Product Release Brief

SE6 safety module – Expanded safety technology for SD6

Frei, Markus

23.11.2018

Safe Motion Monitoring STÖBER

STÖBER

Table of contents

1. Foreword

The 6th generation of STOBER drive controllers includes a wide range of device series featuring various safety functions.

This Product Release Brief describes the optional SE6 safety module for the SD6 drive controller series and its functions at market launch.

At the time of market launch, the SE6 safety module is not compatible with the SI6 and SC6 drive controller series. Due to the significant differences in the designs of the devices, Product Management and Development have not made any effort to change this by the SE6 market launch.

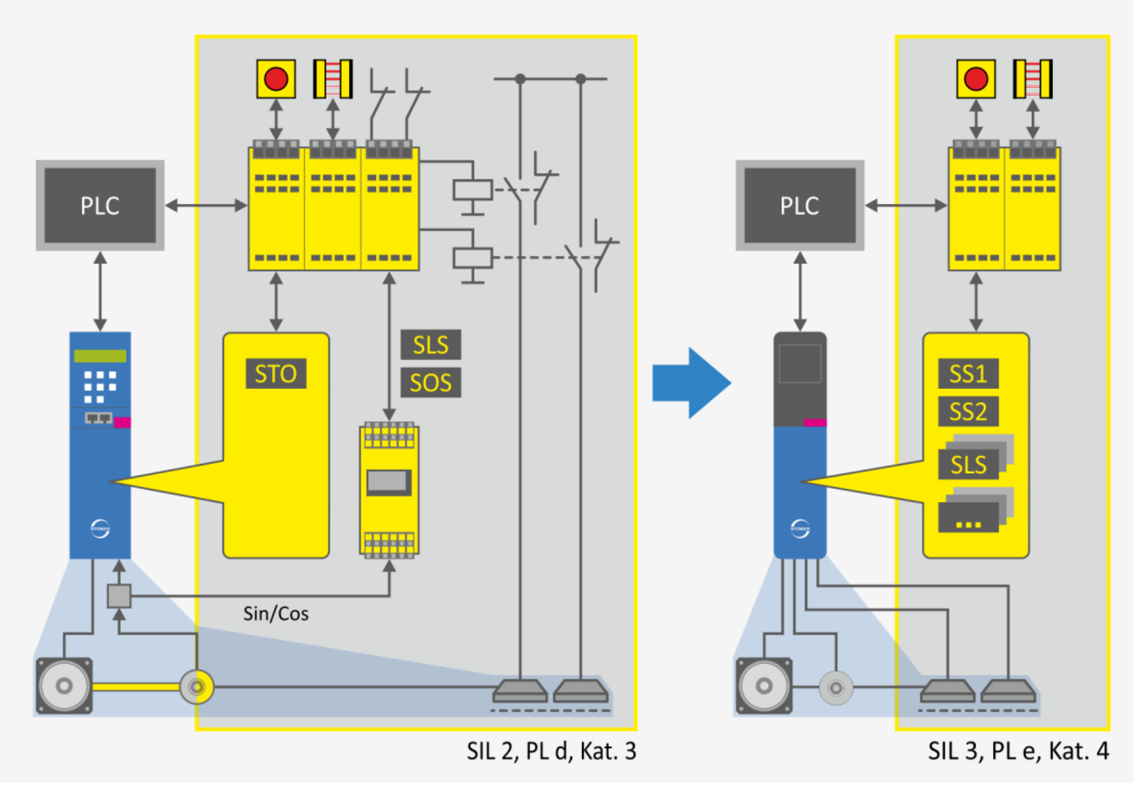

Figure 1: Basic concept of SE6

2. Document history

2.1. Authors

Department	Name (abbreviation)	E-mail contact
SPE	Markus Frei (mf)	markus.frei@stoeber.de

2.2. Changes

The information provided in this document has been researched, compiled and documented to the best of our knowledge and belief.

However, we cannot rule out the possibility that mistakes nonetheless found their way into this document. We are happy to receive feedback indicating helpful or necessary additions or pointing out mistakes. To do this, please send a simple e-mail to one of the authors named in Chapter 2.1.

2.3. Notes about document version V 0.x

Draft version, changes are not documented in the document

2.4. Notes about document version V 1.x and later

Changes and additions to content are documented in this chapter of the document. Orthographic improvements and corrections are not documented.

Date	Name	Note

3. Project overview

3.1. ePEP project

Version A of the SE6 safety module was developed over the course of the ePEP project "E1214 safety technology SD6 V2."

3.2. ePEP project team

In accordance with the principles of the ePEP process, the project team consists of the following roles and members:

ePEP project role	Project member	E-mail contact
Market Manager (MV)	Udo Cyrol (CY)	udo.cyrol@stoeber.de
Product Manager (PV)	Markus Frei (mf)	markus.frei@stoeber.de
Development Manager (EV)	Stephan Dilger (dlg)	stephan.dilger@stoeber.de
Project Manager (PM)	See PV	See PV

Table 1- Project team

The project members are happy to answer any questions about the product or project according to their role in the ePEP process.

3.3. Development goal

Expanded safety functions for the SD6 drive controller with a focus on synchronous servo motors.

Note:
Asynchronous motors were not considered explicitly during development. However, asynchronous motors can be monitored reliably using a second encoder.

3.4. Project history

Time frame	Action
4Q 2012	Project start
…	Market analysis and product definition
2Q 2015	Start of development
2Q 2017	Start of field testing phase
3Q 2017	TÜV advance certificate
1Q 2018	End of development
2Q 2018	SE6 development, warehouse stock (200 units)
2Q 2018	Official certificate; SE6 is offered and sold based on customer demand
2018-11-01	Official market release at SAT
SPS IPC Drives 2018	Official product presentation

Table 2: -Project history

3.5. Application area

The SE6 safety module is available as an optional accessory for the SD6 drive controller from size 0 (SD6A0x) to size 3 (SD6A3x). Its operational environment corresponds to that of the SD6 base device.

The safety module replaces the ST6 safety module integrated into the standard version of the SD6 drive controller with the STO (Safe Torque Off) safety function.

Note:
The SE6 safety module cannot be used with the other STOBER drive controller series (SI6, SC6, etc.).

3.6. Assembly

The safety module is installed in the drive controller during the final production phase of the device at STOBER and checked for proper functioning during the quality control test. In addition to testing for correct integration, the SE6 serial number is also linked with that of the SD6 base device here, for example, for complete traceability of its location.

For organizational reasons, later installation of the SE6 safety module in the field is not possible, neither by a customer nor by a STOBER employee.

3.7. Firmware update

A firmware update of the SE6 safety module in the field is not possible. A firmware update solution is being developed at STOBER and/or PILZ as part of project maintenance. A target date cannot yet be given at this time.

A firmware or application update for the SD6 base device is always possible, regardless of the safety module.

3.8. Configuration/parameterization

The SE6 safety module is configured/parameterized using STOBER DriveControlSuite (DS6). A plugin from PILZ called PASmotion was added to the DS6 for this purpose.

To communicate with the SE6 safety module in the drive controller, PASmotion uses the communication interface of the DS6, which establishes this connection with the drive controller.

The (safety) configuration in PASmotion and in the drive controller is protected by checksums and a password. The safety configuration is stored in the drive controller on both the SE6 and the µSD card. This makes it easy to handle the drive controller in the event of service. A device replacement can be reliably detected.

