Home

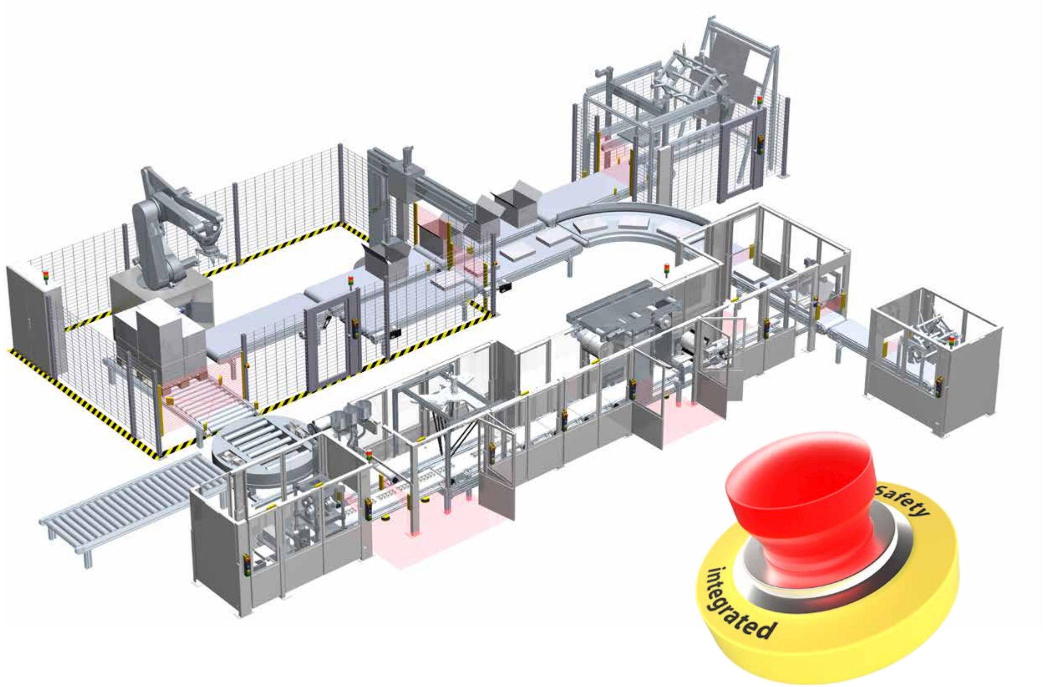
Functional safety

Stop functions

Monitoring functions

Help and maintenance functions

Safety bus



Functional safety

Integrated in the inverter

Functional safety

Functional safety

The functional safety describes the required measures that need to be taken by means of electrical or electronic equipment to prevent or eliminate dangers due to functional errors. For this purpose, the functional safety in the inverter provides safety functions, safe inputs and safe outputs.

This means that the prerequisites on the control and drive side for optimum practical implementation of protective functions for the protection of persons on machines in accordance with the Machinery Directive are met. Planning and installation expenditure is reduced.

Functional safety monitors the safe compliance with limit values. If monitored limit values are exceeded, the functional safety initiates reactions for the error case according to EN 61800-5-2.

This documentation describes the safety functions available in the inverters that can be used for machine safety. The individual functions are described independently of the inverter to provide a basis for risk assessment.

Identification of the components

The functional safety components and the associated terminals are usually marked in yellow. Since the functional safety standards do not prescribe color coding, the components and terminals can also be designed in other colors.

Certification

The certification of the integrated safety is based on these test fundamentals:

- EN ISO 13849−1: Safety of machinery − safety-related parts of control systems − Part 1
- EN ISO 13849−2: Safety of machinery − safety-related parts of control systems − Part 2
- EN 60204−1: Safety of machinery − electrical equipment of machines − Part 1
- IEC 61508, Part 1−7: Functional safety of safety-related electrical/electronic/programmable electronic systems
- EN 61800−5−1: Adjustable speed electrical power drive systems − Part 5−1: Safety requirements − electrical, thermal and energy
- EN 61800−5−2: Adjustable speed electrical power drive systems − Part 5−2: Safety requirements − functional safety
- IEC 62061: Safety of machinery − functional safety of safety-related electrical/electronic/programmable electronic control systems

Functional safety

Risk assessment

Before a machine can be put into circulation, the manufacturer of the machine has to conduct a risk assessment according to the 2006/42/EG: Machinery Directive [UKCA: S.I. 2008/1597 - The Supply of Machinery (Safety) Regulations 2008] to determine the hazards associated with the use of the machine.
For the preparation of the risk assessment, the relevant guidelines, standards and laws must be taken into account.

