of liability

The observance of the following documentation and the documentation for the connected products from Panasonic Corporation is the basic prerequisite for a safe operation and for obtaining the indicated qualities and performance specifications of the products.

Panasonic Corporation is not responsible for personal injury, property damage, or financial loss resulting from a failure to follow this documentation. All defect warranties are disclaimed in such cases.

1.6 Trademarks

The product names used in this documentation are trademarks or registered marks of the respective mark owner.

1.7 Related documents

Be aware of the following applicable documents:

- Online help in the PANATERM for Safety software
- Configuration report of the PANATERM for Safety software. Serves as a test certificate for validation.
- Reference Specifications,

Document Name
REFERENCE SPECIFICATIONS - Power supply module and Driver module -
TECHNICAL REFERENCE - Function Specification -
TECHNICAL REFERENCE - PANATERM for Safety Programming Manual -

(Note) See our Web site for the above documents.

Always use the current edition of the documentation and software.

In case of lack of clarity or need for further information, please contact the publisher directly.

2

Safety Information

2.1 Safety information

The following fundamental safety instructions serve to avoid personal injury and damage to property. The operator must ensure that these fundamental safety instructions are noted and observed.

Make sure that all persons responsible for design, integration, layout and operation, as well as those who work on the device under their own responsibility, have fully read and understood the manual.

In case of lack of clarity or need for further information, please contact Panasonic Corporation.

2.1.1 General

- Never install or commissioned damaged products. Please report any damage to the transport contractor without delay.
- A danger of serious personal injury or damage to property arises from unpermitted removal of the required enclosure, inappropriate use, and improper installation or service.
- Further details can be found in the documentation.

2.1.2 Target group

- Those persons involved in the design and integration of the module devices as well as their use in applications must have the necessary qualifications. These generally consist of a college or technical education for electrical / electronic systems in combination with specialized knowledge of the laws, regulations, standards and guidelines for the protection of persons and property in dealing with machines and systems.
- All work on installation, start-up, troubleshooting and maintenance are to be carried out by a qualified electrical professional (see IEC 60364 and CENELEC HD 384 or DIN VDE 0100 and IEC 60664 or DIN VDE 0110 and national accident prevention regulations).
- Qualified electrical personnel as referred to in these fundamental safety instructions are people who are familiar with the set-up, assembly, start-up, programming, parametrization and operation of the product and who have corresponding qualifications of employment. They must additionally be familiar with the applicable safety regulations and laws, especially with the requirements of EN ISO 13849-1 and the other norms, guidelines and laws named in this documentation.
- The persons referenced above must have express internal authorization to operate, program, parametrize, label and ground all devices, systems and circuits according to the standards of safety technology.
- All work in the remaining areas of transport, storage, operation and disposal must be carried out by persons who are appropriately trained.

The following table explains each of the individual competencies of the target groups.

Target group	Qualification	Knowledge
Installer	Technical education (technical school, engineering degree or equivalent work experience).	• The working principle of Programmable logic controller (PLC) • Safety regulations • The application • Installation and validation of safety controls • Installation of EMC-appropriate system structure
Electrical Assembler	Electrical technical education (according to the educational standards of the industry).	• Safety regulations • Wiring guidelines • Circuit diagrams, • Appropriate establishment of electrical connections.
Commissioner	Technical education (technical school, engineering degree or equivalent work experience).	• Safety regulations • Working principle of the machine or system • Fundamental functions of the application • System analysis and troubleshooting • Controls setting options • Validation of safety controls
Service Technician	Technical education (technical school, engineering degree or equivalent work experience).	• The working principle of PLC • Safety regulations • Working principle of the machine or system • Diagnosis options • System failure analysis and troubleshooting

2.1.3 Appropriate use

The safety part is a programmable safety control for the manufacture of safety functions, safe monitoring and the shut-down of driver module. It was developed as a safety expansion of the MINAS A6 Multi Series and can be implemented for the following:

- Logic processing for PL e according to EN ISO 13849-1 as well as for SIL 3 according to EN 61508
- Freely programmable safety control with function-oriented programming
- Safely and non-safety-related evaluation of position data of different encoders / encoder combinations for up to 2 axes
- Provision of parameterizable Safe Monitoring Functions (SMF) for driver-module monitoring and shut-down in the device.
- Provision of an appropriate interface for programming of the SF in the device (PANATERM for Safety).
- Control of 4 safety outputs (2x SDO, 2x SBC)
- Import and processing of 4 safety grouped digital inputs
- Import and processing of 1 safety non-grouped digital input

The safety part may only be used for the use cases described in the technical description and in accordance with the prescribed technical framework.

The safety part may only be operated with recommended and/or permitted third-party devices.

The safety part was developed, completed, tested and documented under the applicable guidelines and standards. Thus, when following the prescribed guidelines and safety instructions, no dangers to property or person arise from the product under normal circumstances.

The use of safety part for installation in machines is not permitted until it is determined that the machine meets local laws and guidelines. Where applicable, the Machinery Directive 2006/42/EG as well as EMC Guideline 2014/30/EU should be followed.

The EMC test protocols EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-6, EN 61000-6-2 and EN 61800-3 are taken as fundamental. EN 60204-1 is also to be followed.

CE

The safety part is a safety component according to Appendix IV of the EC Machinery Directive 2006/42/EG. They were developed, designed and manufactured in compliance with the above Directive and EC EMC Directive 2014/30/EU.

◆ NOTE

- **The safety part is an incomplete product under the Machinery Directive and is generally combined with a control component for non-safety-related uses.**
- **The product may not be used without further safety measure that must be considered and carried out by the integrator of the product. The safety instructions in this document must be followed!**

⚠ Caution

Machinery Directive

Where applicable, the Machinery Directive 2006/42/EG as well as EMC Guideline 2014/30/EU must be followed!

The technical data and the specifications for connection conditions are found in the label and in this documentation and must be followed.

2.1.4 Transport and storage

Obey the instructions for transport, storage and correct handling.

Climate conditions are to be observed according to the chapter “3.3 Technical specifications”.

2.1.5 Assembly

The assembly, installation and cooling of the safety part must be determined as appropriate to the environmental and operational conditions according to the below-mentioned safety values and data.

The devices are to be kept from impermissible exposure. Especially during transport and handling, components must not be bent nor any insulation spacing modified. Touching of electronic components and contacts is to be avoided.

This product contains electrostatically sensitive components which can be easily damaged by inappropriate handling. Electrical components must not be damaged or destroyed (under certain circumstances this could cause bodily injury!).

⚠ Warning

Appropriate Placement

- The following use areas are expressly prohibited for this product:
  - Use in areas at risk for explosion or fire
  - Use in mining sites
  - Outdoor use
  - Use in damp spaces or spaces with a risk of being sprayed with water
  - Use in environments with strongly polluted air
  - Use in environments with damaging oils, acids, gases, vapours, dusts, rays, etc.
  - Use in non-stationary implementations if by doing so the mechanical safety ranges could be exceeded.

Other products should be used for these purposes!

- The standard EN ISO 13849 and further standards of functional safety

⚠ Beware

Destruction of the safety part or the control system through inappropriate handling!

The safety part must not be removed even though supply voltage is turned off. Otherwise the safety part can be destroyed or undefined signal conditions can lead to damage to the control system.

◆ NOTE

- **It is requested that all potentially dangerous incidents which arise in connection with Panasonic Corporation safety technology be reported to us immediately.**
  It is further requested that safe products that have failed due to a defect and are not considered repairable be sent to Panasonic Corporation for analysis.
- **Panasonic Corporation takes no liability or responsibility for consequential damages that arise due to :**
  - **Failure to follow standards and guidelines**
  - **Unauthorized modifications**
  - **Inappropriate use**
  - **Failure to follow the instructions in this document**

2.1.6 Electrical connection

While working on devices under voltage, the applicable national accident prevention regulations (e.g., BGV A3) are to be observed.

The electrical installation is to be carried out according to applicable regulations (e.g., wire cross-sections, safeguarding, and grounding connections). Additional instructions are in this documentation.

Instructions for EMC-appropriate installation - such as shielding, grounding, use of filters and arrangement of wires - are found in the documentation (Reference Specifications) of the MINAS A6 Multi series. It is the responsibility of the manufacturer of the equipment or machine to stay within the safety values required by the EMC legislation.

Protection measures and apparatus must meet the applicable regulations (e.g., EN 60204-1).

⚠ Warning

Danger of personal injury from electric shock

Supply the device exclusively with voltage sources that have safety extra-low voltage (e.g., SELV or PELV under EN 61131-2)

If a SELV voltage source is used, it can become PELV through the architecture of the component and the connections (earthing!).

Safety extra-low voltage circuits must always be safely isolated from circuits with dangerous voltage.

⚠ Caution

Fire danger from component failure

Ensure that in the end use an appropriate safeguarding is in place for the DC 24 V power supply of the control system! (Please find information on this point in the section on Supply Voltage).

2.1.7 ESD notes

Electronic components are generally endangered due to electrostatic discharge (ESD).

Electrostatic discharge can arise by any mobile activity.

ESD can arise from any contact.

Most discharges are so small that they are not perceived. However, they can endanger or destroy unprotected electronic components. Therefore, in general handling of exposed electronics is only permitted under effective ESD protection.

When handling open or exposed electronics, observe the following ESD-measures:

- Only touch exposed electronics when absolutely necessary. Only handle exposed components by the edge of the board.
- Use anti-static ESD wristbands
- Use anti-static working documents.
- Make conductive connections between the device/system, documents, wristband and grounding connection.
- Wear work clothes made of wool instead of synthetic materials.
- Keep the work area free of highly isolating materials (e.g., Styrofoam, plastics, nylon ...).
- Keep the devices in the original packaging and do not remove them until just before installation.
- Also use ESD protection with defective components.

 **Caution**
Electrostatic Discharge Destruction of electrical components. Low risk of personal injury Follow the ESD notes.

2.1.8 Operation

Equipment in which this product is used must in each case be provided with additional monitoring and protection apparatus according to the applicable safety standards, e.g., laws related to technical work equipment and accident prevention regulations.

The fact that LEDs and other indicators are off is not a sufficient indicator that the device is disconnected from power and not under voltage.

Safety features internal to the device can result in motor stoppage. Resolving the cause of the interruption, or a reset, can cause the driver module to start up again on its own. If this is not acceptable for safety reasons for the machine being driven, disconnect the device from power before troubleshooting.

2.2 Definitions

The term "safe" as used herein refers to the classification as a safe function on the basis of EN ISO 13849-1.

The term “not safe” refers to functions and data interfaces which do not meet, or do not completely meet, the requirements of the previously referenced standards.

The software “PANATERM for Safety” is a programming interface for this product.

The description “Safe Monitoring Function(s)” or SMF is used in reference to monitoring and muting functions previously defined in their functions which are only parametrized by the user but cannot be changed in their mode of operation.

3

Description of the Safety Part

3.1 Description of the Safety part

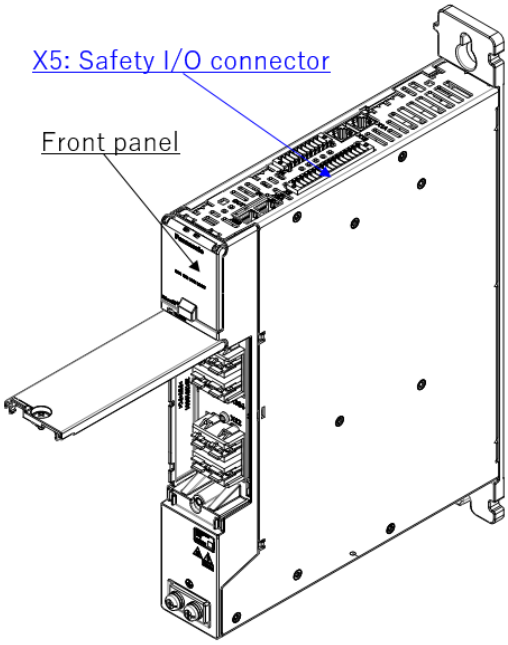
This product is a programmable safety control system for the creation of safety shut-offs and safety functions. It was developed as a safety expansion of the MINAS A6 Multi series. The component has the following basic specifications:

- Logic processing for PL e according to EN ISO 13849-1 as well as for SIL 3 according to EN 61508.
- Freely programmable safety control with function-oriented programming
- Safety and non-safety-related evaluation of position data of different encoders / encoder combinations for up to 2 axes.
- Provision of parameterizable Safe Monitoring Functions (SMF) for driver-module monitoring and shut-down in the device.
- Provision of an appropriate interface for programming of the SF in the device (PANATERM for Safety).
- Control of 4 safe outputs (2x SDO, 2x SBC)
- Import and processing of 4 safe grouped digital inputs
- Import and processing of 1 safe non-grouped digital input

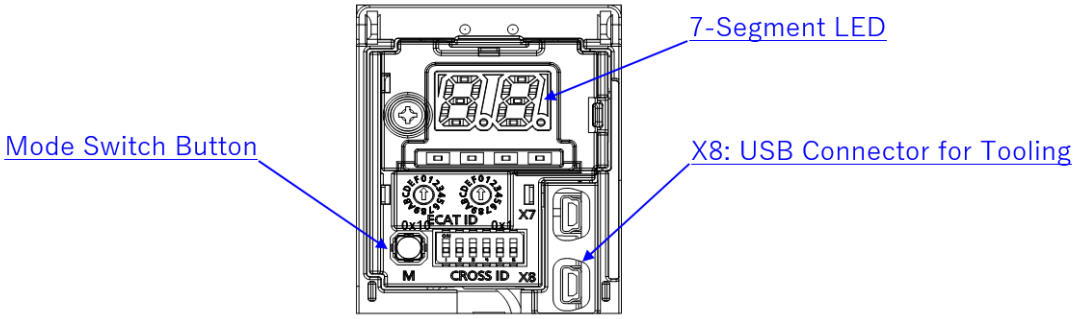
3.2 Mechanical specifications

3.2.1 Overview and positions of plugs

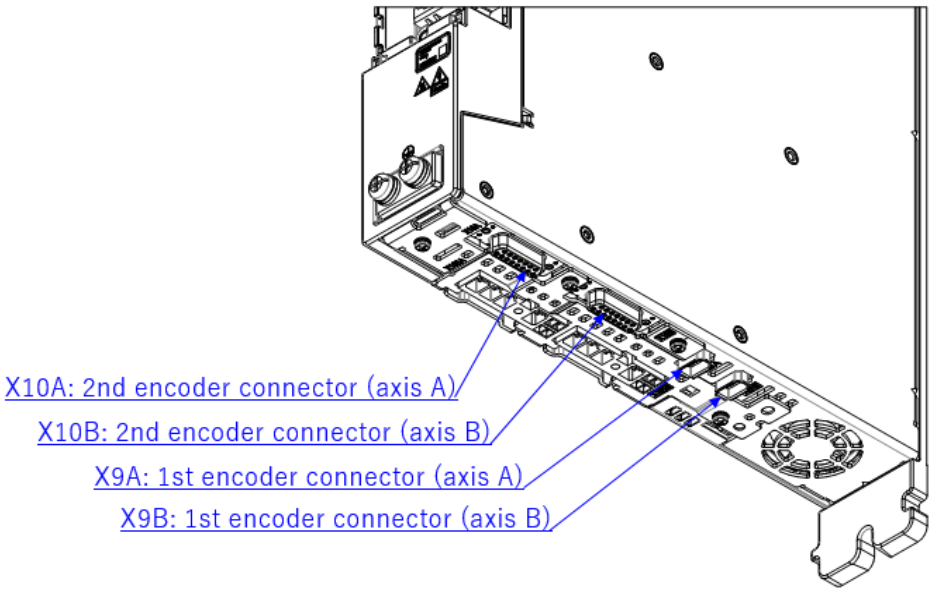
■ **3D overvew**



■ **Inside view of front panel**

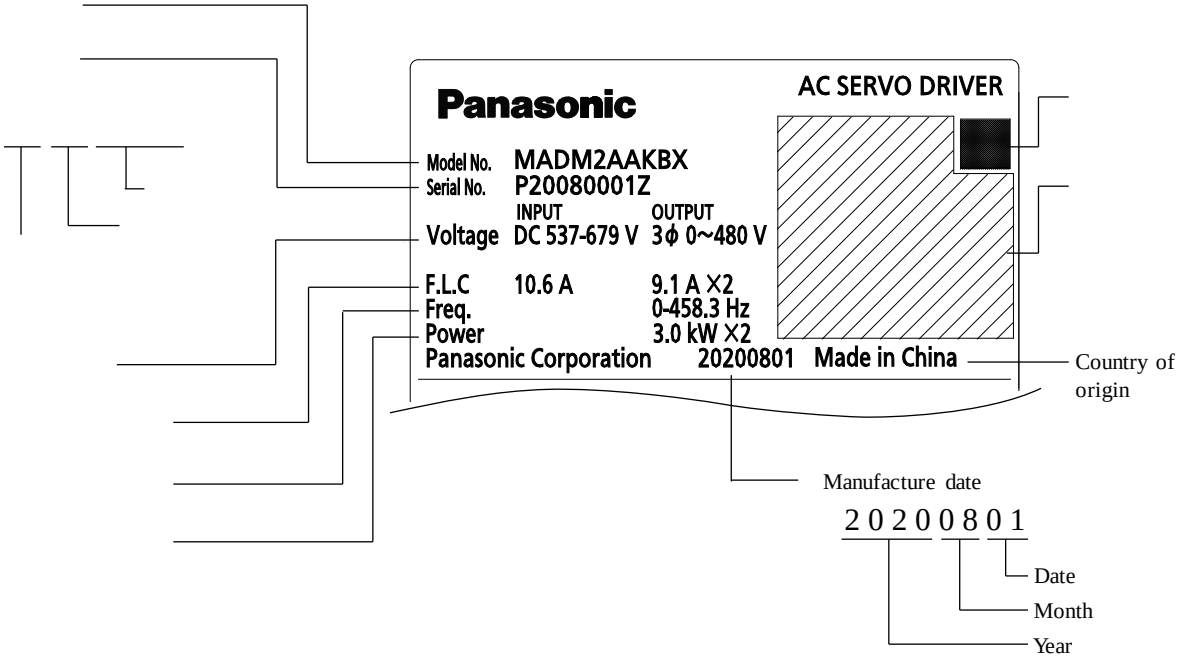


■ **Bottom view**



3.2.2 Identification label

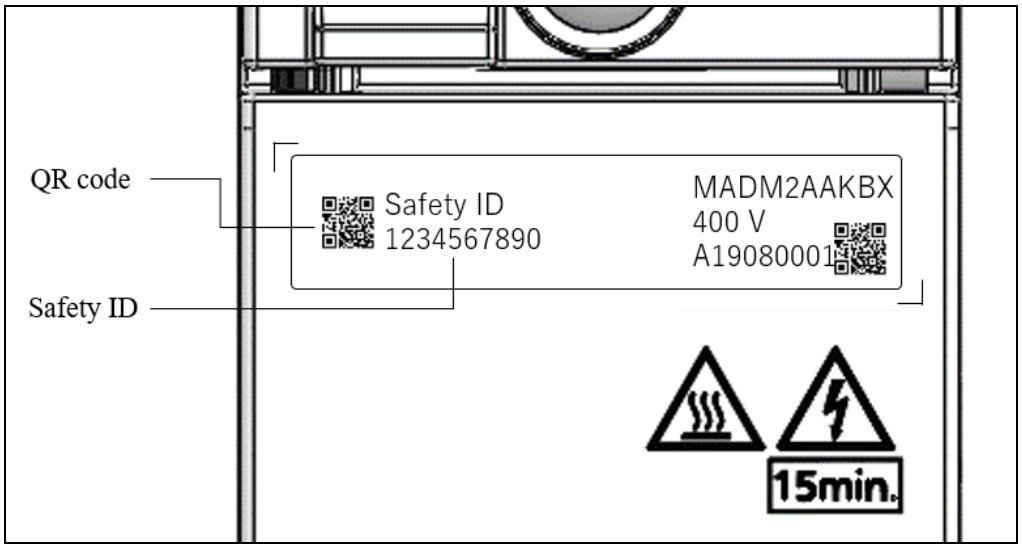
■ **Label of Driver Module**



■

◆ NOTE

- **The firmware and hardware versions are indicated by the QR code.**



Safety ID Label

3.2.3 Safety information display

The 7-segment LED on the front panel has safety information display mode.