In PASmotion, a report for the safety configuration can be created in the form of a PDF file containing the configuration and parameterization of the SE6.

Note:
A lost or forgotten password cannot be restored, even by STOBER.

3.9. Documentation

A separate manual is available for the SE6, as is typically used at STOBER. At market launch, the manual will be available in German and English.

It will be translated into other languages as needed.

3.10. Validation and verification

Prior to delivery and following any modifications, our customers must verify and document that the machine's safety functions are working properly. This also includes validating and verifying the safety functions in which the SE6 is involved.

The SE6 safety functions can be checked using the scope function of the DS6.
The customer can include any scope images that are made in the corresponding documents (safety check, safety acceptance report, etc.).

> Note:
> Experience has shown that the documents for validating the safety functions have widely differing designations among our customers.

3.11. Type testing

By definition, components from the area of safety technology are subject to the Machinery Directive. This includes our drive controllers with integrated safety technology.

That is why we require device type testing to be able to bring our drive controllers to market in accordance with regulations. This was issued by TÜV-Süd for the SD6 in combination with the new SE6 safety module at the start of 2018, and can be downloaded from our website's download area as needed.

3.12. Start of sales

The safety module is officially available at STOBER as of November 1, 2018. At this time, the SE6 is unlocked in the SAP system for a gross sales price of €595 and is immediately available from the warehouse.

The SE6 will be officially introduced at SPS IPC Drives 2018 in Nuremberg as one of the STOBER trade fair highlights.

4. Safety functions

Following the market analysis, it was decided at the start of the project that not all safety functions described in DIN EN 61800-5-2 "Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional safety" would be implemented. The effort and expense would not have been proportionate to the estimated benefits.

When implementing the safety functions and their interfaces, attention was given not only to fulfilling the requirements of 61800-5-2 (Safety Integrity Level (SIL)), but also to implementing them such that our customers can also use these in accordance with the requirements of DIN EN ISO 13849-1 "Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design" (Performance Level (PL)).

When applied correctly, all safety functions available on the SE6 can achieve the highest safety level defined in mechanical engineering: SIL 3/PL e/Category 4.

Note:
Only the safety functions implemented in the E1214 project are mentioned in this chapter.

Thanks to the safety functions implemented in the SE6, it is also possible to fulfill the requirements of other standards not explicitly mentioned here, such as EN 13850 "Safety of machinery - Emergency stop function – Principles for design".

4.1. Normative safety functions based on DIN EN 60204-1

DIN EN 60204-1 "Safety of machinery – Electrical equipment of machines – Part 1: General requirements" is one of the most foundational standards in mechanical engineering. In addition to the requirements for basic electrical safety, it also describes stop categories for shutting down movements.

Note:
Many of our customers use these terms because they are not familiar with the EN 61800-5-2 standard relevant to drive controllers. This sometimes leads to misunderstandings regarding the term "category".

Safety function	Description
Stop category 0	Corresponds to the STO safety function of DIN EN 61800-5-2
Stop category 1	Corresponds to the SS1 safety function of DIN EN 61800-5-2
Stop category 2	Corresponds to the SS2 safety function of DIN EN 61800-5-2

Table 3: Normative safety functions based on DIN EN 60204-1

4.2. Normative safety functions based on DIN EN 61800-5-2

DIN EN 61800-5-2 "Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional safety" is the basic standard for the safety of drive controllers and frequency inverters. In addition to the safe stop functions, this standard also describes other safety functions for limiting and monitoring movements, as well as added functions such as Safe Brake Control.

4.2.1. Safe stop functions

Safety functions for safely shutting down movements

Safety function	Description	Response to detection of a limit value violation
STO	Safe Torque Off	-
SS1	Safe Stop 1 Controlled or monitored transition into STO	STO
SS2	Safe Stop 2 Controlled or monitored transition into SOS	SS1

Table 4: Safe stop functions based on EN 61800-5-2

4.2.2. Safe movement functions

Safety functions for monitoring movements. If a limit value is violated, one of the STO or SS1 stop functions is introduced to stop the movement.

Note:
If a limit value violation is detected due to a movement function, the SS1 safety function is always activated. If necessary, this can be configured so that an STO is triggered immediately. However, it usually does not make sense to do this.

Safety function	Description	Response to detection of a limit value violation
SLS	Safely-Limited Speed	SS1
SSR	Safe Speed Range	SS1
SDI	Safe Direction	SS1
SOS	Safe Operating Stop	SS1
SLI	Safely-Limited Increment	SS1
SLP	Safely-Limited Position	SS1

Table 5: Safe movement functions based on EN 61800-5-2

4.2.3. Safe brake functions

Safety functions for safely controlling one or more brakes.

Safety function	Description	Response to detection of a limit value violation
SBC	Safe Brake Control	SS1

Table 6: Safe brake functions based on EN 61800-5-2

4.3. Normative safety functions based on DIN EN 14118

DIN EN ISO 14118 "Safety of machinery – Prevention of unexpected start-up" describes the requirements for preventing machines from starting unexpectedly.

> Note:
> This essentially concerns ensuring that, after the drive controller has been switched into the STO safe state, it will not leave this state until acknowledgment has occurred.

Safety function	Description	Response to detection of a limit value violation
SRL	Safe Restart Lock	STO

Table 7: Safety functions based on EN 14118

4.4. Safety functions not described in standards

To increase the practical suitability of the SE6, some of the safety functions described in EN 61800-5-2 have been implemented without a direct fault response. To make it easy to identify them, the abbreviation "M" for "Monitoring" has been added to the basic safety functions.

In the case of SBT, the safety function described in 61800-5-2 was expanded to close the normative gap with 13849-1 in the area of "safe brake management" in accordance with the recommendations of German Social Accident Insurance (Deutsche Gesetzliche Unfallversicherung (DGUV)).

Safety function	Description	Response to detection of a limit value violation
SLS-M	Safely-Limited Speed – Monitoring	Status report
SSR-M	Safe Speed Range – Monitoring	Status report
SDI-M	Safe Direction – Monitoring	Status report
SOS-M	Safe Operating Stop – Monitoring	Status report
SLI-M	Safely-Limited Increment – Monitoring	Status report
SLP-M	Safely-Limited Position – Monitoring	Status report
SBT	Safe Brake Test	SS1

Table 8: Safety functions not described in standards

5. Principal function

The SE6 safety module uses a calculated virtual encoder to check motor encoder plausibility and monitors the movement of the drive.

Limitations are not made in the drive controller. The SE6 intervenes in the functional part of the SD6 drive controller only for the SS1 and SS2 stop functions in the optional "Drive-controlled" mode.

5.1. Available safety functions

The individual safety functions can be subdivided into the following groups.

5.1.1. Safe stopping

- Safe Stop 1 (SS1)
- Safe Stop 2 (SS2)

5.1.2. Safe limiting

The speed and position are limited by a forced stop when a limit value is violated. The SS1 safety function is activated for this purpose.

- Safely-Limited Speed (SLS)
- Safe Speed Range (SSR)
- Safe Direction (SDI)
- Safe Operating Stop (SOS)
- Safely-Limited Increment (SLI)
- Safely-Limited Position (SLP)

5.1.3. Safe reporting

All safety functions available for limiting the speed and position are also offered as a variant that only safely reports a limit value violation instead of forcing a stop.