The risk assessment procedure

Safety of machinery, risk assessment and risk reduction are described in DIN EN ISO 12100:2013-08. With the result of the risk assessment, the machine manufacturer determines the required risk reduction (SIL, PL) for the selected safety functions according to DIN EN ISO 13849-1 or EN 62061.

⚠ **DANGER!**

Improper installation of the safety technology can cause an uncontrolled starting action of the drives.

- Possible consequence: Death or severe injuries
- Possible remedy:
  - Safety technology may only be installed and commissioned by qualified personnel.
  - Observe the documentation of the respective inverters.

Project planning

Note during project planning:

- Use of additional components
  - Only components that are appropriate to the risk reduction of the application may be used.
- Service life
  - For functional safety components, the service life must be observed.
  - After the service life of a component has expired, the component must be replaced. Further operation is not permitted!
- Acceptance
  - The machine manufacturer must check and prove the operability of the safety functions used.
- Functional test
  - After installation and after every modification, the machine operator must check and validate the safety function.
  - During operation, the safety functions must be checked and validated at regular intervals. The risk assessment or prevailing regulations determine the time intervals between the inspections.

For detailed project planning and error-free handling of the safety functions, it is essential that you observe the "Original operating instructions/project planning document" documentation of the inverter.

Functional safety

Safety functions

With the safety functions in the inverter, limit values of motion functions can be monitored safely. In the event of an error, operation of the system is stopped via the stop functions.

There are special help and maintenance functions for setup operation and maintenance of the system.

The available safety functions depend on the inverter series. Observe the features of the inverters.

Stop functions

These safety functions cause the system to stop:

- Safe torque off (STO)
- Safe stop 1 (SS1)
- Safe stop 2 (SS2)
- Safe stop emergency (SSE)
- Safe operational stop (SOS)
- Safe brake control (SBC)
- Cascading STO (CAS) (trigger STO in several inverters simultaneously)

Monitoring functions

These safety functions monitor limit values of speed-dependent or position-dependent motion functions:

- Safe maximum speed (SMS)
- Safely limited speed (SLS)
- Safe speed monitoring (SSM)
- Safely limited increment (SLI)
- Safe direction (SDI)
- Safely limited position (SLP)
- Safe position-dependent speed (PDSS)
- Safe cam (SCA)

Help and maintenance functions

These functions are used to set up and maintain the system:

- Safe homing (SHOM)
- Operation mode selector (OMS)
- Repair mode selector (RMS)
- Enable switch (ES)
- Safe Muting (MUT)

Safety bus

A safety bus can be established via the following networks:

- PROFINET or PROFIBUS with PROFIsafe protocol
- EtherCAT with FSoE protocol

Safe parameter setting

To use the safety functions, the appropriate parameters must be set in the inverters. These parameters are not directly accessible, but are subject to "safe parameterization". These are set via a separate dialog in the Engineering Tools "EASY Starter", "PLC Designer" or "Engineer".

Functional safety

Safety instructions

By safety instructions, we mean information for the use of products that serves to warn the user of hazards and to instruct behavior that will not result in harm to people. In this document, these are distinguished as follows according to ANSI Z535.6:

⚠ DANGER!

Indicates an extremely hazardous situation. Failure to comply with this instruction will result in severe irreparable injury and even death.

⚠ WARNING!

Indicates an extremely hazardous situation. Failure to comply with this instruction may result in severe irreparable injury and even death.

⚠ CAUTION!

Indicates a hazardous situation. Failure to comply with this instruction may result in slight to medium injury.

NOTE

Indicates a material hazard. Failure to comply with this instruction may result in material damage.