Refer to

For details of the other display modes, refer to the Functional Specification (SX-DSV03455).

By pressing and holding the mode switch button for 3 seconds, you can switch between the driver information display mode and the safety information display mode.

In the safety information display mode, various information on the safety part of the driver module is displayed.

By pressing the mode switch button for 1 second, you can switch the following four display contents.

Axis A alarm and Axis B alarm

The display is repeated in the order of below:

Mode display (about 2[s]) → Axis name (about 2[s]) → Alarm number

Mode display

(M1)

Axis name

or

When the safety status is normal, alarm number is displayed "4" for about 2[s].

When a safety error/alarm occurs, the error code / alarm code is displayed one digit at a time, followed by a one-digit alphabet (F / A / E) indicating the type of error / alarm.

Normal

Error code/Alarm code

Refer to

For alarm number display, also refer to the technical document PANATERM for Safety Programming Manual (SX-DSV03508).

3.3 Technical specifications

■ Safety-related specifications

Item	Description
Maximum reachable SIL according to EN 61508.	SIL 3
Maximum reachable PL according to EN ISO 13849.	Pl e
PFH / MTTFd / DCavg / Architecture	System model without depending on the encoder (Target safety functions: STO, SBC) PFH = 2.2 x 10^{-8} [1/h] MTTFd = 172 [years] : High DCavg = 97 [%] : High System model with single non-safety encoder (Target safety functions: SS1, SLS, SSR, SSM) PFH = 4.6 x 10^{-8} [1/h] MTTFd = 109 [years] : High DCavg = 96 [%] : High System model with double non-safety encoders (Target safety functions: SS1, SLS, SSR, SSM, SS2, SOS, SLI, SDI, SLA, SAR) PFH = 2.2 x 10^{-8} [1/h] MTTFd = 94 [years] : High DCavg = 98 [%] : High
Proof Test Interval	20 Years = maximum life cycle
Second/Multiple Fault Occurrence Time	> 30 min

■ I/O - Interfaces

Item		Description
Safe digital inputs (grouped)		4
Safe digital inputs (non-grouped)		1
Safe digital outputs	SDO	2x H/H
	SBC	2x H/L
	STO	2x H/H/H/H
Pulse outputs		2
Connection Type		Terminal
Max. Length of connecting cable		20 m

■ Encoder Interfaces (Axis A/B)

Item	Description
1st Encoder	Panasonic A6
2nd Encoder	ABZ SSI EnDat 2.2 (non-safety) Panasonic Serial Protocol

■ Electric Data

Item		Description
IO-Supply		DC 24 V ±20 % Type SELV/PELV
Encoder supply voltage (The voltage is generated internally by safety part depending on the configuration)		DC 5 V -5 % +10 % DC 8 V -5 % +10 % DC 10 V -5 % +10 %
Digital input values		DC 24 VDC; Type 2 according to EN61131-2
Digital output values	SDO	DC 24 V; 75 mA (High-/ High-Combination) DC 24 V; 1500 mA
	SBC	

■ Environmental Data

Item		Description
Temperature	Humidity	Meet EN 61800-2, IEC 60721-3-2 Class 2K3 (Temperature -25 °C to +70 °C)
	Storage	Meet EN 61800-2, IEC 60721-3-2 Class 1K3 (Temperature -20 °C to +65 °C)
	Operation	Meet EN 61800-2; IEC 60721-3-2 Class 3K3 (Temperature +0 °C to 40 °C without freezing)
Humidity		20 to 85 % RH (Operating / Storage, No-condensation)
Climate Class		3K3 EN 60721-3
Altitude		1000 m
Vibration		5,88 m/s^2 or less, 10 to 60 Hz
Protection Class		I
Overvoltage category		III
Pollution degree		II or I
Degree of protection		IP20 according to EN 60529 Connectors IP00
EMC		IEC 61800-3: 2018 IEC 61800-5-2:2017 EN 61000-6-2:2019
Vibration Resistance		Meet EN 61800-5-1 and IEC 60068-2-6

3.4 Encoder specifications

The encoder interfaces can be configured as ABZ, SSI, EnDat 2.2, Panasonic Serial Protocol and Panasonic A6.

■ ABZ

Item	Description
Supply Voltage	DC 5 V ±5 %
Physical Layer	TTL DC 5V
Measurement Signal A/B	Trace with 90-degree phase offset
Maximum Frequency of the Input Clocks	500 kHz
Maximum Cable Length	20 m
Connection Type	D-SUB 15 pol

■ SSI

Item	Description
Supply Voltage	DC 5 V ±5 % DC 8 V ±5 % DC 10 V ±5 %
Data Interface	Synchronous Serial Interface (SSI)
Frame Length	12 to 32 Bit (configurable)
Data Length	12 to 32 Bit (configurable)
Data Format	Binary and Gray Code
Physical Layer	RS-422 compatible
Operating Mode	Master Mode
Clock Rate	Configurable: 125, 250, 500, 1000, 2000 kHz
Maximum Cable Length	20 m
Connection Type	D-SUB 15 pol

■ EnDat 2.2

Item	Description
Supply Voltage	DC 5 V ±5 % DC 8 V ±5 % DC 10 V ±5 %
Data Interface	Digital RS485 (half duplex)
Encoder Types	LC415FS, EQI1131FS SSI ROQ425 (non-safety)
Encoder Protocol	EnDat 2.2 protocol
Polling cycle EnDat Master, Safe	1 ms
Polling cycle EnDat Master, Non-Safe	62.5 µs
Reaction time of the partial safety function	4 ms
Max. cable length	20 m
Clock frequency	4 MHz
Maximum Cable Length	20 m
Connection Type	D-SUB 15 pol

■ Panasonic A6

Item	Description
Supply Voltage	DC 5 V ±5 %
Encoder Protocol	Panasonic protocol
Resolution per Revolution	23 Bit
Multi-Turn Resolution	16 Bit
Maximum Cable Length	50 m

■ Panasonic Serial Protocol

Item	Description
Supply Voltage	DC 5 V ±5 %
Encoder Protocol	Panasonic protocol
Absolute Positional Data	48 Bit
Maximum Cable Length	20 m
Connection Type	SUB-D 15 pol

4

Connection of the Safety Part

4.1 EMC protection measures

Maintenance of the specified environmental and EMC specifications is to be ensured as to the protection measures as well as to the surrounding electronic components in relation to the component and its environment.

Further, in the operating and installation directions of the overall layout, notes should be made of proper EMC-appropriate installation and wiring.

■ **Particular attention should be paid to the following:**

Because the safety part is intended for industrial use, the EMC regulations EN 61800-3 and EN 61326-3-1 are applicable and fundamental. It is assumed that the electromagnetic compatibility of the complete system is ensured by using the appropriate conventional precautions. The following measures ensure the appropriate use of the safety part:

- Place signal wires and cables from converters in separate cable conduits. The distance between the cable ducts must be at least 10 mm.
- Only shielded motor supply cables should be used near the driver module.
- Observe EMC-appropriate installation of converters near the safety part. Take special note of the cable routing and the quality of the shielding of the motor supply cables and the connection of the braking resistor.
- All protections around the safety part must be fitted with an appropriate suppressor element.
- Use shielded leads for the safety-directed control wiring.
- You must place the shielding of the encoder supply voltage on both sides of the housing.

◆ NOTE

- **The functioning of the component in light of the EMC influences of the surrounding components of the overall layout is to be proven by appropriate tests in the scope of the certification of the overall layout.**
- **In the operating and installation directions of the overall layout, the preceding notes should be made of proper EMC-appropriate installation and wiring.**

4.2 Connections and wiring

⚠ Beware

Improper handling can lead to damage to the driver module.

Turn off the supply voltage and unplug any interface cables before mounting, installation and maintenance work.

■ **Cable Specification**

Type, diameter and material of the connected wires are determined by the manufacturer-specific data sheet of the plugs being used, national and international installation regulations, the type and size of the wiring protection and the components to be connected.

For stranded wires, the use of wire terminations is recommended.

4.2.1 Supply voltage

4.2.1.1 DC 24 V IO supply voltage

⚠ Warning

Loss of safety Function and/or Risk of Personal Injury Due to Excessive Voltage

Supply the device exclusively with voltage sources that have safety extra-low voltage (e.g., SELV or PELV under EN 61131-2)

If a SELV voltage source is used, it can become PELV through the architecture of the component and the connections (earthing!).

Safety extra-low voltage circuits must always be safely isolated from circuits with dangerous voltage.

⚠ Beware

For the DC 24 V IO supply voltage, ensure that in case of failure no higher voltage than 60 V can arise.

The safety part requires an IO supply voltage of DC 24 V.

Nominal	Tolerance	
	Minimum	Maximum
DC 24 V	DC 19.2 V	DC 28.8 V

(Note) The minimum and maximum tolerances of the DC 24 V IO supply voltage must be strictly respected.

4.2.2 Grounding

This product requires a connection to the appropriate grounding for safe operation.

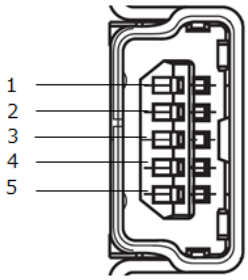
The screw terminals for grounding can be found on the housing of the driver module.

After completion of the installation procedures, testing of the protective conductor function with the connected components must be tested according to the respective national standards.

4.2.3 Pin assignments of connectors

4.2.3.1 USB connector (for safety) X8

■ **Terminal pin assignment**



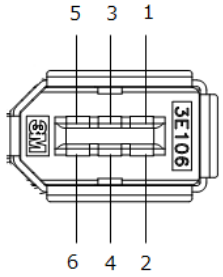
Pin No.	Symbol	Polarity	Description
1	VBUS	-	VBUS
2	D-	IN/OUT	USB signal terminal
3	D+	IN/OUT	USB signal terminal
4	-	-	For manufacturer
5	GND	-	Signal ground

(Note) The connector type is USB mini-B.

4.2.3.2 Encoder connectors

1st Encoder Connector X9 (X9A, X9B)

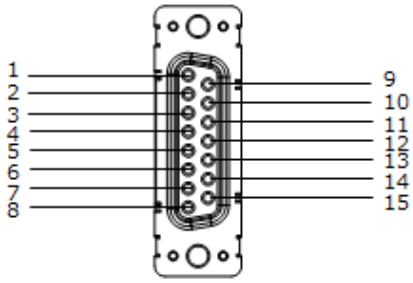
■ **Terminal pin assignment**



Pin No.	Symbol	Polarity	Description
1	E5V	-	1st Encoder power output
2	E0V	-	1st Encoder ground
3	-	-	-
4	-	-	-
5	PS	IN/OUT	1st Encoder signal non-inverting input/output
6	/PS	IN/OUT	1st Encoder signal inverting input/output
Shell	FG	-	Frame ground

2nd encoder connector X10 (X10A, X10B)

■ Terminal pin assignment

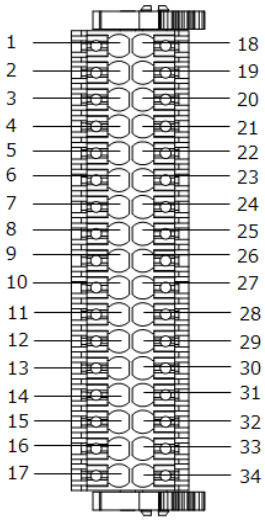


Pin No.	Symbol	Polarity	Description
1	EX5V	-	2nd Encoder power output (Panasonic / ABZ)
2	EX0V	-	2nd Encoder ground
3	EXPS	IN/OUT	Serial signal non-inverting input/output
4	/EXPS	IN/OUT	Serial signal inverting input/output
5	EXA	IN	A-phase signal non-inverting input
6	/EXA	IN	A-phase signal inverting input
7	EXB	IN	B-phase signal non-inverting input
8	/EXB	IN	B-phase signal inverting input
9	EXZ	IN	Z-phase signal non-inverting input
10	/EXZ	IN	Z-phase signal inverting input
11	DATA	IN/OUT	Serial signal non-inverting input/output (EnDat 2.2 / SSI)
12	/DATA	IN/OUT	Serial signal inverting input/output (EnDat 2.2 / SSI)
13	CLK	OUT	Clock signal non-inverting input/output (EnDat 2.2 / SSI)
14	/CLK	OUT	Clock signal inverting input/output (EnDat 2.2 / SSI)
15	EVDD	-	2nd Encoder power output (EnDat 2.2 / SSI)

(Note 1) X10A connector is for A axis, and X10B connector is for B axis.
(Note 2) Terminal pin assignment is common to A and B axes.

4.2.3.3 Safety I/O connector X5

■ **Terminal pin assignment**



Pin No.	Symbol	Polarity	Description
1	FG	-	Frame ground
2	BRKO1-	OUT	Safety brake output 1-
3	BRKO1+	OUT	Safety brake output 1+
4	SDO2A	OUT	Safety output 2A
5	SDO1A	OUT	Safety output 1A
6	NC	-	*Do NOT connect.
7	NC	-	*Do NOT connect.
8	NC	-	*Do NOT connect.
9	NC	-	*Do NOT connect.
10	PULSA	OUT	Diagnostics pulse output
11	SDIN	IN	Non-Grouped Safety digital input
12	SDI4A	IN	Grouped safety digital input 4A
13	SDI3A	IN	Grouped safety digital input 3A
14	SDI2A	IN	Grouped safety digital input 2A
15	SDI1A	IN	Grouped safety digital input 1A
16	COMA	-	Safety input common A
17	EX24V	-	External power supply +24 V for safety
18	FG	-	Frame ground
19	BRKO2-	OUT	Safety brake output 2-
20	BRKO2+	OUT	Safety brake output 2+
21	SDO2B	OUT	Safety output 2B
22	SDO1B	OUT	Safety output 1B
23	NC	-	*Do NOT connect.
23	NC	-	*Do NOT connect.
24	NC	-	*Do NOT connect.
25	NC	-	*Do NOT connect.
26	NC	-	*Do NOT connect.
27	PULSB	OUT	Diagnostics pulse output
28	GND	-	Signal ground
29	SDI4B	IN	Grouped safety digital input 4B
30	SDI3B	IN	Grouped safety digital input 3B
31	SDI2B	IN	Grouped safety digital input 2B
32	SDI1B	IN	Grouped safety digital input 1B
33	COMB	-	Safety input common B
34	EXGND	-	External ground

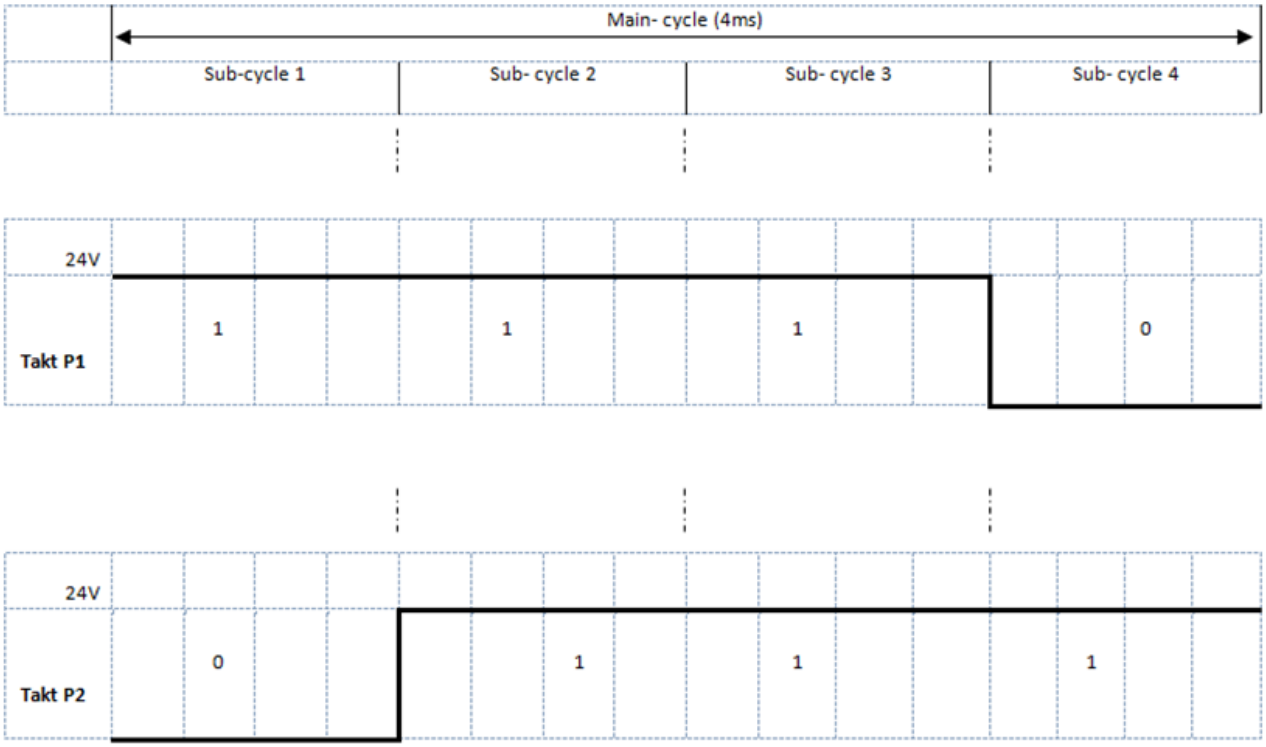
4.3 Connection of safe digital inputs (SDI)

The safety part has 4 grouped and 1 non-grouped safe digital inputs. The grouped inputs (SDI1A/SDI1B, SDI2A/SDI2B, SDI3A/SDI3B and SDI4A/SDI4B) are to be used redundantly and are suitable for connection to dual-channel signals with and without pulse and cross-connection. The non-grouped input SDIN1 can be used individually and is suitable for connection to single-channel signals with and without clocking and cross-connection.