5.1.4. Safe brake management

Safe brake management (SBM) consists of two safety functions:

- Safe Brake Control (SBC)
- Safe Brake Test (SBT)

5.2. Response to a limit value violation

When a limit value violation is detected, the SE6 offers various response options:

- Safe reporting (-M functions)
- Safe stop (SS1)
  - Drive-based stopping
  - Controller-based stopping

5.3. Brief explanation of safety functions

The most important available safety functions are briefly explained in the following sections. If necessary, details of the functions can be found in the SE6 manual.

5.3.1. Safe Stop 1 (SS1)

After the safety function is activated by the SS1_ACT (SS1_Activate) control signal, the safety function controls and/or monitors the stopping of the drive. Various options are available for this purpose. After the configured time t_max has expired, the power unit in the drive controller is switched off (STO).

Drive-based stopping:
The SE6 triggers a stop command with the defined brake ramp. The brake ramp and/or stop can be monitored in addition to the time t_max and can activate the shutoff of the power unit (STO) before the time t_max expires.

Control-driven stopping: The higher-level controller brakes the drive to a stop. The brake ramp and/or stop can be monitored in addition to the time t_max and can activate the shutoff of the power unit (STO) before the time t_max expires.

Note:
If a limit value violation is detected during a control-driven SS1 and active brake ramp monitoring, such as due to a fault in the functional controller, the SE6 offers another fallback level. In this case, a "fallback" can be activated so that the SE6 triggers a drive-based stop.

If the configured brake ramp is not maintained during active brake ramp monitoring or a prohibited movement is detected after stop monitoring is activated, this is identified as a limit value violation.

The status of the safety function is provided to the user through the outputs SS1_ACK (Safe Stop 1_Acknowledge) and STO_ACK (Safe Torque off_Acknowledge).

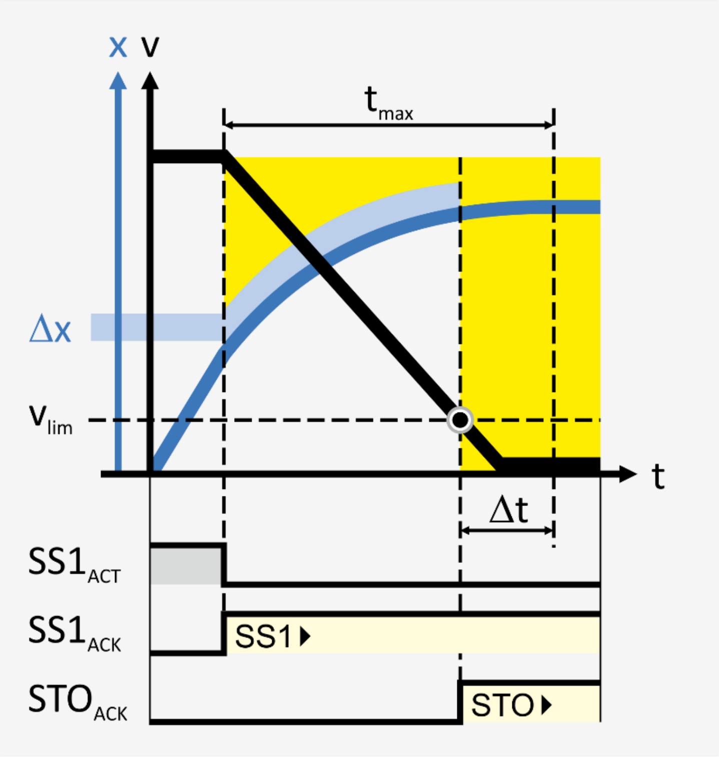

Figure 2: Safe Stop 1 (SS1)

5.3.2. Safe Stop 2 (SS2)

After the safety function is activated by the SS2_ACT (SS2_Activate) control signal, the safety function controls and/or monitors the stopping of the drive. Various options are available for this purpose. After the configured time t_max expires, the drive is still energized and is monitored for a stop (SOS).

Drive-based stopping:
The SE6 triggers a stop command with the defined brake ramp. The brake ramp and/or stop can be monitored in addition to the time t_max and can activate stop monitoring (SOS) before the time t_max expires.

Control-driven stopping:
The higher-level controller brakes the drive to a stop. The brake ramp and/or stop can be monitored in addition to the time t_max and can activate stop monitoring (SOS) before the time t_max expires.

If the configured brake ramp is not maintained during active brake ramp monitoring or a prohibited movement is detected after stop monitoring is activated, this is identified as a limit value violation.

The status of the safety function is provided to the user through the outputs SS2_ACK (Safe Stop 2_Acknowledge) and SSA_ACK (Safe Standstill_Acknowledge).

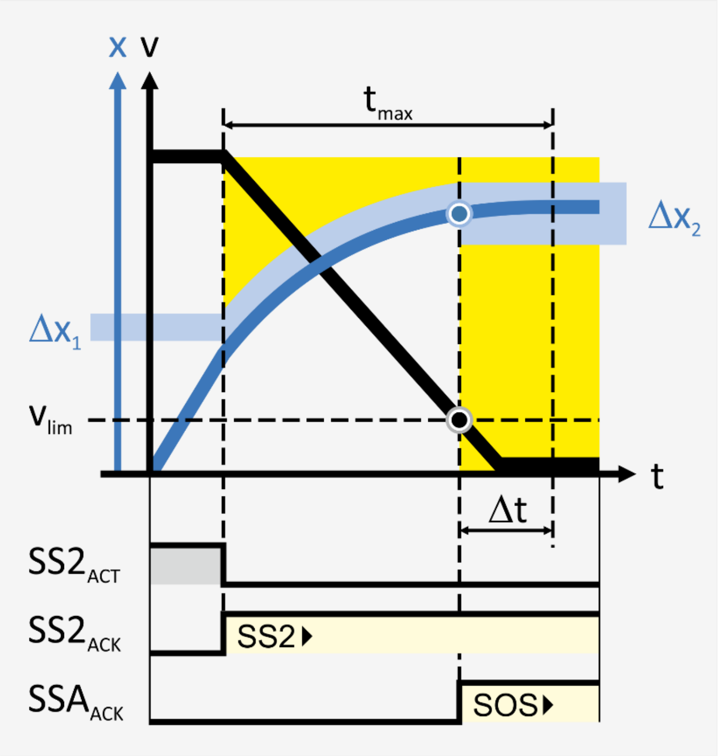

Figure 3: Safe Stop 2 (SS2)

5.3.3. Safely-Limited Speed (SLS)

After the safety function is activated by the SLS_ACT (SLS_Activate) control signal and the delay time t_delay has expired, the safety function monitors to make sure the configured speed is not exceeded. If the amount of the speed limit value is exceeded or undershot, a limit value violation is identified.

The output SRA_ACK (Safe Range_Acknowledge) provides the status of the safety function to the user.