Numeric notation

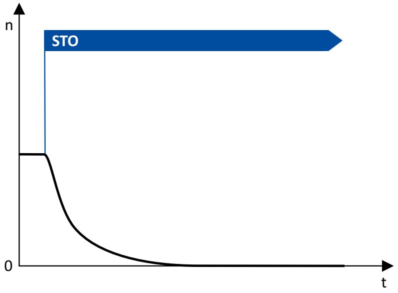
As a rule, a period is used as a decimal separator in this documentation.
Example: 1234.56

Stop functions

STO | SS1 | SSE | SS2 | SOS | SBC | CAS

Safe torque off (STO)

The STO safety function causes the drives to coast during shutdown. The STO safety function corresponds to "Stop category 0" according to EN 60204. With this function, additional measures are required for an "emergency switching off" according to EN 60204-1.



Direct activation

This safety function can be activated via a safe input or via a safety bus.

Triggering this safety function

Automatically after the safety functions have expired:

- Safe stop 1 (SS1)
- Safe stop emergency (SSE)

As a consequence in case of errors in the safety functions:

- Safe operational stop (SOS)
- Safe maximum speed (SMS)
- Safely limited speed (SLS)
- Safely limited increment (SLI)
- Safe direction (SDI)
- Safely limited position (SLP)
- Safe position-dependent speed (PDSS)

⚠ **DANGER!**

The power supply is not safely disconnected.

- Possible consequence: Death or severe injuries due to electrical voltage.
- Possible remedy: Turn off the power supply.

Uncontrolled rotation of the motor possible.

- Possible consequence: Death or severe injuries
- Possible remedy: Set the motor to standstill mechanically.

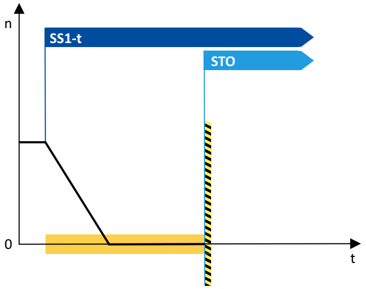
Automatic restart can occur if the request of the safety function is deactivated.

- Possible consequence: Death or severe injuries
- Possible remedy: External measures that ensure an acknowledged restart ensure that the drive does not start until acknowledged.

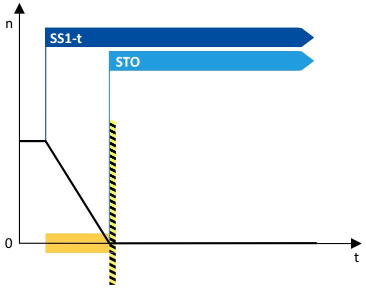
Stop functions

Safe stop 1 (SS1)

With the SS1 safety function, the drive is brought to a standstill over an elapsed time. In addition, a delay for the automatic triggering of STO can be set. The safety function SS1 corresponds to "Stop category 1" according to EN 60204.
Alternatively, the zero speed can be monitored and then STO can be triggered immediately.



Via deceleration time



Via standstill

When setting the values, make sure that the drive actually comes to a standstill after the time has elapsed, since the STO function is activated after the time has elapsed. If the drive is not at standstill at the time, it coasts to a stop.

Direct activation

This safety function can be activated via a safe input or via a safety bus.

Triggering this safety function

Automatically after the safety functions have expired:

- Safe stop emergency (SSE)

As a consequence in case of errors in the safety functions:

- Safe maximum speed (SMS)
- Safely limited speed (SLS)
- Safely limited increment (SLI)
- Safe direction (SDI)
- Safely limited position (SLP)
- Safe position-dependent speed (PDSS)

⚠ **DANGER!**

The power supply is not safely disconnected.

- Possible consequence: Death or severe injuries due to electrical voltage.
- Possible remedy: Turn off the power supply.

Uncontrolled rotation of the motor possible.

- Possible consequence: Death or severe injuries
- Possible remedy: Set the motor to standstill mechanically.