The connected signals must have a “High” level of DC 24 V (DC +11 V... DC +30 V) and a “Low” level of (DC -3 V... DC +5 V, Type 2 according to EN61131-2). The inputs are internally provided with input filters.

A diagnosis function internal to the device cyclically tests the correct operation of the inputs including the input filter. A detected failure puts the safety part in an alarm condition. At the same time, all outputs of the safety part are rendered passive.

In addition to the signal inputs, the safety part provides two clock outputs P1 and P2. The clock outputs are toggling DC 24 V outputs.



The clock outputs are intended exclusively for monitoring the digital inputs and cannot be used for any other functions in the application.

The clock outputs are specified for a maximum current of 250 mA.

Additionally, permitted OSSD-outputs can be connected to the digital inputs without restriction.

Every input of the safety part can be individually configured for the following signal sources:

- Input is assigned to clock P1.
- Input is assigned to clock P2.
- Input is assigned to DC 24 V continuous voltage

NOTE

- **For single-channel use of the inputs, the obtainable safety level is restricted to SIL 2 and PL d if the safety function is required at regular intervals.**
- **A safety use of the inputs is only intended in connection with the pulse outputs.**
- **If the clock outputs are not used, external measures (especially a suitable cable routing) must be used to prevent a short in the external wiring between various inputs and with the supply voltage of the safety part .**

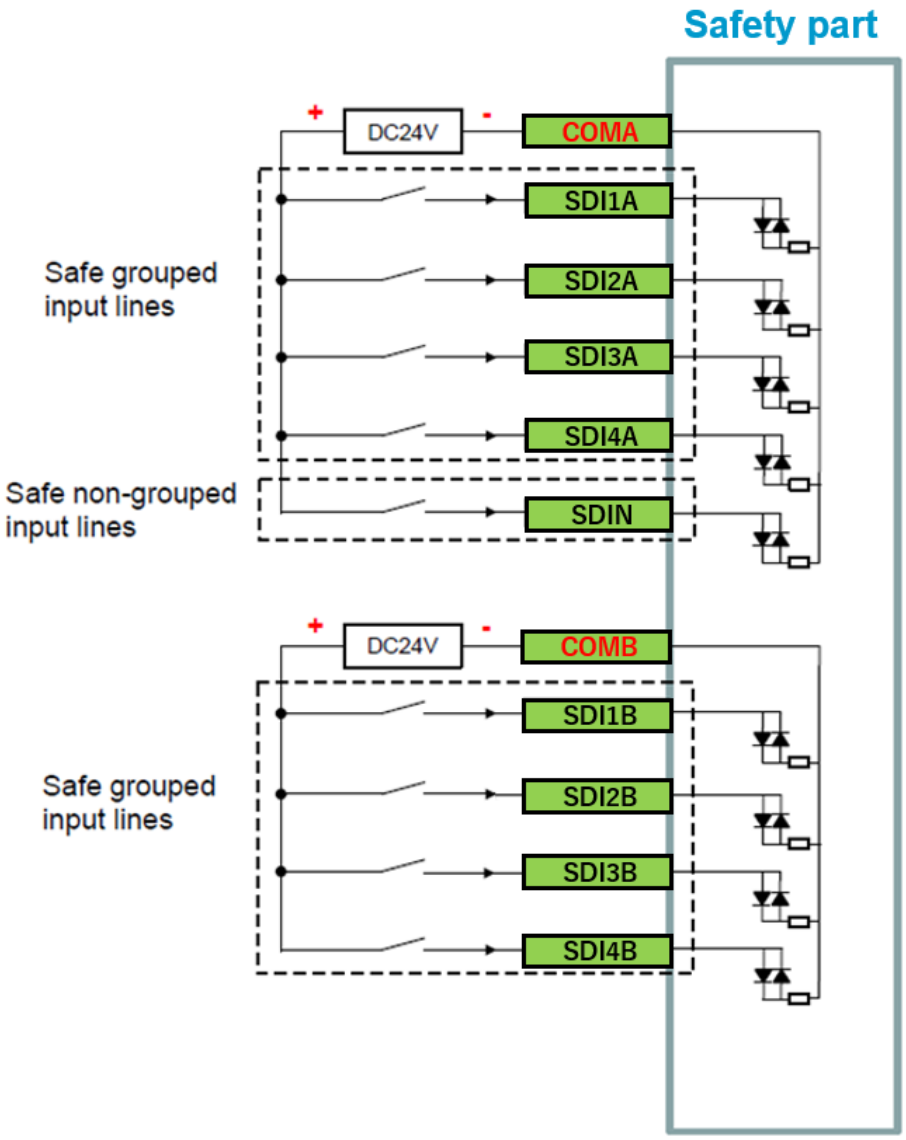
4.3.1 Control of the digital inputs with HIGH level

The safety part inputs can be controlled with HIGH (24 V/P1/P2) level as well as with LOW (0 V) level.

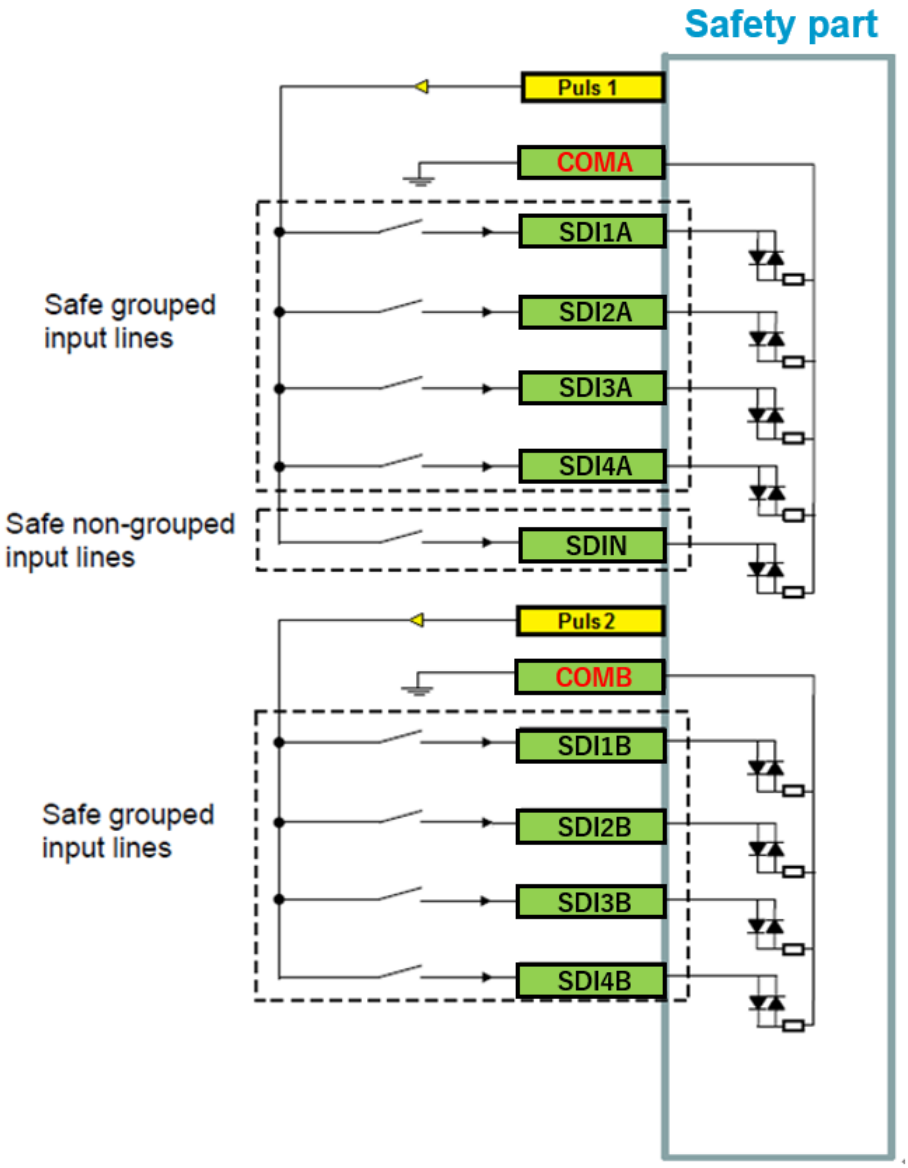
For the control of the safety part inputs with HIGH level (24 V/P1/P2), the signal 0 V (GNDSUIN) is connected to the “Common” connector.

The signals connected to the digital inputs must have a “High” level of DC 24 V (DC +11 V... DC +30 V) and a “Low” level of (DC -3 V... DC +5 V, Type 2 according to EN61131-2).

Sink connection (DC 24 V)



Source connection (Puls 1 / Puls 2)

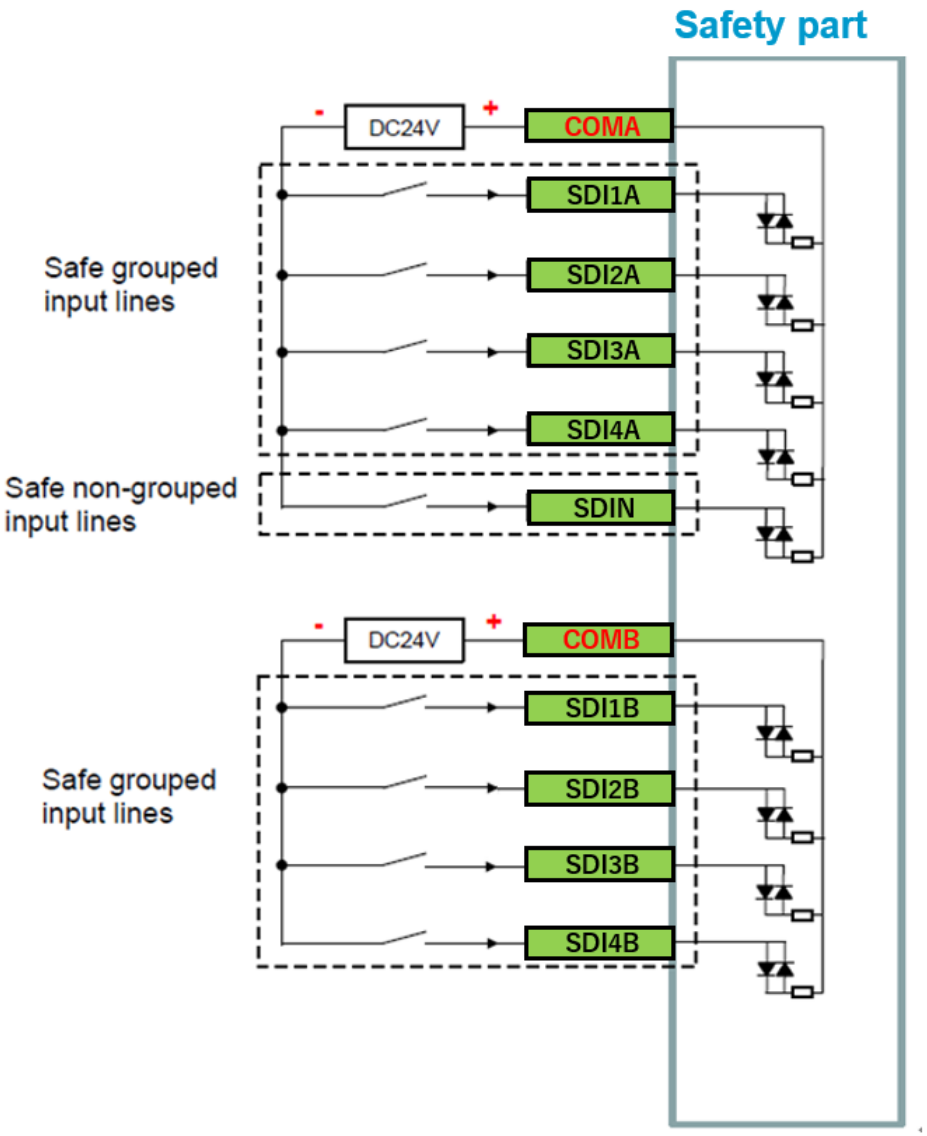


4.3.2 Control of the digital inputs with LOW level

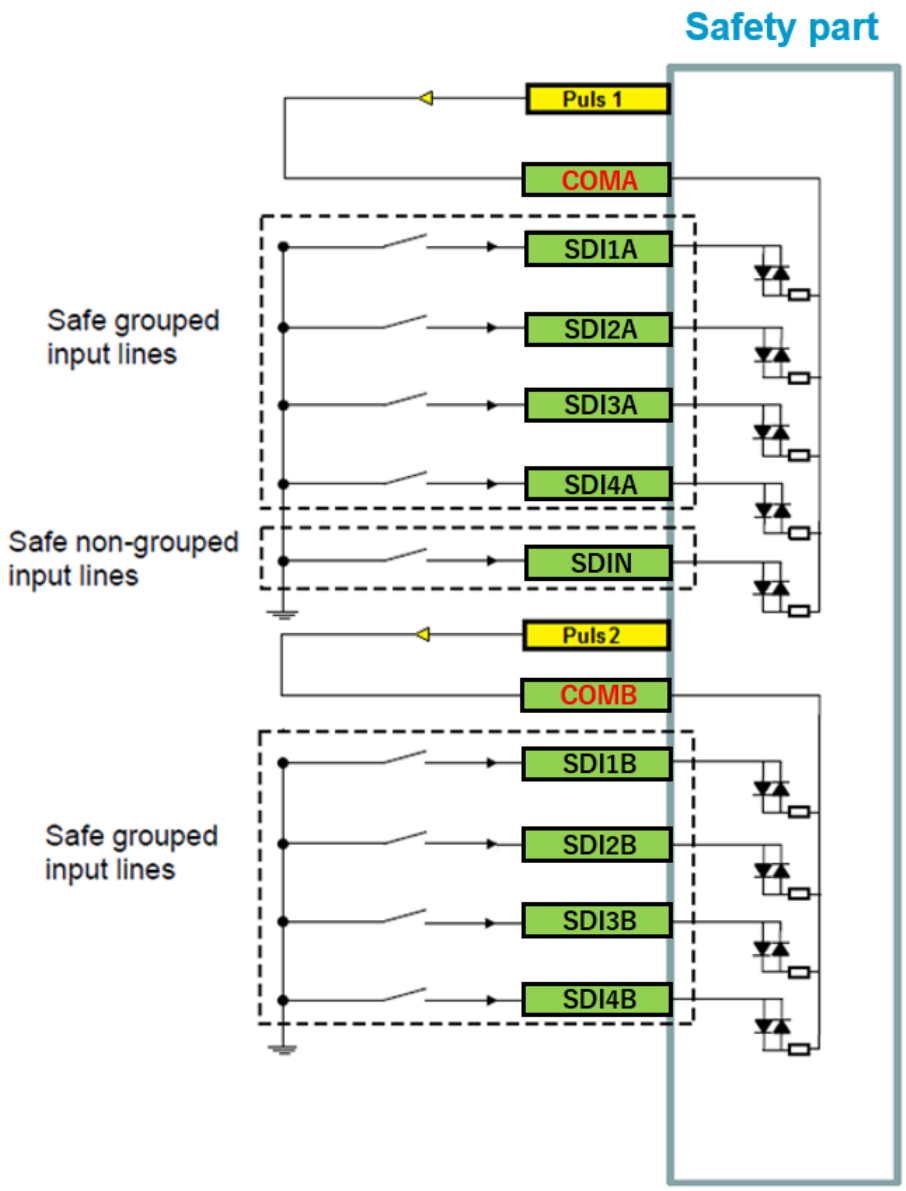
For the control of the safety part inputs with LOW level (0 V), the signal 24 V P1 or P2 is connected to the “Common” connector.

The signals connected to the common connector must have a “High” level of DC 24 V (DC +11 V... DC +30 V) and a “Low” level of (DC -3 V... DC +5 V, Type 2 according to EN61131-2).