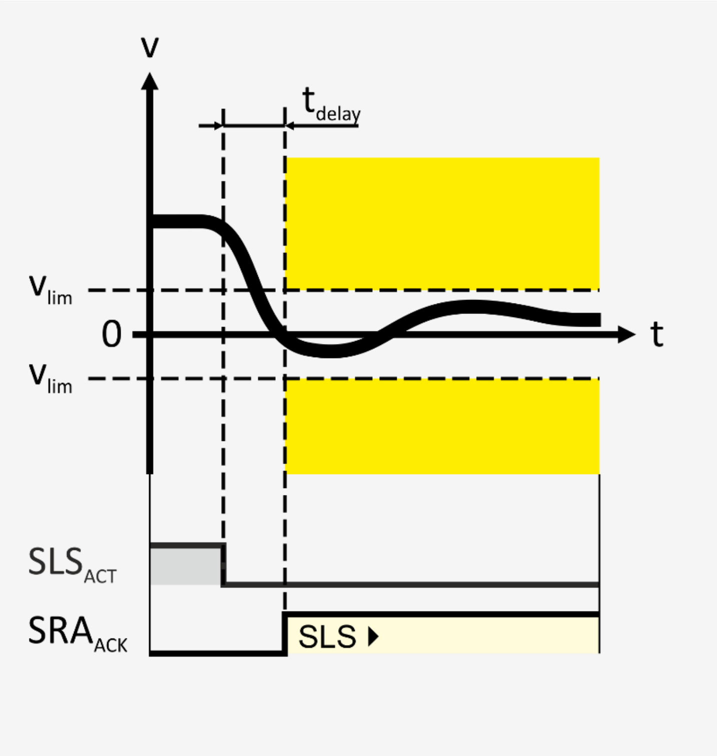

Figure 4: Safely-Limited Speed (SLS)

5.3.4. Safe Speed Range (SSR)

After the safety function is activated by the SSR_ACT (SSR_Activate) control signal and the delay time t_delay has expired, the safety function monitors to make sure the configured speeds are not exceeded. If one of the two projected speed limits is exceeded or undershot, a limit value violation is identified.

The output SRA_ACK (Safe Range_Acknowledge) provides the status of the safety function to the user.

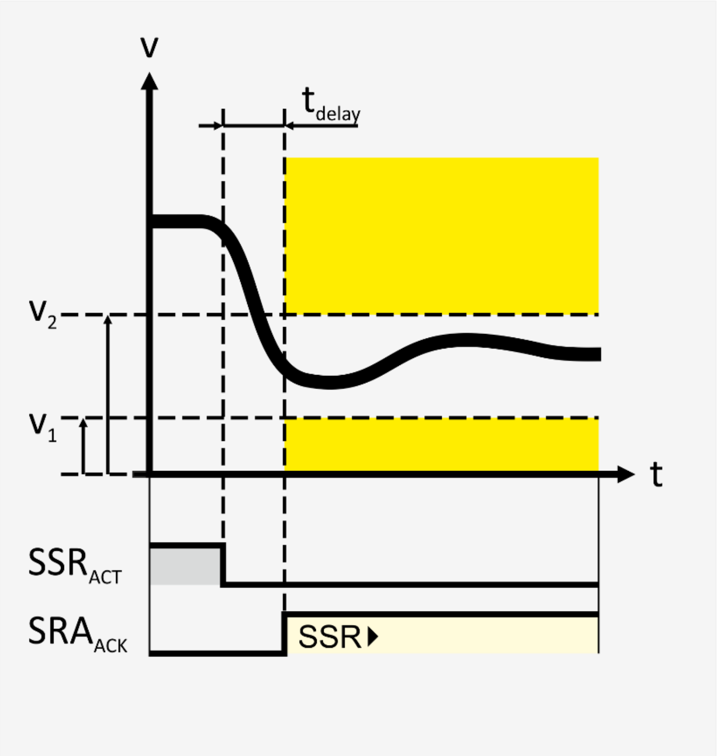

Figure 5: Safe Speed Range (SSR)

5.3.5. Safe Direction (SDI)

After the safety function is activated by the SDI_ACT (SDI_Activate) control signal and the delay time t_delay has expired, the safety function monitors to make sure the configured direction of motion is maintained.

For this purpose, when monitoring begins, a monitoring position is formed from the actual position of the motor shaft and the configured tolerance range. If the axis moves in the permitted direction, the monitoring position is updated.

If the axis moves in the prohibited direction of rotation and reaches the monitoring position, a limit value violation is identified.

The output SDA_ACK (Safe Direction_Acknowledge) provides the status of the safety function to the user.

Note:
With the help of position-based monitoring, the SDI safety function is very sensitive to speed fluctuations due to encoder noise.

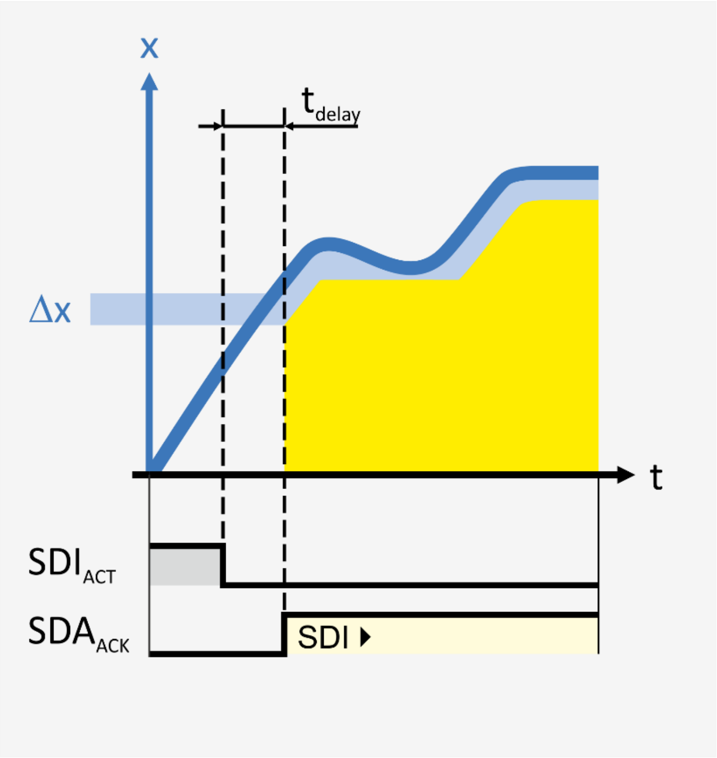

Figure 6: Safe Direction (SDI)

5.3.6. Safe Operating Stop (SOS)

After the safety function is activated by the SOS_ACT (SOS_Activate) control signal and the delay time t_max has expired, the safety function monitors to make sure the drive does not move. The delay time until monitoring is activated can be reduced using optional standstill detection.

When monitoring begins, a position window is formed around the actual position of the motor shaft with the configured tolerance range. If the axis exceeds one of the position limits, a limit value violation is identified.

The output SSA_ACK (Safe Standstill_Acknowledge) provides the status of the safety function to the user.

> Note:
> With the help of position-based monitoring, the SOS safety function is very sensitive to speed fluctuations due to encoder noise.