Sink connection (DC 24 V)



Sink connection (Puls 1 / Puls 2)



5

Integrated Safety Features

5.1 Integrated safety features

The following described safety technology of this product fulfils the following safety requirements:

- Performance Level e according to EN ISO 13849-1
- SIL 3 according to IEC 61508

For a complete safety design of an entire piece of equipment using this product, further documentation must be prepared by the user which is not further discussed herein.

Please determine the applicable requirements of the underlying standards.

◆ NOTE

- **An EU-type examination has been carried out. A copy of the EU-type examination certificate can be requested from Panasonic Corporation.**

The following chapter describes the architecture and the fundamental structure of the safety part safety control.

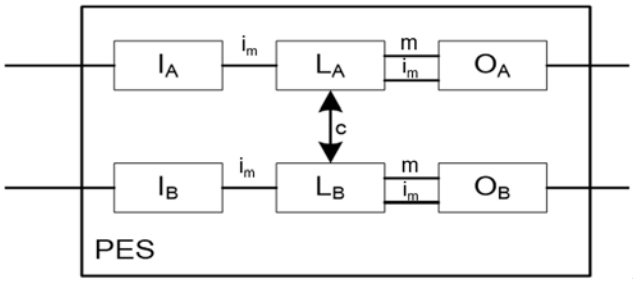
The connection options are described whereby the safety part can be connected with sensors.

In connection with the same and with the diagnostics used, under EN ISO 13849-1 a safety category and maximum reachable Performance Level (PL) can be determined.

5.2 Safety technology architecture of the safety part

The internal layout of this product consists of two separate channels with comparison of results on each side. In each of the two channels, sophisticated diagnostic mechanisms are used for fault recognition.

The layout corresponds in architecture and functionality to category 4 of EN ISO 13849-1.



PES : Programmable Electronic System
I_A : Input Channel A
I_B : Input Channel B
L_A : Logic Channel A
L_B : Logic Channel B
O_A : Output Channel A
O_B : Output Channel B
c : Cross-comparison
m : monitoring
i_m : connecting means

The overall architecture has the following layout:

Double reading of the input information (through a sensor or digital input) and diagnostics by cross-comparison.

The specific safety characteristics of each component (sensor, actuator) are to be found in their respective technical data.

For the safety evaluation of the overall system, the provided safety characteristics of the component system safety part (PES) can be used (see Chapter “3.3 Technical specifications”).

NOTE

- **When using multiple sensors of various functions, they should be understood as series connections for purposes of safety evaluation of the overall system. On this topic, see the BGIA-Report 02/2008 "Functional Safety of Machine Controls – Application of EN ISO 13849".**
- **With respect to the relevant exclusion of faults, EN ISO 13849-2 is provided in the tables under D in the Appendix.**
- **The examples described in this handbook and their characteristic architecture are relevant for assignment to a category according to EN ISO 13849-1. The resulting maximum possible Performance Level according to EN ISO 13849-1 is dependent on the following factors of the external components:**
  - **Structure (simple or redundant)**
  - **Measures against Common Cause Failures (CCF)**
  - **Diagnostic Coverage (DCavg)**
  - **Mean Time To Failure (dangerous) (MTTFd) of a channel.**

5.3 Sensor interface

5.3.1 Safety-related specifications and wiring of safe digital inputs (SDI)

The safety part has complete redundant signal processing channels for each safe input.

Further, measures are implemented for each to obtain the highest possible diagnostic coverage (DC) values. The maximum possible safety category as well as the Performance Level are determined according to EN ISO 13849-1.

5.3.1.1 Diagnostics of safe digital inputs (SDI)

The safety part provides expansive diagnostic functions for the input subsystem.

These are continuously and optionally carried out (cross-comparison, cross-circuit test, 2 or more channel sensor with time monitoring, start test).

Cable interruptions of sensors lead to a safe condition (proven safety concept according to EN ISO 13849-2)

Internal diagnostic functions

Item	Description
Cross-comparison	The safe inputs of the safety part are internally laid out in dual channels. The status of the input signals is continuously cross-compared. Only in the case of a High signal in both input subsystems is the SDI evaluated as “High”, otherwise it is evaluated as “Low”.
Dynamic Test of Thresholds	The thresholds for recognition of the High level are cyclically tested at a high rate. If the defined threshold is not met, the safety part goes into a safe mode (module alarm).
Dynamic Test of Switching Capacity	The switching capacity of the input component at Low level is tested for all safe inputs at a high rate. In case of problems, the safety part changes to a safe mode (module alarm).

Parametrizable diagnostics of external circuitry

Item	Description
Cross-fault test (Note)	The safety part has two test data outputs (TDO), each of which has an identifying signature. In use of the cross-fault test the switch elements of the digital controllers are to be provided by the test data outputs of the safety part. The signature is consequently marked with the High signal level of the sensors and tested by the safety part. Through the signature testing, cross-faults in the external wiring can be recognized to the High signal level and to neighboring SDIs with various TDOs. Where redundant inputs are used, varying TDOs are recommended.

Note

The cross-fault test does not recognize:

- Cable short on a sensor contact
- Direct short between TDO and the SDI itself

Item	Description
Start Test after Turning on this product	Each time this product is turned on, a test of the sensor at the Low signal level (=defined Safe Status) must be carried out, e.g., activation of the emergency shut-off button of a locking device after the equipment starts. [Advantage] Recognition of faults that arise during an interruption in operation.
Comparison of Multi-Polar Contacts Without Time Monitoring	Where redundant sensors are used at more than one SDI, all sensors must be in a predefined setting so that the input result is evaluated as High.
Comparison of Multi-Polar Contacts with Time Monitoring	The same test as before, however additional monitoring of the input signals for correspondence of the defined level contexts within a time window of 3 s. If any discrepancies arise over a window > 3 s the safety control goes into the mode. [Advantage] Immediate recognition of a faulty contact is possible and the DC increases.
Manually Supported Tests	It is additionally possible to force regular tests in the application, which for example may require manual interactions by the user. For example, timers for a time monitoring of a signal change can be used, which is only possible through a manual test in which upon running out of the timer the machine is automatically shut down. These tests forced by the controller (“forced dynamic sampling”) can be additionally used in evaluation of the DC. An example of this is that the guard door is opened at least once per shift in order to test the functionality of the sensor. If it is not possible to open the guard door within this time, the timer runs out and the safety part witches to the safe mode.

For the safety evaluation of the overall system, the following diagnostics can thus be used for the input sensors:

○: Can be used, x: Cannot be used

Characteristic input element	Parametrized / Operating tests				DC [%]	Definition of the measure	Notation
	Cross-fault test	With time monitoring	Start test	Cyclical test in operation			
One-channel	-	-	○	○	>60	Cyclical test impulse through dynamic modification of the input signals.	A sufficiently high test- rate must be provided.
	×	-	-	-	90	Cyclical test impulse through dynamic modification of the input signals.	Only effective if pulse assignment is active
	×	-	○	○	90 to 99	Cyclical test impulse through dynamic modification of the input signals.	DC is dependent on the frequency of the Start/Cyclical Test DC = 90 Test only at intervals > 4 Weeks DC = 99 Test at least once per day and 100-fold demand
Dual-channel	-	-	-	-	90	Cross-comparison of input signals with a dynamic test, if cross-faults cannot be detected (in case of multiple inputs and outputs)	In troubleshooting a short of up to DC = 99 is possible
	-	-	○	○	90 to 99	Cyclical test impulse through dynamic modification of the input signals.	DC is dependent on the frequency of the Start/Cyclical Test
	×	-	-	-	99	Cross-comparison of input signals with immediate and intermediate results in the logic (L) as well as timing and logical program execution monitoring and detection of static failures and short circuits (with multiple inputs/outputs)	Only effective if pulse assignment is active
	-	×	-	-	99	Plausibility checking, for example use of closing and opening contacts = non-equivalent signal comparison of input elements	Only effective in connection with active time monitoring function for the input element

5.3.1.2 Circuitry of the test data output (TDO)

In addition to the binary inputs SDIx the safety part also has two data outputs (clock outputs) TDOx available. The data outputs are switching DC 24 V outputs that are intended only for monitoring of the binary inputs.

For other functions within the application, the data outputs may not be used.

The data outputs may only be subjected to a net current of 250 mA.

◆ NOTE

Without use of pulsing the binary inputs can be wired as follows:

- **With single-channel, self-monitoring sensors structures up to Category 2 can be built and thus a corresponding Performance Level can be reached according to EN ISO 13849-1.**
- **With dual-channel sensors without a function test within 24 hours, structures up to Category 3 can be built and thus a corresponding Performance Level can be reached according to EN ISO 13849-1.**
- **With dual-channel sensors and a function test within 24 hours, structures up to Category 4 can be built and thus a corresponding Performance Level can be reached according to EN ISO 13849-1.**
- **Ensure that external measures (especially a suitable cable routing) are used to prevent a short in the external wiring between various inputs and with the supply voltage of the safety part.**

Every binary input of the safety part option can be individually configured for the following signal sources:

- Binary input is assigned to Pulse TDO1
- Binary input is assigned to Pulse TDO2
- Binary input is assigned to DC 24V continuous voltage.

◆ NOTE

- **An alternating pulse assignment for the inputs is recommended.**

5.3.1.3 Architecture of the input elements

In this chapter the internal architecture of the inputs is described. The safe digital inputs are laid out in fully redundant fashion except for the input terminals.

◆ NOTE

- **For a safety evaluation of the "Sensor System" the manufacturer's data (MTTFD, FIT-Numbers, etc.) are to be used.**
- **The DC-values provided in the table are to be used conservatively and the boundary conditions (see table under "Notations") are to be maintained.**
- **Troubleshooting is permissible according to the applicable standards. The boundary conditions laid out are to be maintained permanently.**
- **If multiple sensor systems are required for proper functioning of a single safety function, their component values are to be correctly combined according to the selected procedure.**

In order to recognize a cross-fault in the signals of concern, the device's internal pulse voltages can be interconnected with the binary inputs.

You can use the binary inputs individually or combined in groups, according to the required Performance Level. For this purpose, the software interface PANATERM for Safety has various ready-made input elements available (see the programming handbook, Chapter "Input Modules").

The safety part has complete separate signal processing paths for each safe digital input (SDI).

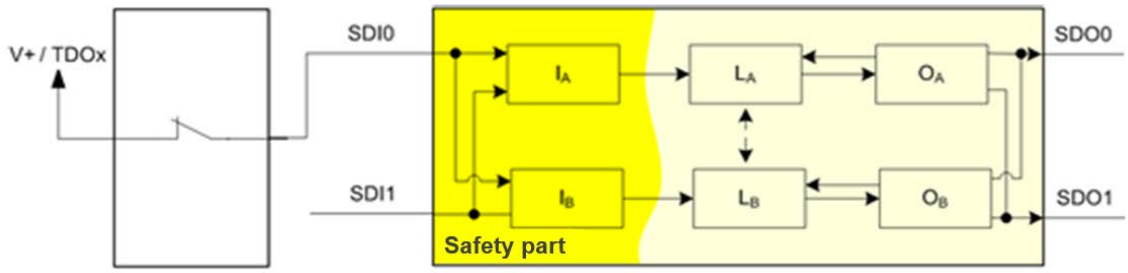
The digital inputs are laid out in fully redundant fashion, with the exception of the electromechanical input terminals. The details for classification, the DC, and the obtainable PL and SIL are listed below.

The safety part provides expansive diagnostic functions for the input subsystem, in order to obtain the highest possible DC values (Diagnostic Coverage = diagnostic coverage level). These are continuously and optionally carried out (cross-fault monitoring with pulse recognition). For the safety evaluation of the overall system, the DC values for the input sensor system in the Chapter "Diagnostic Values" can be used.

◆ NOTE

- **In the following switching examples, it is presumed that the switching elements used are chosen according to the desired Performance Levels according to EN ISO 13849-1 and have a corresponding safety authorization for the specific use case.**

Single-Channel Sensor and Use of 1 SDI



Where a single-channel sensor is used with pulsing, the following faults are detected:

- Short in the DC 24 V supply voltage
- Short in the DC 0 V
- Cable break (power interruption is safe state!)

However, be cautious in case of a cable short between the two sensor connections, because this is not detected!

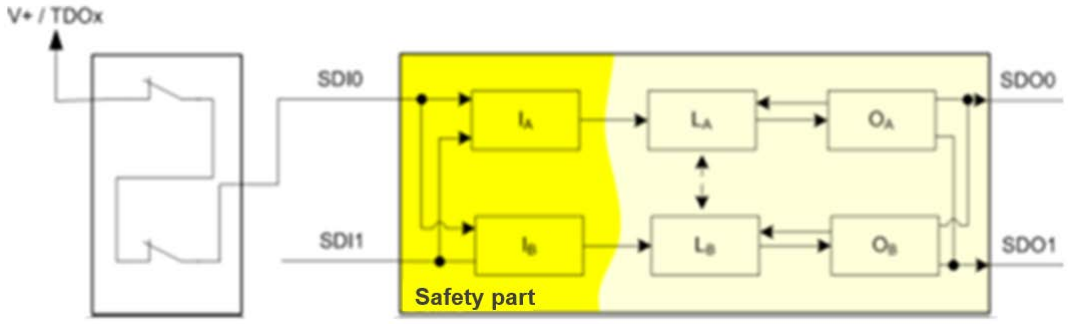
Due to the single-channel character of the switching element / sensor, fault exclusion is necessary in case of its failure. This is permissible when using positively disconnecting switches with correct constrained actuation.

Equivalent to this is a series connection of 2 switching elements with corresponding exclusion of a double fault. This can be implemented, for example, with the safe outputs of an electronic monitoring device (light curtain, safety mat) with internal dual-channel shut-off.

◆ NOTE

- **PL d or higher can be reached according to EN ISO 13849-1 if the short between an input and the associated pulse output, as well as the short between the sensor connections can be excluded. It must be noted that the switch must be normally closed in case of failure according to EN 60947-5-1. Additionally, the sensor must be triggered at regular intervals and the safety function must be activated. Fault exclusions can be achieved according to EN ISO 13849-2. For single-channel use of the inputs, the attainable safety level is restricted to SIL 2 and PL d if the safety function is demanded at regular intervals.**
- **A series connection of 2 switching elements with fault exclusion of double faults requires a test of suitability according to the intended safety level for this element. Note the applicable rules of the EC Machinery Directive 2006/42/EC.**
- **For single-channel sensors, a safety-related use of the inputs is only intended in connection with the pulse outputs.**

Dual-Channel Sensor in Series and Use of 1 SDI

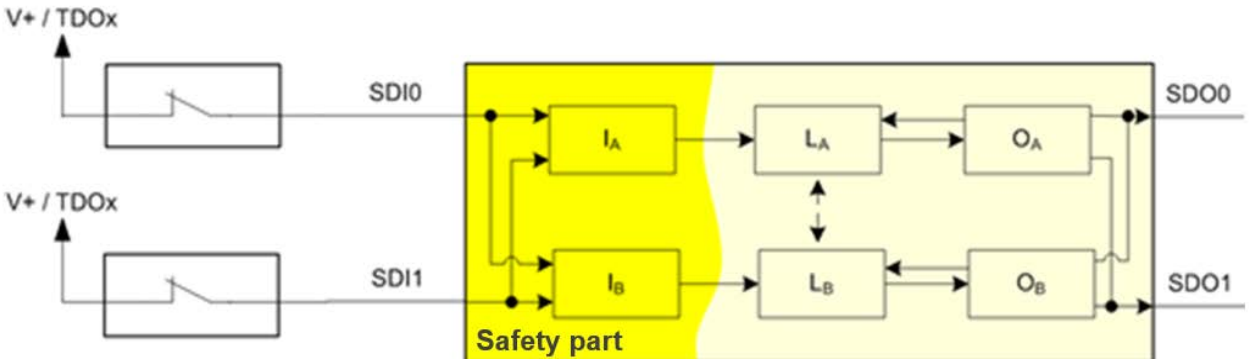


Dual-channel input elements in series connection (Cat. 4, fault tolerance 1) with low to medium DC through signal processing in two channels and diagnostics by means of cyclical testing.

◆ NOTE

- **Fault exclusion is necessary with this single-channel wiring, which can lead to failure of both contacts of the sensor!**
- **Exclusion of a short between both sensor contacts**
- **Exclusion of mechanical failure of a common actuator of both sensor contacts. Thus some product standards expressly require, for example for guard doors, the use of independent locking mechanisms!**

2 Sensors / Dual-Channel Sensor and Use of 2 SDI



Faults are detected at least upon demand. The DC is medium and can be changed to high level by use of cyclical tests (start tests, operational / organizational tests) depending on the frequency of testing.

The following faults are detected:

- Short in the DC 24 V voltage supply
- Short in the DC 0 V
- All cross-connections
- Cable break (power interruption is safe state!)

For safety applications, only normally closed contacts are to be used for this purpose.

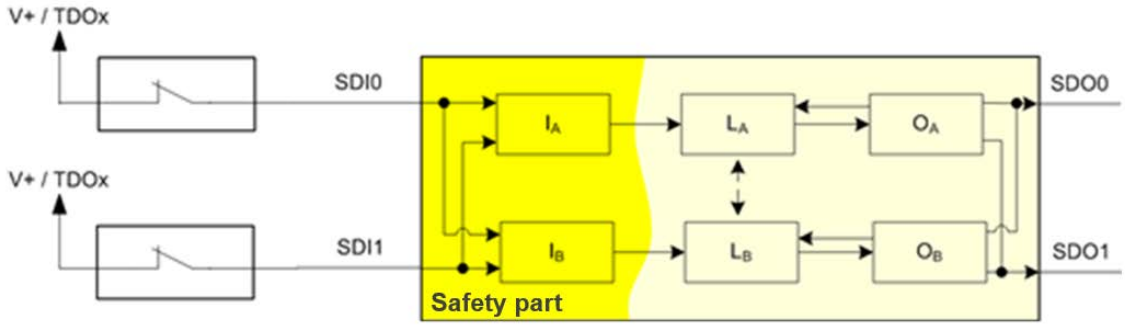
PL d according to EN ISO 13849-1 can be achieved by use of sensors / switching elements with fault exclusion for not opening the switch contacts. This is permissible when using positively disconnecting switches with correct constrained actuation. The use of sensors with self-monitoring output contacts is also permitted.

PL e according to EN ISO 13849-1 can be achieved by use of redundant sensors / input elements with sufficiently high MTTFd in connection with a time and plausibility monitoring and sufficiently high dynamization of the switch condition = dynamic testing.

◆ NOTE

- **PL d or higher according to EN ISO 13849-1 is achieved by use of switching elements / sensors with normally closed contacts and positive actuation according to EN 60947-5-1**
- **It is permitted to use devices for which switching elements the fault exclusion of double faults can be met for the desired safety level. Note the applicable rules of the EC Machinery Directive 2006/42/EC.**

2 Sensors / Dual-Channel Sensor and Use of 2 SDI in Combination with Time Monitoring and Test Pulses



Through the use of two independent clock signals on a homogeneous sensor, all cross-faults as well as connections to DC 24 V and DC 0 V can be detected.

For safety applications, only normally closed contacts are to be used for this purpose.

PL d or higher according to EN ISO 13849-1 can be achieved by use of sensors / switching elements with fault exclusion for not opening the switch contacts. This is permissible when using positively disconnecting switches with correct constrained actuation. The use of sensors with self-monitoring output contacts is also permitted.

◆ NOTE

- **PL d or higher according to EN ISO 13849-1 is achieved by use of switching elements / sensors with positive actuation**
- **Where two independent sensors with independent actuation are used, PL d or higher can be achieved according to EN ISO 13849-1.**
- **With the use of common elements in the actuation chain, a fault exclusion is required. The corresponding restrictions and criteria of EN ISO 13849-1 is to be observed.**

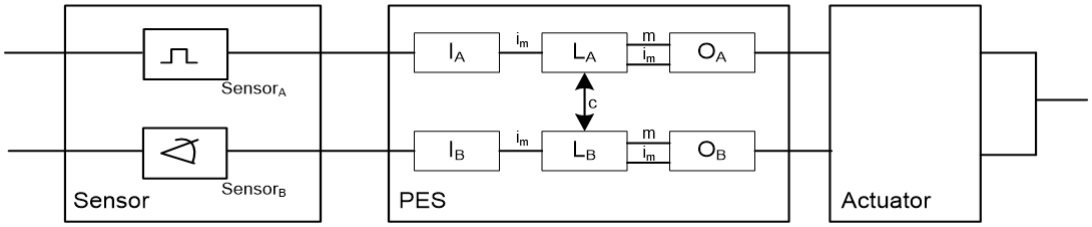
5.3.2 Safety-related specifications and wiring of position and speed sensors

5.3.2.1 General safety-related layout

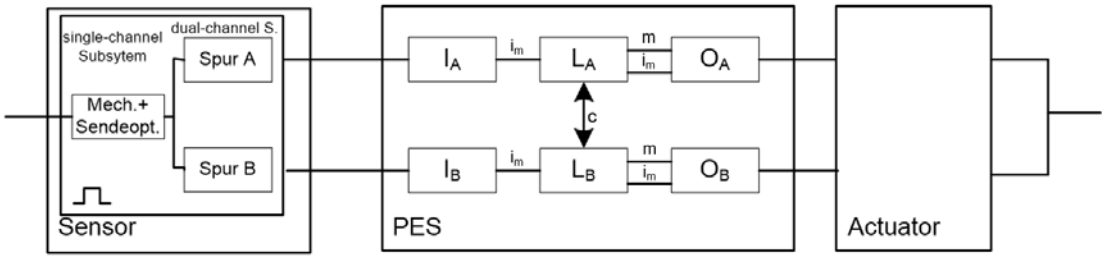
The safety part has external and internal encoder interfaces for connection to incremental, digital and absolute encoders common in the industry.

According to the encoder type and encoder combination, various safety levels can be achieved. For the corresponding subsystem the following system analysis is obtained:

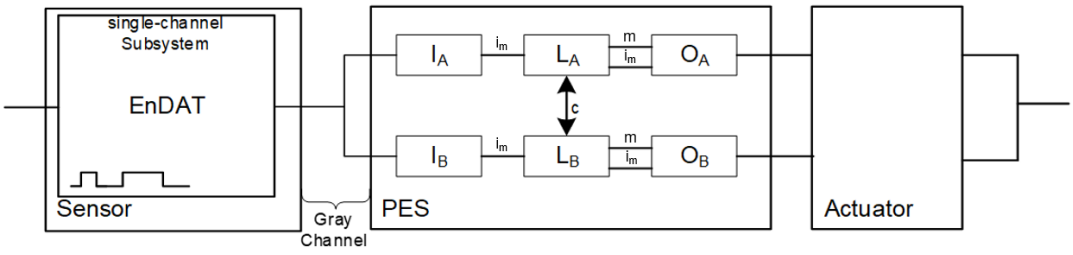
- **Dual-channel sensor system with separate signal processing in two channels, diagnostic through cross-comparison in the PES**



- **Sensor System with single and dual-channel subsystem (e.g., incremental encoder). Diagnostics by separate signal processing in two channels and cross- comparison in the PES as well as further specific diagnostics.**



- **Sensor System with single-channel subsystem (e.g., EnDat 2.2, Panasonic encoder). Diagnostics by separate signal processing in two channels and cross- comparison in the PES as well as further specific diagnostics.**



◆ NOTE

- **For a safety evaluation of the "Sensor System" the manufacturer's data (MTTFD, FIT-Numbers, etc.) and DC are to be used. For safe digital encoders (EnDat 2.2, Panasonic), the manufacturer's PFH value is to be used in the evaluation of the encoder system.**

5.3.2.2 General diagnostic measures for the encoder interface

For fault detection in the sensor system, a series of diagnostic measures are implemented in the safety part depending on the selected encoder types and their combination. The activation takes place automatically with selection of the encoder type.

In principle, the diagnostic measures can be classified according to their type and effectiveness:

Measure	DC [%]	Notation	Use
Cross-comparison of input signals with immediate and intermediate results in the logic (L) as well as timing and logical program execution monitoring and detection of static failures and short circuits (with multiple inputs/outputs)	99	Only to be used for: • Dual-channel sensor systems (two separate sensors), • the dual-channel subsystem of single-channel sensors • Diagnostics for the single and double-channel subsystem of specially suited sensor systems (SIN/COS-Encoder) • Dynamic operation / no standstill monitoring	Monitoring of dual-channel sensor systems and the corresponding subsystem of sensors for dynamic operation Not to be used for standstill monitoring!
Cross-comparison of input signals without dynamic test	80 to 95	DC is dependent on the frequency of the dynamic status, i.e., standstill or movement and on the quality of the monitoring measure. (80 to 90 % for incremental encoders, 95 % for SIN/COS encoders and digital encoders)	Monitoring of dual-channel sensor systems and the corresponding subsystem of sensors for non-dynamic operation. Especially to be used for standstill monitoring!
Monitoring of some features of the sensor (response time, range of analogue signals, e.g., electrical resistance, capacitance)	60	Diagnostics of specific sensor features	Monitoring of the single-channel subsystem of single-channel sensor systems

5.3.2.3 Encoder types and their combinations, diagnostic characteristic data

For SIL 3 EN 61508 and PL e according to EN ISO 13849-1, two independent, decoupled encoder systems are required.

Encoder 1	Encoder 2	Safe direction	Safe speed	Safe absolute position	Fault exclusion	DC [%]		
						Single-channel subsystem	Dual-channel subsystem dynamic	Dual-channel subsystem non-dynamic
NC	NC	-	-	-		-	-	-
Panasonic A6	NC	✓	✓	✓	Fault exclusion mech. Shaft fracture, form-locking encoder shaft connection required	90	99	90 to 95
Panasonic A6	Panasonic 3rd Party	✓	✓	✓		-	99	90 to 95
	ABZ	✓	✓	✓		-	99	90 to 95
	SSI	✓	✓	✓		-	99	90 to 95
	EnDat 2.2 (non-safety)	✓	✓	✓		-	99	90 to 95

5.3.2.4 Specific diagnostic measures in relation to the encoder type used

	Encoder type				
	Interface X10A/X10B				**Interface X9A/X9B**
	Panasonic 3rd party	**ABZ**	**SSI**	**EnDat 2.2 (non-safety)**	**Panasonic A6**
Supply Voltage Monitoring	✓	✓	✓	✓	✓
Plausibility Test Position Signal MPUA/MPUB	✓	✓	✓	✓	✓
Plausibility Test Speed Signal MPUA/MPUB	✓	✓	✓	✓	✓
Comparison of the Encoder Raw Values MPUA/MPUB	✓			✓	✓
Encoder Diagnostic According to Corresponding Safety Manual	✓			✓	✓
Difference Level Monitoring					
Monitoring of the Permitted Quadrants					
Monitoring of the Counter Signal Separated for Track A/B					
SIN/COS Plausibility Monitoring					
Input Signal Level Monitoring					
Clk-Frequency Monitoring			✓		

5.3.2.5 Safety-related shut-off thresholds and encoder systems for position and speed acquisition

As a basic measure, plausibility tests are carried out with the actual values for position and speed of the safety part between the two measurement channels A and B and tested against the parametrizable thresholds.

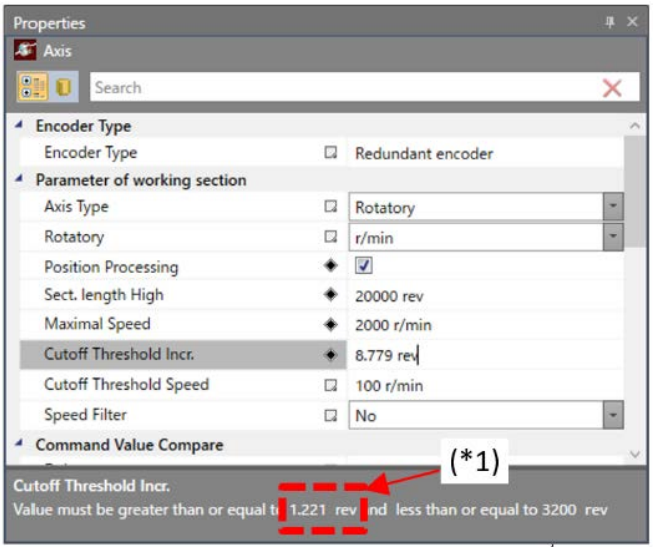
■ **Cutoff Threshold Incr.**

The incremental cutoff threshold describes the acceptable position variation between the two processing channels A and B in the units of the measuring system. The user has to carefully handle this parameter and configure an appropriate value of the incremental cutoff threshold for his application. The range of this the incremental cutoff threshold is taking account of small deviation in safety part and it is defined in PANATERM for Safety. The small deviation in safety part comes from position normalization due to avoid the use of CPU float calculation and additional diagnoses times.

The deviation depends on Sect. length High and encoder Resolution etc., and its value is shown in Cutoff Threshold Incr. Description area which is indicated dotted frame (*1) in below diagram.

The user has to take care the deviation when set Cutoff Threshold Incr.

- For instance, when the deviation is 1.221 rev and mechanical allowable deviation is 10 rev, then Cutoff Threshold Incr. may be set to 8.779 rev.



Deviation value of Cutoff Threshold Incr.

■ **Cut off Threshold Speed**

The speed cutoff threshold describes the acceptable speed variation between the two acquisition channels A and B.

Diagnostic functions are available within the SCOPE dialogue of the parametrization tool for determining the parameter values optimal for the application.

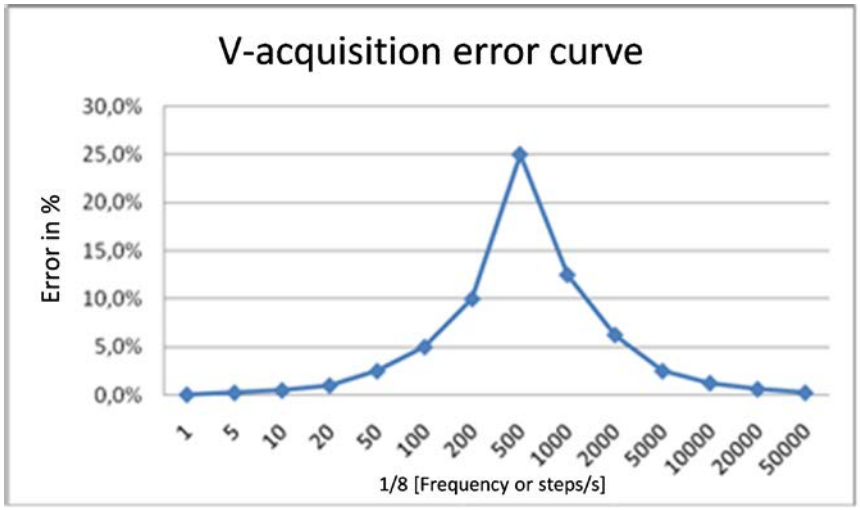
◆ NOTE

- **Speed and acceleration are acquired values with a minimum digital resolution. This situation limits the lowest speed and acceleration that can be acquired and sets the digital step width for the entered values.**

■ Speed Resolution

Speed is acquired using a frequency measurement procedure at a frequency of 4 kHz or

4000 steps/s; below that frequency a time measurement procedure is used. This results in the following acquisition error curve:



⚠ Safety Notes

- The error can be optimized by the appropriate selection of sensor resolution for each use case.
- For applications with limited resolution and/or time variance of the sampling signal, the functionality of the monitoring functions used can be improved by the use of a mean value filter. Digital interference from the sensors can be “smoothed” by using a mean value filter. However, this is accomplished at the cost of an increased response time of the entire system.
- The filter time can be adjusted variably between 0 and 64 in steps of 8. The dimension is “ms”. For determination of the response time of the entire system, the filter times must be added to the given response times of the safety part.
- For a safety evaluation of the “Sensor System” the manufacturer’s data (MTTFD, FIT-Numbers, etc.) are to be used.
- If the manufacturer requires specific diagnostics to safeguard the given safety-related characteristic data, these must be tested with respect to the specific encoder according to the table “Specific Diagnostic Measures for Position and Speed Sensors” above. In case of doubt, clarification by the manufacturer is required.
- The DC values provided in the table are to be used conservatively and the boundary conditions are to be maintained.
- For determination of the DC value for safety functions with standstill monitoring, it is necessary under such circumstances to evaluate the frequency of the dynamic status. As a guideline value, a DC of 90 % can be assumed.
- Troubleshooting is permissible according to the applicable standards. The boundary conditions laid out are to be maintained permanently.
- If multiple sensor systems are required for proper functioning of a single safety function, their component values are to be correctly combined according to the selected procedure. This also applies for a combination of digital and analogue sensors (e.g., safe reduced speed in the case of an open guard door = door contact + encoder for speed acquisition).
- Through appropriate selection of sensor system resolution, a sufficiently small tolerance in relation to each threshold of the individual safety functions can be achieved.
- When using the encoder input filter, the increase in response time is to be considered when evaluating the safety-related function.

5.3.2.6 Safety-related evaluation of the encoder types and their combinations

Due to the monitoring functions implemented in the MDSMD module, there are no special initial requirements of the internal layout of the encoder electronics, i.e. As a rule, standard encoders can be used.

In general, a safety-related evaluation of the overall layout is required. In doing so, the manufacturer's information regarding the encoder (FIT, MTTF) as well as the DC from the tables under DC Digital Sensors/Inputs are to be used.

When using single encoders, at a minimum a fault exclusion for the mechanical actuation chain as well as the single-channel component under observation is required for the applicable prescriptions of EN ISO 13849-1. The notes under 5.3.2 must also be considered.

PL d and higher according to EN ISO 13849-1 is generally attained by a combination of two encoders with essentially different technology and separate mechanical connection.

The use of a compact encoder with internal dual-channel layout with different technology is likewise suitable for uses up to PL e according to EN ISO 13849-1, albeit with consideration of the specifically required fault exclusions and their permissibility. As a rule, encoders with proven safety-related characteristics should be used whose safety level corresponds at least to the required level.

⚠ Safety Notes

- EMC measures such as guarding, etc. are to be observed.
- The use of standard encoders or a combination of standard encoders is permitted. For an overall layout consisting of encoders, further sensors / switching elements for activation of the safety function, the safety part and the shut-off channel, a safety-related evaluation is required. For determination of the attained safety level, among other things the data provided by the manufacturer (FIT, MTTF) and the DC indicated in 5.3.2 is to be referenced.
- When using only one encoder, the fault exclusion of a shaft break or fault in the mechanical encoder connection is required. For this purpose, appropriate measures should be taken, e.g. A positive mounting of the encoder using a groove and key or a locking pin. The applicable notes of the manufacturer as well as the requirements of EN ISO 13849-1 and the permissibility of the fault exclusion must be considered.
- For single encoders, preferably only encoders with proven safety-related characteristics should be used. The safety level of this encoder must correspond at least to the desired safety level of the overall layout. The notes of the manufacturer with respect to diagnostic measures, mechanical attachment and voltage supply measures are to be observed.
- SIN/COS Encoder: The internal layout of the sensor system must be designed such that the generation of output signals on the two tracks are independent from each other and common cause failures can be ruled out. Further, the mechanical layout is to be tested, e.g., the fastening of the encoder disc to the shaft. Preferably, encoders with proven safety-related characteristics should be used.
- When using compact encoders with internal dual-channel layout, for example SSI + incremental/SinCos, the notes of the manufacturer with respect to the safety-related characteristics, diagnostic measures, mechanical attachment and measures for voltage supply are to be considered. The safety level of the encoder must correspond at least to the desired safety level of the overall layout. Preferably, encoders with proven safety-related characteristics should be used.
- Using active position processing up to SIL3 EN61508 and Pl e EN ISO 13849-1, an absolute encoder must be used at least one of the two encoder interfaces.
- When using two equivalent sensors, remember that the sensor with the higher resolution is configured as Sensor 1 (process sensor) and the sensor with the lower resolution is configured as Sensor 2 (reference sensor).