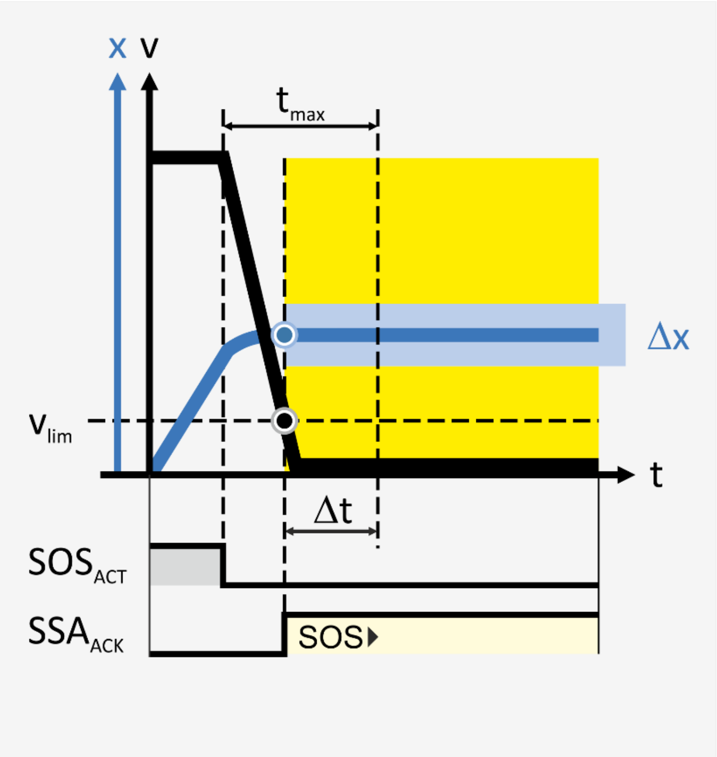

Figure 7: Safe Operating Stop (SOS)

5.3.7. Safely-Limited Increment (SLI)

After the safety function is activated by the SLI_ACT (SLI_Activate) control signal and the delay time t_delay has expired, the safety function monitors to make sure the drive moves only within the permitted range.

When monitoring begins, a position window is formed around the actual position of the motor shaft with the configured limits. If the axis exceeds one of the position limits, a limit value violation is identified.

The output SRA_ACK (Safe Range_Acknowledge) provides the status of the safety function to the user.

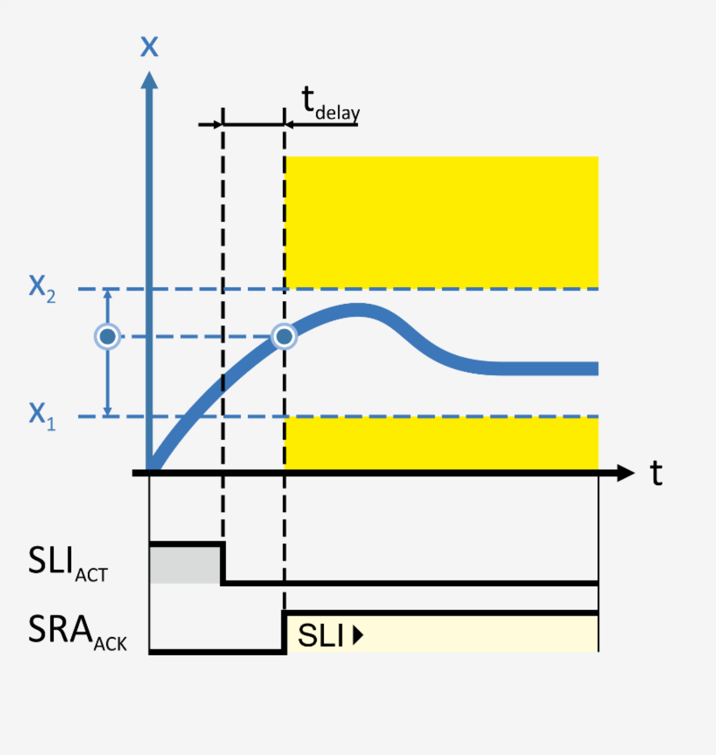

Figure 8: Safely-Limited Increment (SLI)

5.3.8. Safely-Limited Position (SLP)

After the safety function is activated by the SLP_ACT (SLP_Activate) control signal and the delay time t_delay has expired, the safety function monitors to make sure the drive moves only within the configured position range. If the axis exceeds one of the position limits, a limit value violation is identified.

The output SRA_ACK (Safe Range_Acknowledge) provides the status of the safety function to the user.

Note:
The SLP safety function requires a second multi-turn encoder to check motor encoder plausibility. The two encoders have to be synchronized and referenced to each other during commissioning.

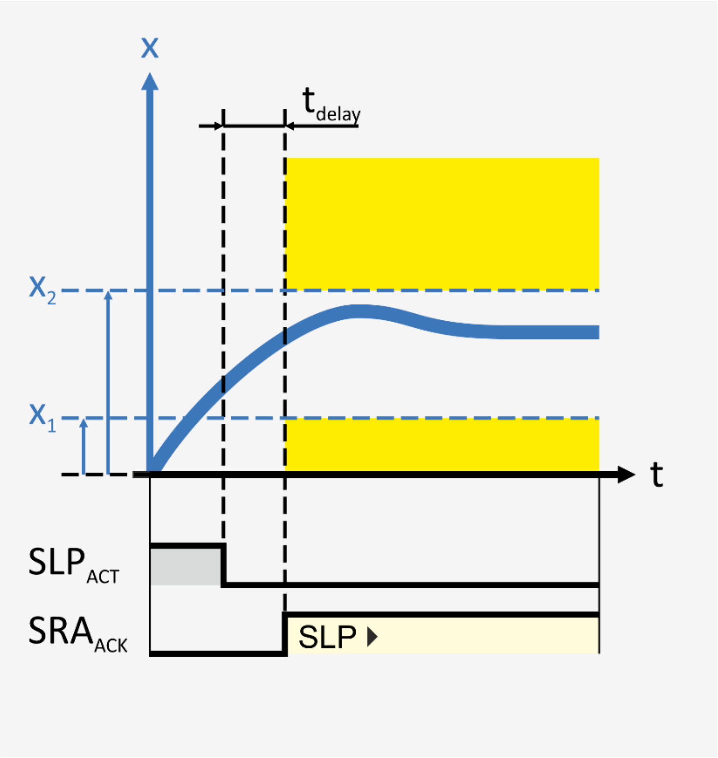

Figure 9: Safely-Limited Position (SLP)

5.3.9. Safe brake management

Safe brake management consists of two components:

- Safe controlling (Safe brake control; SBC)
- Safe monitoring (Safe brake test; SBT)

Safe brake control is ensured by the SE6 hardware and tests during operation that the user cannot see.

After the safety function is activated by the SBT_ACT (SBT_Activate) control signal and the delay time t_delay has expired, the safety function monitors the process defined earlier for the brake test. During the process of the individual test steps, the drive is monitored for a stop. After the device is started and after the time of the defined test cycle has expired, the SBC function reports that a brake test is necessary and starts a tolerance time during which a brake test absolutely must take place. The customer must take this into account in the machine concept.

The outputs SBA_ACK (Safe Brake_Acknowledge) and SSA (Safe Standstill_Acknowledge) provide the status of the safety function to the user.

Note:
The brake test is neither possible nor useful in every position of an axis. Before the brake test, the user has to move the axis to a defined position.

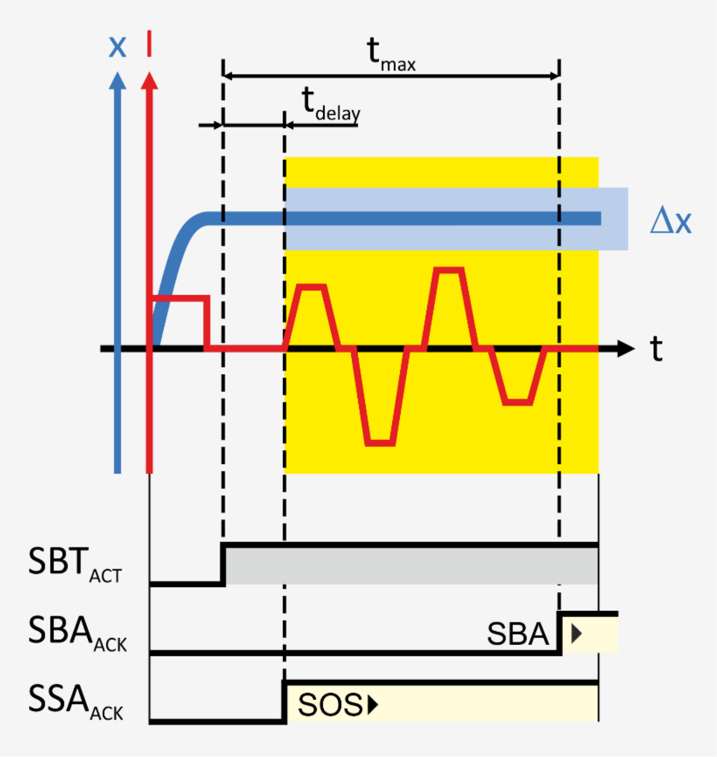

Figure 10: Safe Brake Test (SBT)

6. Special features

The SD6 drive controller with the SE6 safety module provides a few special features for the customer that are not found everywhere on the market.

Customers who need these functions only have a limited selection of alternatives on the market.

Note:
The ePEP project team is very interested in hearing about competitors who offer comparable functions and hopes to get feedback about them from the field.

6.1. Encoder-independent

A special fail-safe encoder is not required to operate the SE6. There are also no special requirements for attaching the encoder. This means that the SD6 also has no trouble safely monitoring motors with a hollow shaft, linear motors, motors with resolvers or inductive encoders.

Note:
At STOBER, the safe encoder attachment to the motor is referred to as FMA (fault exclusion for the mechanical coupling).

The Institute for Occupational Safety ("Institut für Arbeitssicherheit" (IFA)) of the German Social Accident Insurance (DGUV) published "Do safe drive controls also require safe position encoders?" on this topic recently in 2017. Nearly all well-known drive controller manufacturers on the market adhere to the (normative) requirements summarized there.

The solution jointly developed by STOBER and PILZ is only indirectly described in this document. The solution is based on motor encoder plausibility being checked by the drive controller. For this purpose, the SE6 uses the data from the power unit to calculate a "virtual encoder." This also makes it possible to solve the basic problem of the encoder detaching from the motor shaft, which is one of the basic problems in the IFA publication.

An additional (SSI) multi-turn encoder on the SE6 X50 interface is required only for the SLP (Safely-Limited Position) safety function for checking the plausibility of the multi-turn stage of the motor encoder.

6.2. Operation of synchronous servo motors

The SE6 safety module has been developed primarily for monitoring synchronous servo motors. In the case of synchronous servo motors, the motor encoder is calculated during operation using a virtual encoder that was calculated based on the power unit. This replaces a second encoder.

With the help of an external encoder on the X50 interface, it is also possible to monitor asynchronous motors.

6.3. Operation of asynchronous motors

If the speed or position of an asynchronous motor needs to be monitored, a second encoder is required on the X50 interface (TTL or SSI). A virtual encoder cannot be calculated for asynchronous motors.

There are no special requirements for the X50 encoder or how it is attached.

For diversity, it is only necessary that the X50 encoder is independent of the motor encoder. It must be ensured that the two encoders are installed independently of each other to satisfy the requirements for common cause failures.

6.4. Securing gravity-loaded axes

At the time of market launch of the SE6, there is no known harmonized standard in the EU that handles the topic of "gravity-loaded axes."

The draft of DIN EN 16090-1:2016-02 "Machine tools safety – Machining centres, milling machines, transfer machines – Part 1: Safety requirements" is still in progress and has not been harmonized.

The part of the 16090-1 draft in which securing gravity-loaded axes is addressed is based on the recommendations of the DGUV Woodworking and Metalworking Division from Division Information Sheet No. 005 Edition 09/2012.

This document was one of the specifications for safe brake management in the SE6 development project.

Division Information Sheet No. 005 Edition 09/2012 of the DGUV entitled "Gravity-loaded axes" can be obtained by our customers and interested parties at no cost through STOBER "Sales & Product Management Electronics" (SPE). As an alternative, it can be downloaded from the DGUV/IFA server.

Thanks to the SE6, our customers can meet the recommendations compiled in the Division Information Sheet. The SE6 satisfies the recommendations regarding the described solutions based on one brake as well as two.

Note:
The topic of securing gravity-loaded axes is frequently described with varying degrees of technical knowledge by articles in trade journals. STOBER also released a publication about this for the SE6, which was distributed to various agencies in Autumn 2018.

6.4.1. Market situation

The SBC safety function can be found at many competitors with various safety classifications and is also actively advertised.

In general, however, these systems only satisfy the requirements of EN 61800-5-2 for drive controllers. In other words, they provide a safe output for controlling a brake. The expanded requirements of the DGUV for testing and test monitoring are not met.

A well-known exception is PILZ, which offers a solution for the Servostar 700 directly (Servostar base device labeled as Protego) and indirectly through Kollmorgen. However, this comes with a few problems in practice. For example, the Servostar cannot manage two brakes and requires costly accessories to do so.

Bosch has been advertising a solution comparable to STOBER's since mid-2018, following years of using a functional brake test without reliable safety figures. We rank this solution as direct competition.

Mayr brakes from Kaufbeuren, Germany, is advertising a drive-independent solution jointly developed with PILZ that has been implemented on a special safety relay. This must be considered skeptically because this solution also does not provide a brake test.

6.5. Manufacturer-neutral interface

The SE6 safety module provides 8 safe inputs. These can be controlled using contacts or safe (monitored) semiconductor outputs (referred to as OSSD signals). In addition to inputs, the safety module provides 5 safe (semiconductor) outputs for status messages. The inputs and outputs can be assigned flexibly to the configured safety functions.

This means that the SE6 can be connected to well-known safety controllers on the market, regardless of the manufacturer.

An interesting feature of the SE6 is that the basic SS1 safety function provides an additional input for directly selecting STO. All other safety functions require only a connecting cable for activation.

This enabled overall wiring requirements to be reduced.

Note: The ePEP project team is looking for parties potentially interested in an FSoE and/or PROFIsafe connection. We welcome feedback on this from the market.

6.6. Prevention of false triggering

The motor speed is determined based on the position measurement of the motor encoder.
Due to the resolution, measuring tolerances and unfavorable scanning timing lead to errors in calculating the motor speed.

For example, if an absolute encoder with 12-bit resolution scans every 250 µS, the speed resolution is about +/- 60 rpm if one bit too many or too few has been measured. Depending on mechanical effects such as chains, additional interference pulses can affect the measured speed.

To prevent false triggering during motor monitoring, the SE6 provides the option of specifically suppressing interference pulses. This way, it is possible to approach limit values specified in standards with a small safety distance.

6.7. Multi-instance capability

The SE6 is also able to monitor up to 10 safety functions simultaneously for the basic SS1 safety function. The user can put together these safety functions however they choose.

For example, the user can safely monitor up to 10 speeds (SLS) or 10 movement ranges (SLI).

Note: To date, we have not seen any competitor with the multi-instance capability for safety functions in the form we are offering.

6.8. Response to limit value violations

The SE6 provides various options for responding to detected limit value violations.

6.8.1. Safe reporting

The SE6 provides one monitoring variant for each of the safety functions for motion monitoring. If an activated monitoring function detects a limit value violation, this is only reported to the higher-level safety controller without a direct response in the drive controller.