The following general faults are detected by the MDSMD module:

- Shorts between the safety-related signal lines
- Interruptions of the safety-related signal lines
- Stuck at 0 or 1 on one or all safety-related signal lines

For every encoder type, further specific diagnostics are assigned for fault detection of the external encoder system. Each of the diagnostic measures are listed with the individual encoder types with the boundary conditions

⚠ Safety Notes

- By their nature, the diagnostic measures present tolerances resulting from inexact measurement. These tolerances are to be considered in the safety-related evaluation.
- The boundary conditions for each of the diagnostic measures are partially parametrizable and partly fixed. The resulting diagnostic coverages are to be evaluated according to the application and to be considered in the overall safety evaluation.

⚠ Beware

- The encoders must not be connected or disconnected during operation. Electrical components of the encoder interface could be destroyed.
- Turn off voltage to the connected encoder and this product before connecting or disconnecting the encoder connections.
- With externally supplied encoders, pay attention to switching off the external supply voltage (e.g. converter).
- For the data and clock signals and tracks A and B, twisted pair cables are to be used for signal transmission according to RS485. When selecting the wire cross-section, the current usage of the encoder and the cable length in the installation for the specific case are to be considered.

5.3.2.7 Sensor configuration

The most important input variables for the monitoring functions of the safety part are the safe position, speed and acceleration. These are generated in dual-channel fashion by the connected sensor systems. For PL e according to EN ISO 13849-1, an architecture corresponding to category 4 is required, i.e. continuous dual-channel acquisition with a high diagnostic coverage. For any single-channel elements (e.g., mechanical connection of the sensor / encoder with only one shaft/fastening), fault exclusions can be defined according to EN ISO 13849-2. For PL d according to EN ISO 13849-1, you can work with reduced diagnostic coverage. Taking into account the permissible fault exclusions according to EN ISO 13849-2, in certain circumstances even simple sensors may be adequate (speed monitoring only).

The safe configuration of the safety part must result from the safety application of the safety control.

These configuration data are created using the provided configuration tool (PANATERM for Safety) or through editing of configuration files. Please find more detailed information on configuration in the documentation of the provided configuration tool.

5.4 Actuator interface

5.4.1 Safety-related specifications and wiring of safe digital outputs (SDO)

The safety part provides 2 redundant safe semiconductor outputs (SDO). The semiconductor outputs are laid out in dual-channel fashion and are positive switching. The maximum possible safety category as well as the Performance Level is determined according to EN ISO 13849-1.

5.4.1.1 Diagnostics of safe digital outputs (SDO)

The safety part provides expansive diagnostic functions for the shut-off circuit. Certain diagnostic functions also include the external part of the shut-off channel.
Depending on the use of these diagnostic functions, different DC values result.

Internal Diagnostic Functions

Item	Description
Crosswise Reading of the SDO	The SDOs of the safety part are laid out in dual channels. The status of the output signals is continuously cross-compared. The SDO is set at the High level only when both output subsystems are at the High level, otherwise it is set at the Low level.
Cyclical Testing of the Shut-Off Capability of the SDO	In the turned-on state the SDOs are tested for correct function with a cyclical test pulse, in that the output is set at the Low value for a test period of < 500 us.

Diagnostics of the External Wiring (Parametrizable)

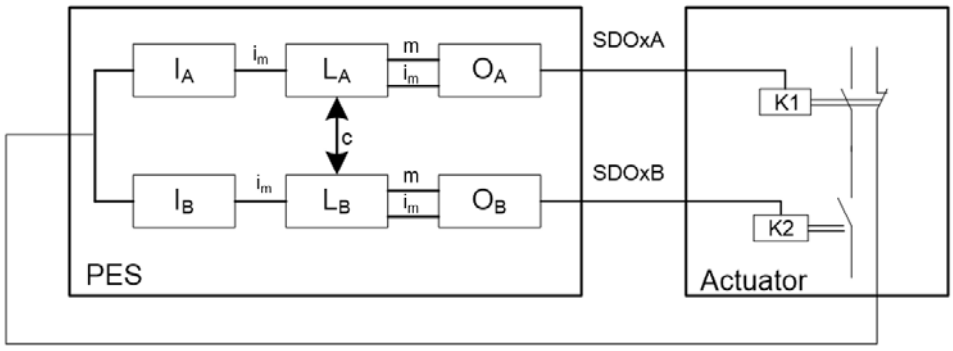
Item	Description
External Device Monitoring (EDM)	Is a function for monitoring of the switch position of external devices (actuators). The state of the actuator is read from its auxiliary contact (e.g., protective auxiliary contact) into the safety control, whereby positively driven contacts must be employed in the actuator. Turning on of the safety application is only permitted through the EDM function if the feedback circuit is closed. If for example the main contacts are soldered to a single contactor, then it is ensured by the positively driven contact that the auxiliary signal contact in the feedback circuit remains open and a fault is detected. In order to increase the DC, it is recommended to provide the auxiliary contact with a test pulse signal TDO. A testing by the EDM is only possible with the actuator turned off. For Performance Level d and safety category 3 as well as SIL 2 and HFT 1, a shut-off procedure must take place at least every 12 months. For PL e and safety category 4 as well as SIL 3 and HFT 1, a shut-off procedure must take place at least every month.

5.4.1.2 Architecture of the output elements

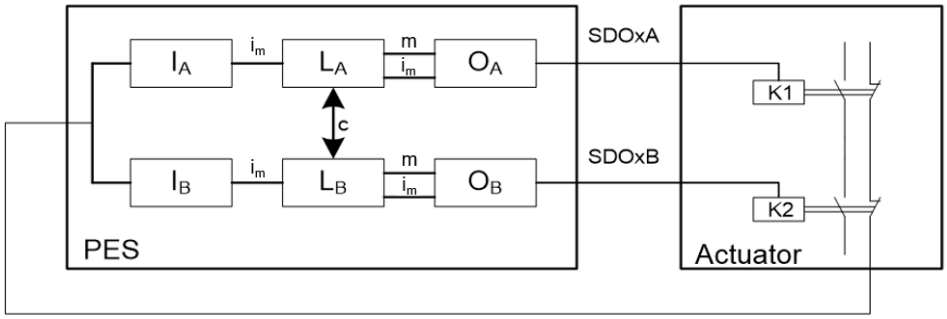
In this chapter the internal architecture of the outputs is described. The safe digital outputs are laid out redundantly and the SDO is only set at the High level when both channels give the enabling signal.

In the following explanations, a contactor (or relay) is taken as an example of an actuator.

- **Dual-channel output safety part and dual-channel actuator with at least single-channel diagnostic**



- **Dual-channel output safety part and dual-channel actuator with dual-channel diagnostic**



A diagnostic function internal to the device cyclically verifies the correct function of the digital outputs in the turned-on state. In this plausibility test, the binary output is set at its respective inverse value for the test period (< 500 µs), i.e., each output is briefly set to DC 0 V potential.

In case of detected faults, the safety part changes to the alarm/failure mode.

The safety part has complete separate signal processing paths for each safe output.

The safety part option provides expansive diagnostic functions for the output subsystem, in order to obtain the highest possible DC values. It is to be noted in particular that elements for switching amplification such as relays, contactors, etc. must be included in the shut-off circuit.

For the safety evaluation of the overall system, the DC values for the output sensor system in the Chapter “Diagnostic Values” can be used.

◆ NOTE

- **The maximum output capacity of each binary output is to be taken into account.**
- **For safety-related applications, only external switching elements with a minimum holding current (leakage current) of > 0,5 mA may be used.**

5.4.1.3 Overview of DC related to selected diagnostic functions

Measure	DC [%]	Notation	Use
Monitoring of the outputs through one channel without dynamic test	0 to 90	DC depends on the switching frequency In use of elements for switching amplification (external relays or contactors), only effective in connection with the reading function of the switch contact	Monitoring of electromechanical, pneumatic or hydraulic actuators / outputs
Redundant shut-off channel with monitoring of one of the driver-module elements	90	In use of elements for switching amplification (external relays or contactors), only effective in connection with the readback function of the switch contacts	Monitoring of outputs functioning directly as a safety circuit or Monitoring of safety circuits with elements for switching amplification or pneumatic / hydraulic control valves in connection with the readback function of their switch state
Cross-comparison of input signals with immediate and intermediate results in the logic (L) as well as timing and logical program execution monitoring and detection of static failures and short circuits (with multiple inputs/outputs)	99	In use of elements for switching amplification (external relays or contactors), only effective in connection with the readback function of the switch contacts For applications with more frequent demand of the safety shut-off, testing should be carried out at short intervals, e.g. at the beginning of each shift, 1 x per week. However, a test must take place at least once a year.	Monitoring of outputs functioning directly as a safety circuit or Monitoring of safety circuits with elements for switching amplification or pneumatic / hydraulic control valves in connection with the readback function of their switch state

5.4.2 Safety-related specifications and wiring of safe brake controls (SBC)

For brake control, the safety part provides a redundant safe semiconductor output (SBC) for each axis. The SBC output is laid out in a dual-channel manner and consists of a high/low combination.

The maximum possible safety category as well as the Performance Level are determined according to EN ISO 13849-1.

5.4.2.1 Diagnostics of the safe brake control (SBC)

The safety control safety part provides expansive diagnostic functions for the shut-off circuit. Certain diagnostic functions also include the external part of the shut-off channel.
Depending on the use of these diagnostic functions, different DC values result.

Internal Diagnostic Functions

Item	Description
Crosswise Reading of the SBC Output Signal	The SBC of the safety part is laid out in a dual-channel manner. The status of the output signals is continuously cross-compared. The SBC is set at the active only when both output subsystems are at High level, otherwise it is set at inactive.
Cyclical Testing of the Shut-Off Capability of the SBC	In the turned-on state the SBC is tested for correct function with a cyclical test pulse, in that the output is tested in the inactive state for a test period of < 500 us.

Diagnostics of the External Wiring (Parametrizable)

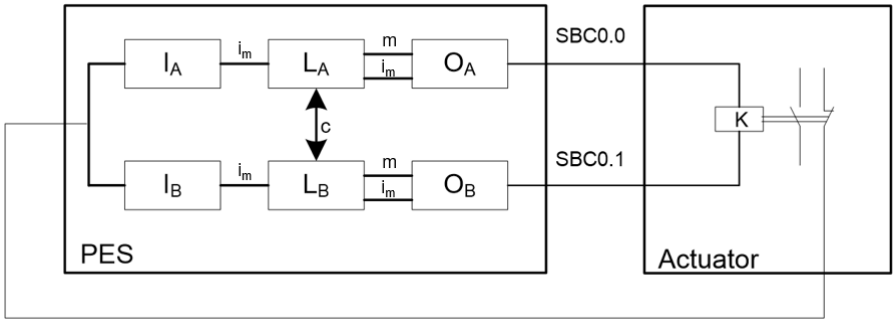
Item	Description
External Device Monitoring (EDM)	Is a function for monitoring of the switch position of external devices (actuators). The state of the actuator is read from its auxiliary contact (e.g., protective auxiliary contact) into the safety control, whereby positively driven contacts must be employed in the actuator. Turning on of the safety application is only permitted through the EDM function if the feedback circuit is closed. If for example the main contacts are soldered to a single contactor, then it is ensured by the positively driven contact that the auxiliary signal contact in the feedback circuit remains open and a fault is detected. In order to increase the DC, it is recommended to provide the auxiliary contact with a test pulse signal TDO. A testing by the EDM is only possible with the actuator turned off. For Performance Level d and safety category 3 as well as SIL 2 and HFT 1, a shut-off procedure must take place at least every 12 months. For PL e and safety category 4 as well as SIL 3 and HFT 1, a shut-off procedure must take place at least every month.

5.4.2.2 Architecture of the safe brake control (SBC)

In this chapter the internal architecture of the outputs is described. The SBC is laid out in a redundant manner and consists of a high/low combination. The output is only set at active when both channels give the enabling signal.

In the following explanations, a contactor (or relay) is taken as an example of an actuator. If you want to use dual-channel actuator, use configuration using SDOxA and SDOxB described in “5.4.1.2 Architecture of the output elements”.

- **Dual-channel output safety part and an actuator with single-channel diagnostic**



A diagnostic function internal to the device cyclically verifies the correct function of the SBC outputs in the turned-on state. In this plausibility test, the binary output is set at its respective inverse value for the test period (< 500 µs), i.e., the shut-off capability of each output is briefly tested.

In case of detected faults, the safety part changes to the alarm/failure mode.

The safety part has complete separate signal processing channels for each safe output.

The safety part option provides expansive diagnostic functions for the output subsystem, in order to obtain the highest possible DC values. It is to be noted in particular that elements for switching amplification such as relays, contactors, etc. must be included in the shut-off circuit.

For the safety evaluation of the overall system, the DC values for the output sensor system in the Chapter “Diagnostic Values” can be used.

◆ NOTE

- **The maximum output capacity of each binary output is to be taken into account.**
- **For safety-related applications, only external switching elements with a minimum holding current (leakage current) of > 0,5 mA may be used.**

⚠ Safety Notes
• The High-Side and Low-Side Outputs of SBC may not be used individually for safety tasks. Use for safety tasks is only permitted in combination of the High-Side and Low-Side.

5.4.2.3 Overview of DC related to selected diagnostic functions

Measure	DC [%]	Notation	Use
Monitoring of the outputs through one channel without dynamic test	0 to 90	DC depends on the switching frequency In use of elements for switching amplification (external relays or contactors), only effective in connection with the readback function of the switch contacts	Monitoring of electromechanical, pneumatic or hydraulic actuators / outputs
Redundant shut-off channel with monitoring of one of the driver-module elements	90	In use of elements for switching amplification (external relays or contactors), only effective in connection with the readback function of the switch contacts	Monitoring of outputs functioning directly as a safety circuit or Monitoring of safety circuits with elements for switching amplification or pneumatic / hydraulic control valves in connection with the readback function of their switch state
Cross-comparison of input signals with immediate and intermediate results in the logic (L) as well as timing and logical program execution monitoring and detection of static failures and short circuits (with multiple inputs/outputs)	99	In use of elements for switching amplification (external relays or contactors), only effective in connection with the readback function of the switch contacts For applications with more frequent demand of the safety shut-off, testing should be carried out at short intervals, e.g. at the beginning of each shift, 1 x per week. However, a test must take place at least once a year.	Monitoring of outputs functioning directly as a safety circuit or Monitoring of safety circuits with elements for switching amplification or pneumatic / hydraulic control valves in connection with the readback function of their switch state

5.4.3 Safety-related specifications and wiring of “safe torque off” (STO)

For safe retention, the safety part provides a redundant safe semiconductor output. For each axis an STO output is available. The STO output is laid out in dual-channel manner and consists of a 2x high/high combination.

The STO safety function ensures that no torque-building energy can act on a motor and an undesired start-up can be prevented.

The maximum possible safety category as well as the Performance Level are determined according to EN ISO 13849-1.

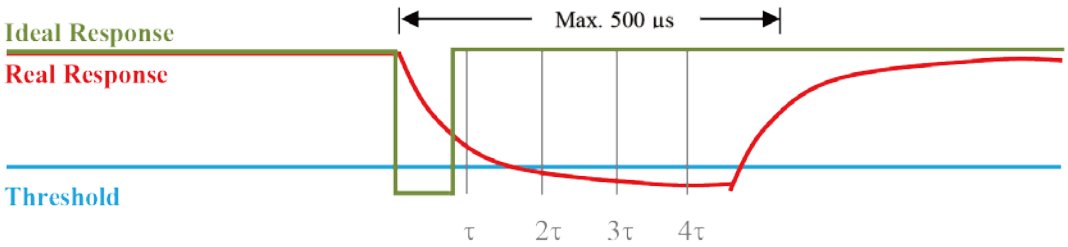
5.4.4 Permitted capacitive and inductive load on safe outputs

The safe outputs of the safety part have an OSSD character. That is, the outputs are cyclically shut off for testing purposes and the status is read back.

The testing of the shut-down capability yields the following criteria / functions:

- After shut-off of the output, the output voltage can be a maximum of 5.6 V.
- The permitted voltage level must be reached within 500 µs at the latest.
- If the permitted voltage level is reached, the test is considered successful and the output is activated again without further delay.
- If the permitted voltage level is not reached even after 500 µs, an alarm is triggered and various safe outputs (dual-channel for safe outputs!) are deactivated

The following depiction shows the ideal (green curve) and typical (red curve) response.



For determination of the maximum permissible capacitance or inductance, the time constant τ of the real RC and RL component of the output are to be taken into account.

This RC and RL component sets the following discharge curve:

The voltage level of max. 5.6V is reached safely after 3t.

Also applicable:

$3t \leq 350\ \mu s$

$t \leq 100\ \mu s$

In this context

$$t = R.C = \frac{L}{R}$$

the maximum usable capacitive or inductive load in connection with their resistive load be determined:

$$C_{max} = \frac{t}{R} = \frac{10^{-4}}{R} \quad \text{and} \quad L_{max} = t.R = 10^{-4}R$$

Typical values for the capacitance C are C=20 nF and for the inductivity L = 100 mH

6

Commissioning

6.1 General information

Prerequisite to a successful commissioning are:

- The correct development of the system.
- The correct and complete assembly of all components.
- The correct and complete wiring of all components.
- A complete programming environment with the necessary configuration tools.
- USB license dongle (password) for the PANATERM for Safety programming software
- Review, knowledge and understanding of the installation and programming handbooks of all components used.

⚠ Caution

Working with Electrical Components

Destruction of electrical components / risk of injury by electrical voltage.

- Perform wiring work only with appropriate qualification and in light of the safety instructions.
- Check the wiring and isolation before turning on the supply power supply.