Depending on the application, the higher-level safety controller can decide whether and how to respond to the status report from the drive controller.

Note:
The monitoring functions are indicated in the project configuration tool by the addition "-M", for example, SLS-M.

6.8.2. Safe shutdown

If one of the safe movement functions (such as SLS) detects a limit value violation, the Safe Stop 1 (SS1) safety function in the drive controller becomes active. In this case, the drive has to be shut down. Two different variants are available for this to match the application.

6.8.2.1. Drive-based stopping

When the SS1 safety function is activated, a stop command is activated on the drive controller with the configured brake ramp. The time between the detected limit value violation and the start of the brake ramp in this case is only a few milliseconds. The SE6 provides various options to monitor for correct function and to shut off the power unit as quickly as possible.

- Brake ramp monitoring
- Standstill detection
- Maximum time

The power unit of the drive controller is safely shut off at the latest after the maximum time expires.

6.8.2.2. Controller-based stopping

When the SS1 safety function is activated, a stop command is triggered on the drive controller. This function is left to the higher-level controller, which thereby retains control over the drive controller. This is particularly advantageous in the case of compound drives with central motion control, as it enables coordinated braking of the machine. The SE6 provides various options to monitor for correct function and to shut off the power unit as quickly as possible.

- Brake ramp monitoring
- Standstill detection
- Maximum time

If the SE6 detects that the brake ramp does not correspond to the projected specifications, it can activate a stop command as a "fallback", such as for drive-based SS1.

The power unit of the drive controller is safely shut off at the latest after the maximum time expires.

6.9. Safety level

The SE6 fulfils the SIL 3/ PL e (Cat. 4) requirements for all safety functions.

The SIL classification is based on our product standard for drive controllers, DIN EN 61800-5-2. SIL 3 is the highest possible classification in this standard.

The PL classification is derived from DIN EN ISO 13849-1, which is to be used for 99.9 % of our customers. PL e is the highest safety level described in it.

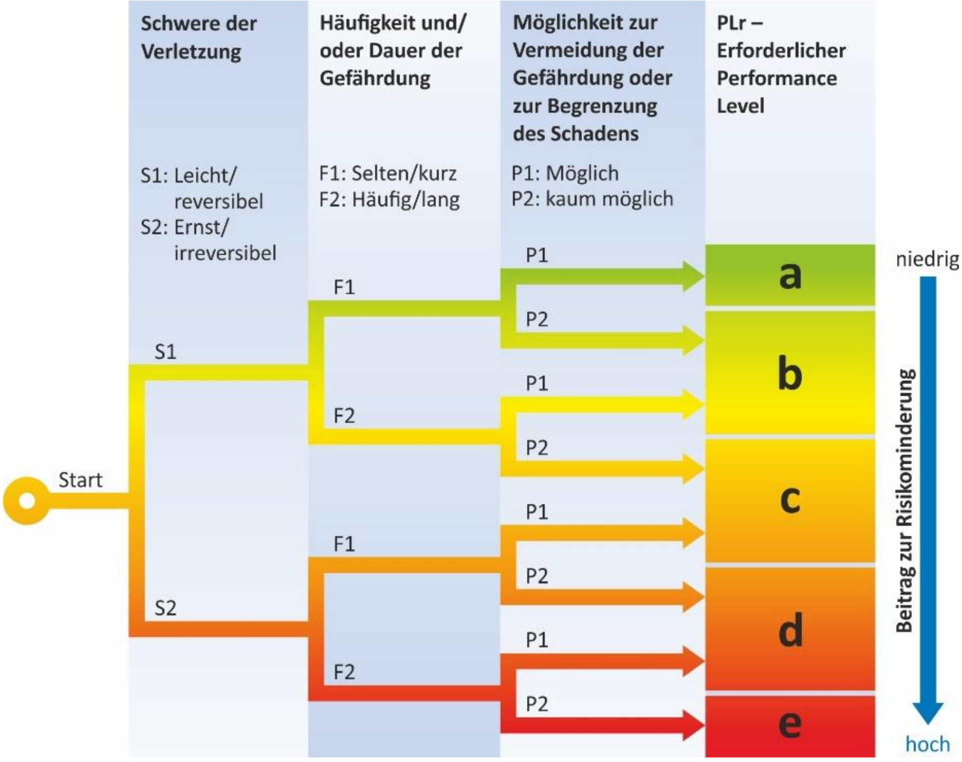
Schwere der Verletzung
Häufigkeit und/ oder Dauer der Gefährdung
Möglichkeit zur Vermeidung der Gefährdung oder zur Begrenzung des Schadens
PLr – Erforderlicher Performance Level
S1: Leicht/ reversibel
S2: Ernst/ irreversibel
F1: Selten/kurz
F2: Häufig/lang
P1: Möglich
P2: kaum möglich
Start
S1
S2
F1
F2
F1
F2
P1
P2
P1
P2
P1
P2
P1
P2
a
b
c
d
e
niedrig
Beitrag zur Risikominderung
hoch

Figure 11: Risk graph of DIN EN ISO 13849-1

6.10. Worst case response time

The time from when a safety function on a machine is triggered until the drives are shut off can be divided into several phases.

The phases of triggering a sensor (for example, an emergency stop button) and its detection and processing of the information in the safety controller are independent from the SE6.

Depending on the output type of the safety controller and its implementation, the inputs from the SE6 may have to be delayed so that test pulses do not cause any false triggering. To do this, the inputs of the SE6 can be configured with filter times up to 10 ms (typically 1 ms).

After this delay time, which is independent of the SE6, has expired, the SE6 detects the activation of a safety function after one program cycle at the latest. An additional cycle is needed to detect a limit value violation. Another cycle is needed for activating the response to the limit value violation (usually SS1).

The time for stopping the drive again depends on the application. This depends on the drive mechanism, its load and the possible brake ramps. In practice, typical values for this range from 100 ms to several seconds.

The SE6 needs a maximum of 3 cycles for the application-independent part of detecting activation of the safety function until the fault response is introduced. The SE6 cycle time is 3 ms, which leads to our advertised worst case response time of 10 ms.

Note:
A wide range of times are advertised on the market. For example, Beckhoff advertises 31.25 µs. These are usually best-case times.
The FSoE watchdog monitoring time in the Beckhoff system, for example, is 100 ms in the default configuration. Values under 50 ms can lead to problems in the system in the event of telegram failures.

6.11. Service concept

The STOBER service concept is extremely simple. for both the motor and the drive controller.

6.11.1. Motor

Since the SE6 safety concept does not have any special requirements for the motor, encoder or encoder attachment, if necessary, it can simply be replaced 1:1 in a de-energized state with a motor of the same type. The motor can also be repaired on site easily.

Limitations based on the industry's standard "fault exclusion for encoder attachment" do not apply.

- Releasing the encoder mounted in a "failsafe" manner.
  If the encoder retaining bolt breaks when attempting to release it, the motor shaft has to be drilled open and reworked.
- Required idle time for the adhesive bond to cure.
  In accordance with the intended use of Heidenhain, the adhesive bond to be used has a curing time of 6 to 12 hours. In practice, this means "overnight".
- Checking the encoder mounting.
- Documentation for verification management.

Note:
In general, motors on which the encoder has to be mounted in a "failsafe" manner must go back to the manufacturer in case of service.