6.2 Steps for commissioning

Ensure that the following points are carried out correctly and according to the application:

- The installation of this product
- The wiring
- The terminal assignment and cable routing
- The safety shut-off
- Prevent unintended start-up of the motor by suitable means.
- Take appropriate additional measures according to the application in order to avoid endangering persons and machines.
- Turn on the power, and where appropriate the DC 24 V I/O power supply
- Parametrize the devices according to the application
- Configure the field bus connections according to the application where appropriate
- Carry out a validation (see the chapter “Validation”).
- Create a configuration report.

⚠ Caution
Before the equipment being commissioned is put into regular use, a validation (see “8 Validation”) must be carried out.

6.3 Operating modes

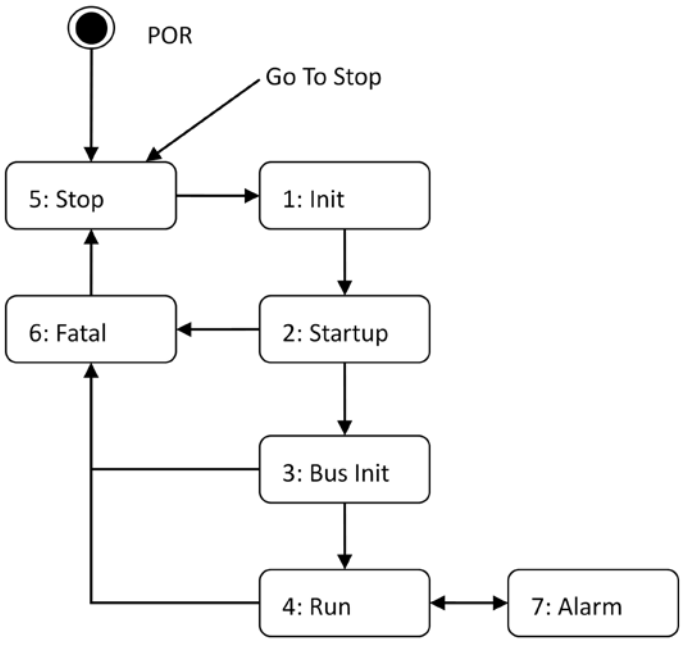
The following states are passed through and forwarded to the servo control part for diagnosis (display by the front side 7-SEG) after each new start and fault-free running of the safety part.

State No.	7-SEG	State Name	Description
“1”	“1”	INIT	Initialization of the MPUs and operating system (OS). All outputs are switched off – Safe state.
“2”	“2”	STARTUP	Initialization of the user application. All outputs are switched off – Safe state.
“3”	“3”	BUS INIT	Initialization of the field bus. All outputs are switched off – Safe state.
“4”	“4”	RUN	System in RUN state. Normal system operation. All outputs are switched according to the current logic status.
“5”	“5”	STOP	System is in STOP state. In stop mode parameter and program data can be loaded externally. All outputs are switched off – Safe state.
“6”	“F”	FATAL	System is critical failure (FATAL) state. All outputs are switched off – Safe state. Fault can only be reset by re-turning on the power of the safety part.
“7”	“A”	ALARM	System is ALARM state. All outputs are switched off – Safe state.
	“E”	MUTED ALARM	System indicates ECS-, ICS- or ACS-alarm state BUT it stays in RUN state.

■ Main State Machine (MSM)

The main state machine is the global device state, which determines the operation of each function of the safety part.

It is visible to the user via diagnosis data (Tooling and 7-SEG displays on the driver module).



Go To Stop: A transition to Stop issued by the user (tooling) is possible in all states

6.4 Reset function

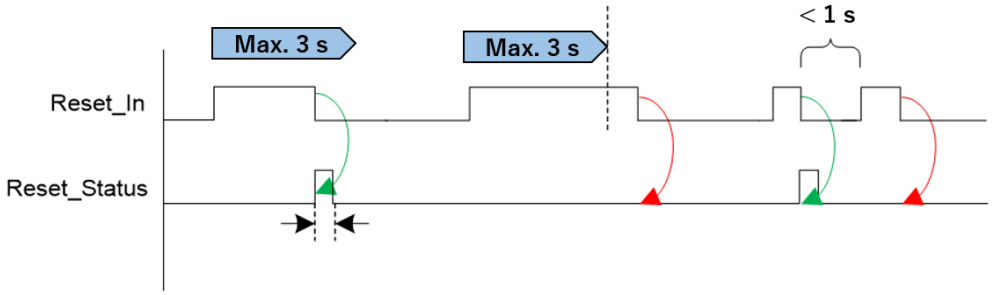
The reset function can be divided into a start-up function after return of voltage (general reset) and a status/alarm reset (internal reset). The latter is triggered by bus (CoE). The table below gives an overview of the reset functions and their effect.

Reset Type	Triggering element	Note
General Reset	Voltage return / equipment start-up	Reset function after a complete shut-down and start-up of the device.
Internal Reset	Reset input	Triggering of the internal reset by configuration of a reset input
	CoE	Triggering of the internal reset by CoE
	Servo Driver-Module Reset	Triggering of the internal reset by servo driver module

6.4.1 Reset timing

The reset input for the internal reset is time-monitored in “RUN” mode. An internal reset is triggered with falling slope of the reset input under the condition 4 ms < T < 3000 ms between increasing and decreasing slope.

The time interval between 2 reset signals is time-monitored. A second reset is allowed after a certain period of time (≥ 1 s) from the first reset is elapsed.



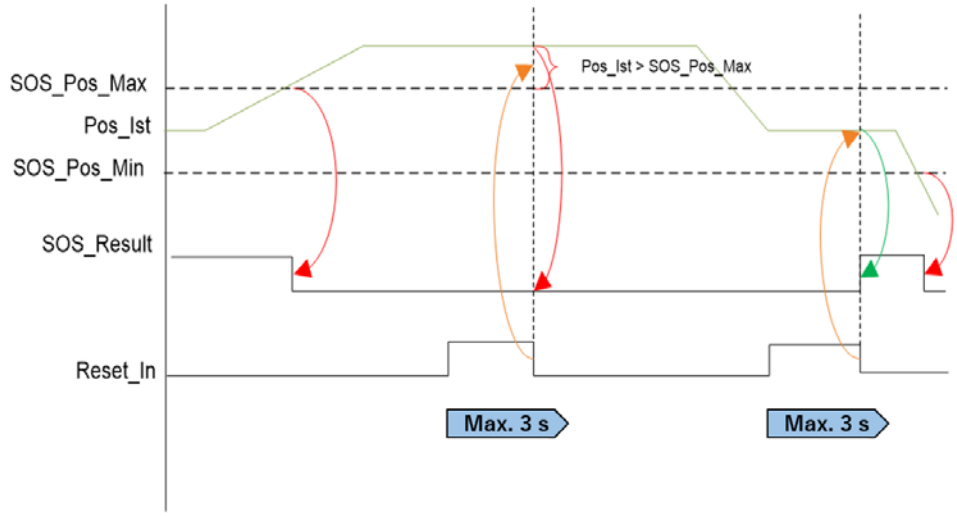
6.4.2 Reset behaviour

Functional Unit	General Reset	Internal Reset	Function
Fatal error	✓		Reset failure
Alarm	✓	✓	Reset alarm
Monitoring functions	✓	✓	Reset of a requested monitoring function
Flip-Flop	✓	✓	Status = Reset
Timer	✓	✓	Timer = 0

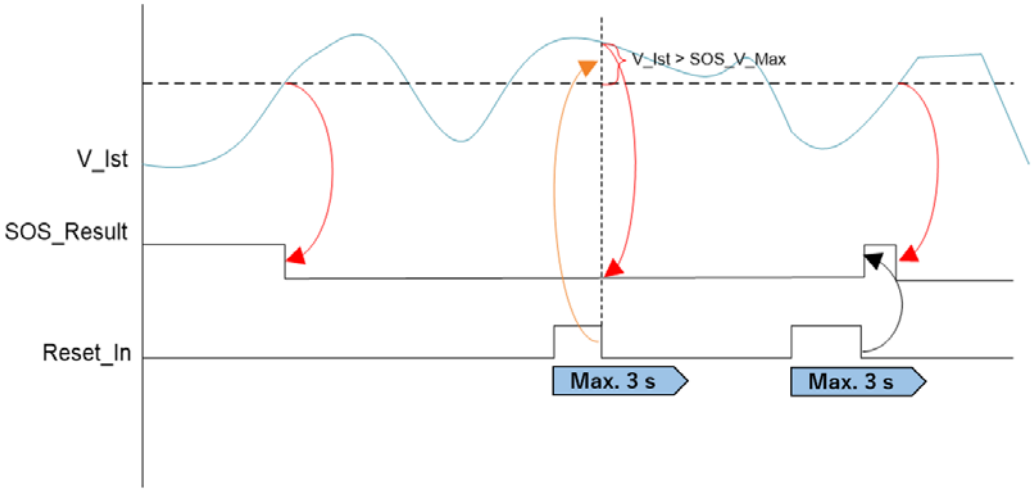
The status of the monitoring function is re-established after a reset.

- The reset of an SMF (Safe Monitoring Function) whose process values continue to exceed parametrized boundaries leads does not lead to changing of the output status of the affected SMF.
- Time-based functions - timers cause a reset of the output status of the monitoring function. A reaction occurs only upon renewed monitoring of the parametrized boundary values.

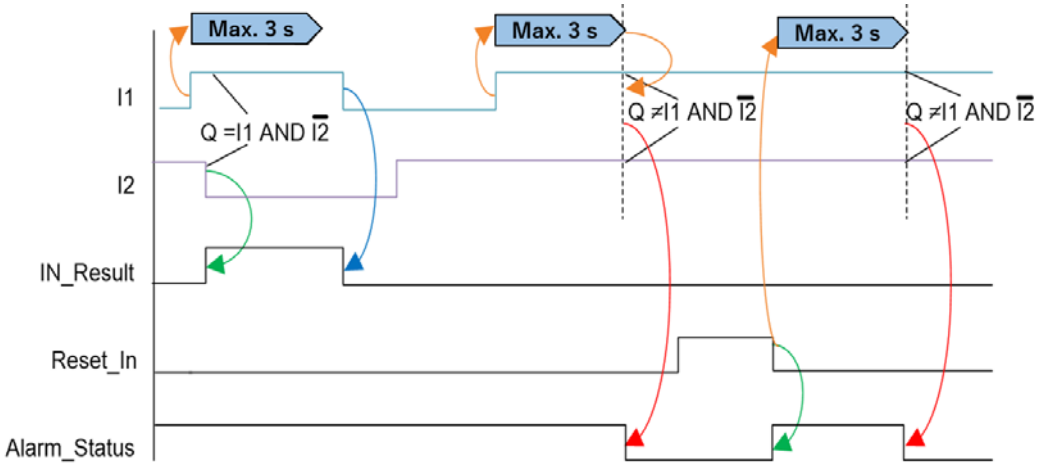
■ **Process value (position) outside of the parametrized boundaries → no change to the output status upon reset in the alarm condition**



■ **Process value (speed) above parametrized boundary → no change to the output status upon reset in the alarm condition**



■ **Time-based function → reset of the output status, reaction upon renewed monitoring of the boundary**



⚠ Safety Notes

- For time-based functions, e.g. Time-monitoring of complementary input signals, the output condition is reset and is not detected as a failure condition until renewed exceeding of the (time) boundary.
- To ensure against incorrect use, e.g., repeated triggering of the reset function for avoidance of an alarm condition, a suitable measure in the PLC programming must be taken where appropriate.

7

Configuration and Parametrization

7.1 Configuration and parametrization

The safety part has a configuration which is intended for the processing of safety functions.

These configuration data are created using the provided configuration tool (PANATERM for Safety) or through editing of configuration files and contain the settings of the device, encoders, axes, test sections and the interconnection of the safety functions in the logic (PLC program).

The configuration data are sent by the PANATERM for Safety to the safety part and are stored there as a standard configuration in (non-volatile) flash memory.

Please find more detailed information on configuration in the documentation of the provided configuration tool.

◆ NOTE

Functional Validation

- **In order to guarantee safety of the safety part, a functional test of the safety functions must be carried out at least once in a year. For this purpose, the elements used in the parametrization (inputs, outputs, monitoring functions and logic elements) must be tested with respect to their function and shut-down.**

8

Validation

8.1 Validation

Every implemented safety function must be validated in order to ensure correct functionality and reliability.

The validation of safety functions is to be carried out to a sufficient degree to verify the correct implementation of the planned measures for risk reduction. A guide for this is given by applicable standards such as EN ISO 13849-2 or DIN EN 61508 among others. Accordingly, the validation at varying levels according to the following guidelines should include:

- Validation of the safety function in the programming tool.
- Additional validation of the safety function in the completed machine.
- Carrying out of functional tests of the diagnostic measures and shut-downs in case of failure.
- Carrying out of fault recognition measures, whereby a correct cabling can also be tested on the machine.

The validation of safety-related controls should include a detailed analysis and failure simulation where appropriate, in addition to the functional testing.

This analysis should take place at the beginning of the design process in order to recognize problems early.

The scope of the analyses and tests carried out in the framework of the validation depends on the complexity of the control and its connection to the machine or equipment.

A validation record should be created for the validation. Depending on the complexity of the control or machine to be tested, this record includes the following information:

- Requirements for completion of the validation
- Operating and environmental conditions of the validation
- Fundamental and proven safety principals which were used and whose implementation must be validated.
- Proven components used - specifications and validation of use
- Failure presumption and fault exclusion
- Analyses and tests used
- Safety function of the controller or machine - functional description and test guide

In order to maintain the performance of safety-related controls after commissioning and validation and to provide safety, a regular service and maintenance with periodic tests is required. The periodic tests should be laid out in the validation plan.

In the following Chapters, the validation of individual machines and mass-produced machines is differentiated. On this point, take note:

- The validation of the prototype of a mass-produced machine follows the same principles and procedures as the validation of an individual machine or equipment.

8.2 Validation of an individual machine or equipment

8.2.1 Prerequisites for the analysis and validation of safety measures in the control

A sufficient analysis of the implementation of safety measures in the control can only take place on the basis of planning and documentation suitable for a safety-related requirement. Thus, in the following chapter, guidelines are provided in addition to the analyses to be carried out.

The analysis requires further-extending knowledge of the operating principle and the scope of the diagnostics carried out by the control, the categories attainable by the same, the exactness / fault tolerances as well as response times and their dependence on other parameters. These are laid out in the corresponding chapters of the handbook.

8.2.1.1 Design of the safety functions

The analysis of the implemented safety functions is fundamentally supported by the type and method of the design, program layout and program input of the safety-related part of a control. The safety functions should be clearly assigned and limited to their planned tasks. They are to be sufficiently described during design, especially:

- The activation parameters (e.g., selection of a certain driver-module type, emergency-off activated, access door opened, light curtain demanded, etc.) are to be clearly named
- Standard monitoring functions used where appropriate should be cited including their parameters (e.g., SLS with shut-off threshold, SOS and their response threshold, etc.)

Further, the safety-relevant equipment components determined during the design, as well as their characteristics, should be documented sufficiently for later review. This includes in particular:

- Type and scope of the planned control components (e.g., safety part in stand-alone)
- Purpose, type and characteristics of control devices, position and condition indicators (e.g., mode switch, dual-channel emergency shut-off, single or dual-channel limit switch, etc.)
- Type and characteristics of special sensors (e.g., speed and/or position sensors, structure of the acquisition being single or dual-channel, resolution and setting parameters)
- Finally, during planning possible failures of the safety-related components should be analyzed and their diagnostics and countermeasures should be designed. Diagnostics and countermeasures can be designed into the application through corresponding program functions as well as using the diagnostic functions in the safety control. Particularly to be understood among these failures and diagnostics:
- Failure of switch parts in control devices or position indicators and their diagnostics (e.g., dual-channel emergency shut-off with monitoring, expectations, etc.)
- Short circuits in the peripheral wiring and their diagnostics (e.g., use of pulses, complementary switching parts or expectations)
- Failure in special sensor systems such as speed and position sensors as well as their diagnostics (e.g., structure of the acquisition, diagnostics carried out by the control and their designations)

8.2.1.2 Program layout and input

A structured programming and program in put forms the foundation of later validation. The PANATERM for Safety software was developed specifically for safety controls and offers an excellent platform for a programming and program entry that is structured, clear, and individualized to the safety function.

It is strongly recommended to use a sheet-by-sheet layout as well as functional assignment. For good readability and review, the following rules should be observed:

- The programming should be planned before the actual entry, and logic functions should be sufficiently described in the design (e.g., truth table, etc.)
- During program entry, good readability should be maintained, connecting lines for the logic functions and other signals should be well separated from each other and kept from crossing as much as possible.
- Turned-on components should be identified with their abbreviation and the function-identifying description in the circuit diagram.
- Signal pre-processing with multiple applications should be entered on separate pages with signals clearly identified.
- Safety functions and their activations should be clearly arranged, where appropriate in a sheet-by-sheet fashion. Sheets should be named appropriately to the safety functions.
- Shut-off channels that are called upon by multiple safety functions should likewise be entered on separate sheets with clear identification.

8.2.2 Theoretical review and analysis of the implemented safety functions

After completed planning and programming of the safety functions, it is recommended to carry out a theoretical review and analysis of the safety measures before commissioning. This review should be repeated iteratively according to the actual conditions and procedure if during commissioning adjustments and additional or modified functionalities are implemented. The review and analysis consist of the parts:

- Review of the attained Performance Level according to EN ISO 13849-1 and the attained SIL according to EN ISO 61508.
- Review of the correct implementation of the provisions for the components used and their failure diagnostics.
- Review of the correct implementation of logic functions and standard safety functions.
- Analysis of the achievable response times and their review in relation to the design provisions.

8.2.2.1 Review of the performance level according to DIN EN ISO 13849-1 and SIL according to DIN EN 61508

After completion of the planning it must be determined whether the required Performance Level (PL r) and SIL determined during the risk evaluation procedure are achieved by the selected system and the selected components, their characteristics and the diagnostics to be used for each safety function.

◆ NOTE

- **In order to validate the achieved Performance Level and SIL, the safety parameters given in the respective handbooks (PFH and Category, suitability for SIL, etc.) should be used.**
- **For the set categories and safety-related structures as well as the classification of the diagnostics available in the safety control and actually used, the data in the handbook should be considered.**
- **The actual determination of the PL and SIL is to be carried out according to the standard provisions. The applicable literature on this topic is expressly referenced here.**

Those persons entrusted with carrying out this review must have sufficient knowledge of the calculation procedures and their fundamental principles.

For the review of the Performance Level According to EN ISO 13849-1, it is recommended to carry out the theoretical review using the free software tool SISTEMA.

8.2.2.2 Review of the correctly-designed implementation of components and functions

After completed entry, the components and logic functions as well as the functions of the safety control should be tested for their fundamental criteria and completeness. It is recommended that this be carried out using a hard copy of the program. Given a structured program entry and consideration of the labelling (see above), a review can be carried out in a simple and clear manner. Where appropriate, after corrections to the program entry and additional labelling should be implemented if no clear assignment can be determined during the review. This also assists in the later practical review of the designed functionality.

8.2.2.3 Determination and review of response times

The response time is an important safety-related characteristic and should be considered for every application / application-specific safety function. In the following chapter, the response times for individual functions are listed, also potentially dependent on further parameters. If these entries are not sufficient for a specific application, the time behavior should be validated against the expected behavior through separate measurements. This applies in particular to the use of filter functions.

⚠ Danger

Significant impairment of safety in case of incorrectly defined response times

The response times are to be determined according to the safety function of each application and should be compared with the actual values using the following data.

Special caution should be taken when using filter functions. According to filter length and time, a significant extension of the response time can arise that should be taken into account during the safety-related design.

For especially critical tasks, the time response should be validated by measurements.

Upon device start-up / alarm or failure reset, under some circumstances (depending on the application program) the outputs can become active during the entire response time. This should be taken into account when planning the safety functions.

Response times in standard operation

The cycle time of the safety part system is foundational to the calculation of response times.

This time is **T cycle = 4 ms**.

The given response times correspond to the maximum duration for each specific use case within the safety part.

According to the use case, further application-dependent response times of the sensor system and actuators used must be added in order to obtain the overall duration.

Function	Response Time [ms] (Note 2)	Explanation
Activation of digital output through digital input	8	Reading of the input information and switching of the output (output information).
Deactivation of digital output through digital input	8	Reading of the input information and deactivation of the output (output information).
Activation of a monitoring function by ENABLE with following shut-down over digital output	12 (Note 1)	Activation of a monitoring function through the ENABLE signal.
Response of an already activated monitoring function including PLC processing for position and speed processing over digital output	12 (Note 1)	In case of a monitoring function activated by ENABLE, the module requires one cycle to calculate the actual speed value. In the next cycle after being calculated the information is further processed by the PLC and reported, i.e., after logic is implemented this leads to (for example) switching of an output.
Mean value filter (for settings see the encoder dialogue in PANATERM for Safety)	0 to 32	Group runtime of the averager. This runtime affects only the monitoring functions in connection with position / speed / acceleration, but not the logic processing.

(Note 1) When using an averager, its response time must be added.

(Note 2) This response time indicates only the time spent at the CPU. The actual response time from safe digital inputs to outputs must add maximum 2 ms.
E.g. The maximum response time of STO is 10 ms (= 8 ms + 2ms).

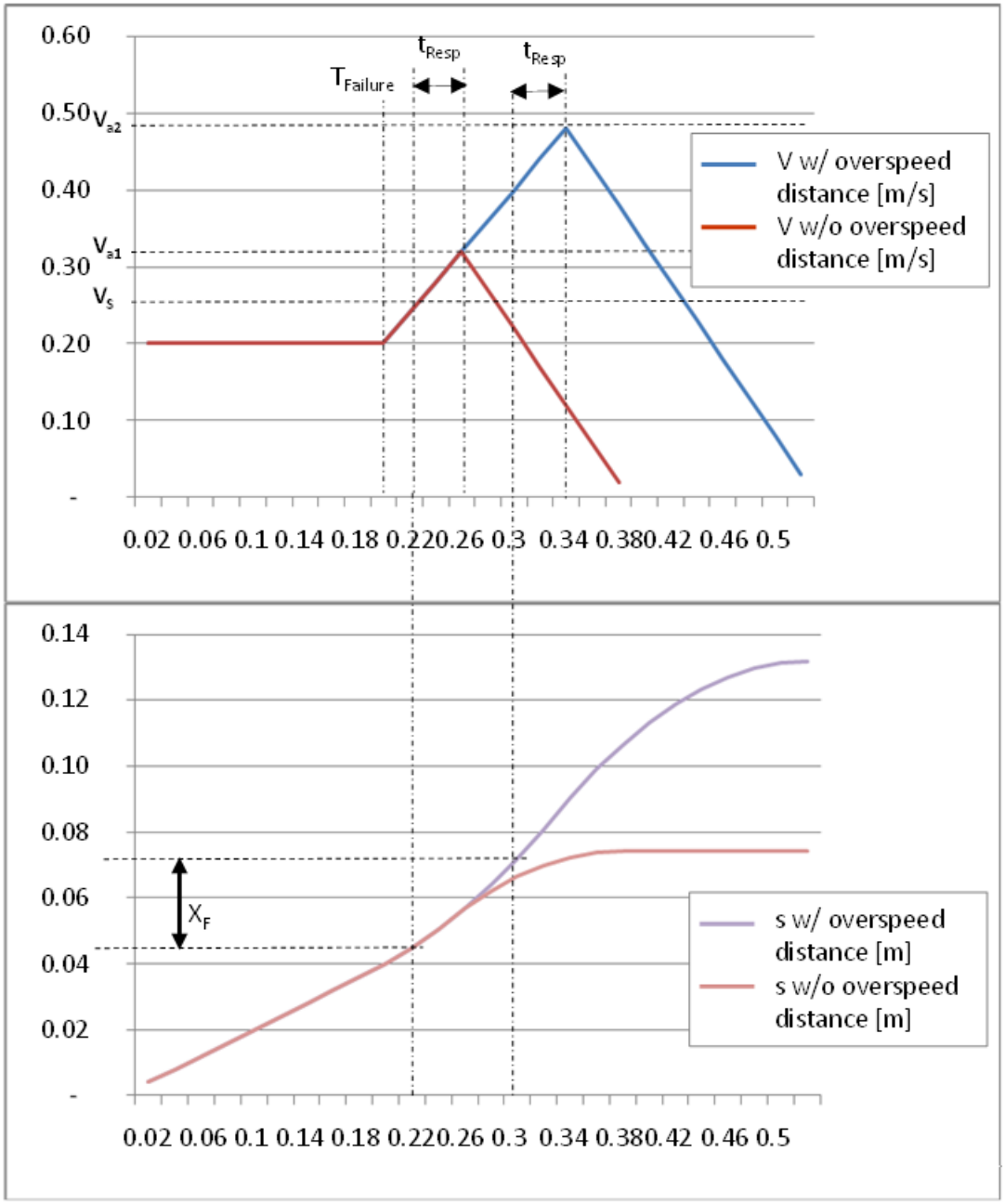
Response times for distance monitoring failure

For the calculation of the worst-case condition, the following calculation scheme is available:

System speed at the sampling time	V(t)
System speed upon response of the safety part	V_A
Threshold for monitoring (SLS or SCA)	V_S = constant for all t
Parametrized filter value	X_F = constant for all t
Maximum possible acceleration of the application	a_F = constant for all t
Delay after shut-down	a_V = constant for all t
Sampling time for occurrence of a worst-case event	$T_{Failure}$
Response time of the safety part	t_{Resp}

For the worst-case consideration, it is assumed that the driver module initially moves at a speed V_K exactly at the parametrized threshold V_0 and then accelerates at the maximum possible value a_0.

■ **Diagram 1: Response of the driver module with and without overspeed distance**



For the curve **V** and **s <u>without</u>** overspeed distance the following relationships are found:

Parameter	Calculation method	Note
t_{Resp}	Value from safety part response time data + delay in the external shut-off chain	Delay in the external shut-off chain from relay / contactor, brake manufacturer data etc.
a_F, a_V	n.a.	Estimation from application
V_{a1}	$= V_S + a_F * t_{Resp}$	

For the curve **V** and **s <u>with</u>** overspeed distance the following applies:

Parameter	Calculation method	Note
t_{Resp}	Value from safety part response time data + delay in the external shut-off chain	Delay in the external shut-off chain from relay / contactor, brake manufacturer data etc.
a_F, a_V	n.a.	Estimation from application
V_{a2}	$= a_F * t_{Resp} + (V_{S2} + 2 * a_F * X_F)^{1/2}$	

◆ NOTE

- **The action of the filter displaces upward the set speed threshold V_a by an amount ΔV_{Filter}. For the application the new values of the response time ($T_{Resp} = T_{safety}$ part + T_{Filter}) as well as the resulting speed upon shut-off by the safety part are to be taken into account.**

8.2.3 Practical implementation of validation after successful commissioning

To ensure correct functioning of all implemented safety functions, a check and documentation of the parameters and logical connections must be carried out by the user after completed implementation, commissioning and parametrizing. This is well supported by the PANATERM for Safety software in the form of a configuration report.

As previously preliminarily mentioned, the validation of the safety functions should also be planned within the framework of their design. The PANATERM for Safety validation report can be used, but an understanding of the individual safety-related characteristics of the safety part is also required.

The design of the safety part is based on the following basic presumptions:

- Parameter data and PLC program code that is stored in the flash memory of the safety part cannot change on their own. Online tests and corresponding signatures ensure the same in the course of basic measures.
- The correctness of a configuration cannot be evaluated by the safety part. This affects the parametrization of sensors, threshold values, and boundary values which are to be tested in the validation by suitable means.
- In order to ensure correctness of the parametrization, it must be reviewed by an expert.
- After a successful commissioning, it must be documented by the user that the specifications match the data of the configuration report and the parameters on the safety part.
- The parametrized values for the test section, sensors and monitoring functions must be individually reviewed by the user in the course of a functional test and be validated and recorded.
- The PLC functions programmed by the user must be reviewed in a suitable way and be validated and recorded. To this end it is recommended that the design provisions be directed to a later review and to carry out the program entry so that the safety part can be practically tested.

8.2.3.1 Configuration report

It is expressly recommended that the validation of the safety module be carried out using a configuration report available through PANATERM for Safety. Alternatively, a custom validation report can be made that documents the following validations.

Layout of the configuration report

The configuration report contains the following data:

- A header region for entry of general project data as well as individually selected checksums (see the following description)
- Documentation of the logical programming using a list of instructions (PLC code)
- Listing of the inputs and outputs used and their parametrization
- All monitoring functions used and their parameters

Creating a configuration report

The configuration report directly reads the programmed codes and parameters contained in the target device. Thus, the report can only be generated with the device connected to PANATERM for Safety.

The function call for generation of the validation report is carried out in the connection dialogue of the parametrizing software PANATERM for Safety and is only possible with an active connection to a safety part.

The data necessary for the report are reported by the connected device and are laid out in readable format in a PDF document. The location of the saved document can be defined by the user upon creation.

The fields to be edited can be edited directly in the PDF document. The documentation of the validation can be carried out by a print-out of the configuration report.

Filling out the configuration report

The configuration report is to be filled out as follows:

- Fill in the equipment-specific data in the “Header” field. These data have an informative status but should be adjusted in content and scope according to the point of delivery / tester.
- The individual data and functions intended to be reviewed each contain review fields which can be filled in for correct testing / matching, e.g., by “checking off” or entering an “x”.
- Check the indicated data in the header (serial number device type, CRC, the configuration) to see if they are identical with the module data and document this review
- Validate the PLC logic program and ensure that the functionality carried out corresponds to the specified functionality.
- In the input/output area, check to see if each entry matches the actual connection of the safety part.
- Check to what extent all safety functions (E.g., SLS, SCA, etc.) match the set design parameters.

◆ NOTE

- **The correct program and parameter data must be loaded for creation of the configuration report for validation.**
- **All listed parameters and program instructions must be validated for the equipment / machine and confirmed in the configuration report.**
- **The tester must validate all configured data in the configuration report by appropriately reviewing all set boundary values of the monitoring functions being used.**
- **The list of PLC instructions primarily serves for documentation. Correct programming should primarily be tested through appropriate stimulation of the logic functions. A review using the PLC instruction list requires expert knowledge and should only be used where the stimulation method cannot be used.**
- **The practical execution of the validation should be carried out directly at the protected machine or equipment. For validation at least the following documents should be available:**
  - **Service manual of the machine or equipment with warning notes**
  - **Circuit diagram of the overall control equipment**
  - **Documentation of the design of the safety-related part as previously described.**
  - **Configuration report in electronic or printed form**

The actual execution should be carried out on the basis of the following guidelines:

(1) The connected components such as control devices, sensors and actuators should be reviewed for the correct connection. This review should be done primarily by activating / stimulating the sensors and checking the status indicator of the safety part.

(2) In use of diagnostic functions such as pulse assignment, a check should be done, e.g., by shorting the pulse, etc.

(3) Insofar as safety functions are employed that use speed and/or position data, the correct acquisition of the speed and/or position is to be checked initially. This test is possible through the selectable diagnostic functions in the PANATERM for Safety for speed and position. In the process, the indicated speed and position should be checked with a suitable device. This test is prerequisite, must be carried out, and cannot be replaced with a theoretical review.

(4) It is also recommended to carry out a test of the diagnostics of the speed and position sensor. This can be done by disconnecting a sensor or a sensor line.

(5) The logic functions are to be checked in relation to the design provisions. This should be done primarily through corresponding stimulation of the inputs, etc. and the effect (e.g., activation of a monitoring function or shut-down of an output) should be tested.

(6) The set parameters of monitoring functions should not only be checked for correspondence to the design provisions but also by exceeding the parametrized boundary conditions and observing the response.

8.2.3.2 Locking the configuration

Locking the configuration is the final step of the validation. Locking means the confirmation of a positive completion of the validation and may be done only in such a case.

Locking can be done using the command tool (PANATERM for Safety).

9

Maintenance

9.1 Safety notes for device maintenance

Caution

Safety Notes for Device Maintenance

If the malfunction occurs, the device must be serviced or replaced by the professional company authorized by Industrial Device Solution Business Unit, Panasonic Corporation.

The other handlings of the device may invalidate warranty.

9.2 Changes to the board of the safety part

- Changes to the hardware are to be made exclusively by the manufacturer.
- Changes to the firmware (firmware update) are to be made exclusively by the manufacturer.
- Changes to the firmware parameter are to be made exclusively by the manufacturer.
- Repairs are to be done exclusively by the manufacturer.

◆ NOTE

- **All safety authorizations and all warranties are terminated upon internal manipulation by the user (e.g., exchange of components, soldering by the user)**

9.3 Device exchange

Upon exchange of the safety part, the new module must be refurnished with corresponding project data.

The CRC (Cyclic Redundancy Check) must be identical before and after the exchange

If this is not the case or no data recovery from the old safety part is possible, then a new approval / validation must take place.

For a corresponding exchange the programming software PANATERM for Safety is required.

9.4 Disposal

Please follow the national regulations on disposal of electrical devices.

The crossed-out trash can symbol means that electrical and electronic devices and their accessories must be separated from general household waste.

The materials can be reused as indicated on their identifications. By reusing, material recycling or other forms of recycling of old devices, you make an important contribution to the protection of our environment.

Dispose of the individual parts separately as appropriate according to their composition and the existing national regulations, for example as:

- Electronic waste
- Metal products
- Metal
- Copper

10

EC/EU Directives and Standards

10.1 EC/EU directives

The following EC/EU directives have been made applicable to the development, operation and validation:

Directive 2006/42/EC	Machinery Directive
Directive 2014/35/EU	Low Voltage Directive
Directive 2011/65/EU	RoHS Directive

10.2 Standards

For validation of the conformity of the system with the directives, the following non-legally-binding European standards are used.

10.2.1 Normative for functional safety

Standard	Title	Edition
IEC 61508	Part 1-7: Functional safety of electrical/electronic/programmable electronic safty-related systems	2010
EN ISO 13849-1	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	2015
EN ISO 13849-2	Safety of machinery - Safety-related parts of control systems - Part 1: Validation	2012
EN ISO 13850	Safety of machinery - Safety-related parts of control systems - Part 1: Validation	2012
EN 62061	Safety of machinery - Functional safety of safety-related electrical, electronic, programmable electronic control systems	2015
EN 61800-5-1	Adjustable speed electrical power drive systems. Part 5-1: Safety requirement - Electrical, thermal and energy	2007 + A1:2016
EN 61800-5-2	Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional.	2017
EN ISO 12100	Safety of machinery - General principles for design - Risk assessment and risk reduction	2011 + A1:2013
EN 60204-1	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	2019

10.2.2 Normative for EMC

Standard	Title	Edition
EN 61800-3	Adjustable speed electrical power drive systems - Part 3: EMC requirements and specific test methods.	2018
EN 61000-6-2	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments	2019

10.2.3 Normative for electrical safety and environmental requirements

Standard	Title	Edition
EN 50178	Electronic equipment for use in power installations	1997
EN 61800-2	Adjustable speed electrical power drive systems - Part 2: General requirements - Rating specifications for low voltage adjustable speed a.c. power drive systems	2015
EN 60721-3-1	Classification of environmental conditions - Part 3 Classification of groups of environmental parameters and their severities - Section 1: Storage	2018
EN 60721-3-2	Classification of environmental conditions - Part 3: Classification of groups of environmental parameters and their severities - Section 2: Transportation	2018
EN 60721-3-3	Classification of environmental conditions - Part 3 Classification of groups of environmental parameters and their severities - Section 3: Stationary use at weather protected locations	2019
EN 61131-2	Programmable controllers - Part 2: Equipment requirements and tests	2008
EN 60664-1	Insulation coordination for equipment within low-voltage systems - Part 1: Principles, requirements and tests	2008
EN 60529	Degrees of protection provided by enclosures (IP Code)	2014 + A1:2017 + A2:2019