6.11.2. Drive controller

The safety project configuration is stored on both the SE6 and the SD card. If the drive controller is replaced due to a defect and the SD card of the "old" device is inserted into the "new" device, the new controller detects this exchange. Deliberate action is needed for the safety application to be applied to the "new" drive controller. This can be done right on the operating unit of the drive controller.

After the device is started, a message appears on the display that must be acknowledged by pressing a button for 2 s within a certain time window.
After the button is pressed for 2 s, the drive controller shows the checksum of the safety configuration, which must be checked by the operator. This rules out the possibility of the drive controller getting mixed up when replaced.

The "new" drive controller is then ready for operation and machine functionality can be tested.

Note:
The service concept is rarely emphasized by our competitors, since replacing a motor or drive controller is not possible without help from the manufacturer or a highly qualified colleague.

7. Market comparison

Solutions available on the market for expanded drive-based safety technology vary widely. The concepts that are offered also sometimes depend on the test institute.

The market can essentially be divided into the following groups:

1. Drive solutions based on failsafe encoders
2. Drive solutions based on conventional sin/cos encoders
3. Systems independent of the drive controller

7.1. Drive solutions based on "failsafe encoders"

Heidenhain and Sick-Stegmann offer encoders for installation in servo motors with safety certification.

Heidenhain offers fully digital, failsafe EnDat 2.2-FS encoders. They are available in optical and inductive variants. A special stack is needed to evaluate the encoders. A manageable number of drive controllers is needed to satisfy the requirements for encoder evaluation. The best known competitor is B&R.

Sick-Stegmann not only offers classic sin/cos-based encoders (Hiperface safety), but also fully digital failsafe encoders (Hiperface DSL safety). For example, customers include SEW or KEB, which uses the sin/cos-based variants.

What all these solutions have in common is that they are based on fault exclusion for the mechanical attachment of the encoder to the motor. Since these encoders based on the FMA attachment only feature SIL 2 certification, this usually also limits the overall system to SIL 2.

Note:
There was an interesting addition to the 2017 edition of the IFA position paper on safe drive controllers and encoders. It explained that the FMA attachment does not necessarily result in the safety level being reduced to SIL 2. This is why various standards were applied during the evaluation, depending on the certifying institute and the certification date.

7.2. Drive solutions based on conventional sin/cos encoders

The majority of our competitors relies on conventional sin/cos encoders, which are monitored by the drive controller. Argumentation based on fault exclusion is used at critical points, which generally leads to an SIL 2 rating.

The systems can be recognized by the use of the optical EnDat 2.1 sin/cos encoders offered by Heidenhain.

7.3. Systems independent of the drive controller

Systems independent of the drive controller are usually based on the sin/cos tracks of the motor encoder. The requirements for these systems are described in the manuals. The systems are usually flexible and offer various options for checking encoder plausibility. Nearly all notable and well-known safety relay manufacturers have corresponding modules in their product line. Examples include PILZ, Siemens, BBH, DINA, Phoenix Contact, Dold, Schmersal and Motrona.

Solutions with an encoder require fault exclusion for the encoder attachment. This is not required when the plausibility of the motor encoder is checked by a second encoder.

Note:
When the drive is monitored using a conventional sin/cos encoder, there are usually requirements for how the encoder is attached. As a result, inductive encoders are usually ruled out.

7.4. SE6 product advantages compared to drives with failsafe encoders

Seq. No.:	Keyword	Note
1	Free motor selection	Suitable sin/cos encoders are not available for all motors
2	No FMA encoder attachment	Price advantage and service advantages
3	Free encoder selection	No limitations for performance, robustness or cost-effectiveness
4	-	-
5	-	-
6	-	-
7	Service concept	Exchange the SD card and that's it!
8	Cost-effectiveness	Project configuration using DS6, economically attractive complete solution
9	Safe brake management	Almost no competition on the market
10	Safety level	SIL 3/PL e/ Cat. 4 for all safety functions
11	Retrofitting	Replace the drive controller and that's it!

Table 9: Product advantages compared to systems with failsafe encoders

7.5. SE6 product advantages compared to classic sin/cos solutions

Seq. No.:	Keyword	Note
1	Free motor selection	Suitable sin/cos encoders are not available for all motors
2	No FMA encoder attachment	Price advantage and service advantages
3	Free encoder selection	No limitations for performance, robustness or cost-effectiveness
4	Simple encoder cables	Price advantage: No need for high-end shielded cables
5	No sin/cos adapters	No adapters needed for feeding out the sin/cos tracks for an external monitoring device
6	Reaction time	The response to limit value violations occurs directly in the drive controller in just a few milliseconds; run times of external components until the drive controller is switched off are eliminated
7	Service concept	Exchange the SD card and that's it!
8	Cost-effectiveness	Project configuration using DS6, economically attractive complete solution
9	Safe brake management	Almost no competition on the market
10	Safety level	SIL 3/PL e/ Cat. 4 for all safety functions
11	Retrofitting	Replace the drive controller and that's it!

Table 10: Product advantages compared to classic sin/cos solutions

8. FAQ

Frequently asked questions we hear when talking with our customers are addressed in this chapter.

Note:
We welcome feedback about "Frequently Asked Questions" so that we can improve our documentation.

8.1. Questions about hardware

Why does the SE6 system not need a safe encoder?

> The SD6 with SE6 does not need a safe encoder because SE6 checks the plausibility of the motor encoder.

Why does the SE6 system not need fault exclusion for attachment of the encoder to the motor?

> The encoder plausibility check also detects faults in the mechanical attachment of the encoder.

Why does the SE6 system achieve SIL 3/PL e/Category 4 for the safety functions, while competitors achieve only SIL 2/PL d despite having a safe encoder?

> The encoder plausibility check results in a comprehensive two-channel system in the sensor system area. There are no structural limitations, e.g. based on fault exclusions.

8.2. Questions about software

Why can the "not safe" scope of the DS6 be used to verify the safety functions?

> The DS6 scope is used to check an expectation of the user. If the scope malfunctions, the expectation would not be satisfied.

8.3. Questions about handling

Why does the SE6 need so long (about 5 s) to change from STO to RUN?

> After the SE6 deactivates the STO state, a system test is carried out before the SE6 switches to the operating mode. Due to these system tests, the end customer does not need to run any cyclical function tests. The SE6 is tested before every hazardous function (drive moves).

How can I bypass the long system diagnostics when deactivating STO?

If movements need to be prevented only for a short time, the SS2 safety function can also be used as an alternative to SS1. If this is deactivated again, there is no appreciable delay time in the system.

When is SS1 needed?

DIN EN ISO 13850 describes the requirements for an emergency stop. The description there mentions only SS1 and STO as possible functions for shutdown.

When is an STO needed?

DIN EN ISO 13850 describes the requirements for an emergency stop. The description there mentions only SS1 and STO as possible functions for shutdown.

The STO can be also used as the basis for a restart lockout based on 14118 to protect against unexpected startup.

What advantages are offered by SS2?

In the case of SS2, the drive controller remains in control and can move the drive immediately after the safety function is deselected.

Particularly in the case of central motion controls, the higher-level controller can remain in control and does not have to be re-referenced.

STÖBER Antriebstechnik GmbH + Co. KG
Kieselbronner Strasse 12
75177 Pforzheim
Germany
Phone: +49 7231 582-0
mail@stoeber.de
www.stober.com

24-hour Service Hotline
+49 7231 582-3000