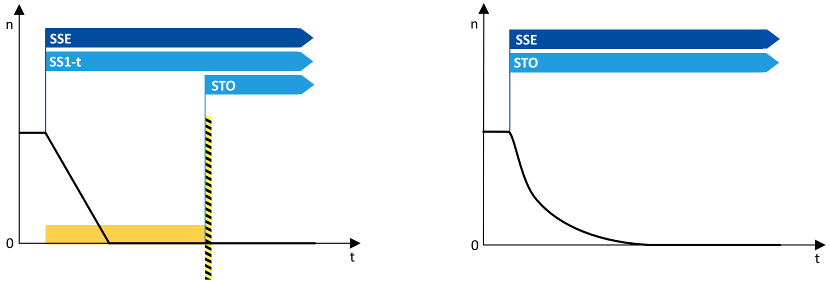
Automatic restart can occur if the request of the safety function is deactivated.

- Possible consequence: Death or severe injuries
- Possible remedy: External measures that ensure an acknowledged restart ensure that the drive does not start until acknowledged.

Stop functions

Safe stop emergency (SSE)

The safety function SSE has a higher priority for triggering SS1 or STO. The safety function SSE is primarily controlled from all states, operating modes or safety functions, and the assigned stop function is triggered immediately



Direct activation

This safety function can be activated via a safe input or via a safety bus.

DANGER!

The power supply is not safely disconnected.

- Possible consequence: Death or severe injuries due to electrical voltage.
- Possible remedy: Turn off the power supply.

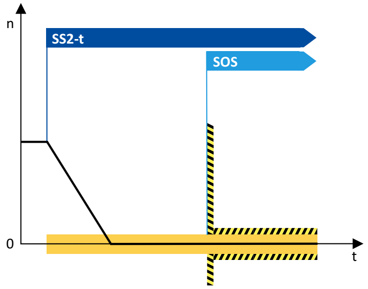
Automatic restart can occur if the request of the safety function is deactivated.

- Possible consequence: Death or severe injuries
- Possible remedy: External measures ensure that the drive only starts after confirmation.

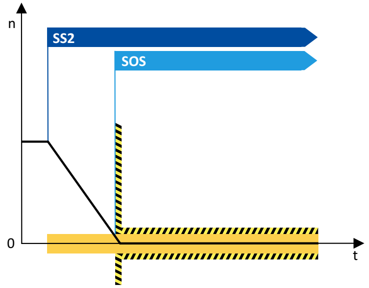
Stop functions

Safe stop 2 (SS2)

With the SS2 safety function, the drive is brought to a standstill over an elapsed time. The position reached is actively held and monitored via the SOS stop function. The SS2 safety function corresponds to "Stop category 2" according to EN 60204.



Via deceleration time



Via standstill

When setting the values, make sure that the drive is actually in the SOS tolerance window after the time has elapsed. If this is not the case, the STO function is activated and the drive is torque-free.

Direct activation

This safety function can be activated via a safe input or via a safety bus.

Triggering this safety function

As a consequence in case of errors in the safety functions:

- Safe maximum speed (SMS)
- Safely limited speed (SLS)
- Safe speed monitoring (SSM)
- Safely limited increment (SLI)
- Safe direction (SDI)
- Safely limited position (SLP)
- Safe position-dependent speed (PDSS)

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety-rated encoder system.

Automatic restart can occur if the request of the safety function is deactivated.

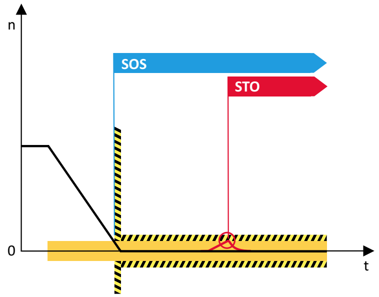
- Possible consequence: Death or severe injuries
- Possible remedy: External measures ensure that the drive only starts after confirmation.

Stop functions

STO SS1 SSE SS2 SOS SBC CAS

Safe operational stop (SOS)

In contrast to the STO function, the SOS safety function does not cause the drive to coast to a stop; instead, the drive is brought to a standstill and the position reached is actively held.



Direct activation

This safety function can be activated via a safe input or via a safety bus.

Triggering this safety function

Automatically after the safety functions have expired:

- Safe stop 2 (SS2)

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Automatic restart can occur if the request of the safety function is deactivated.

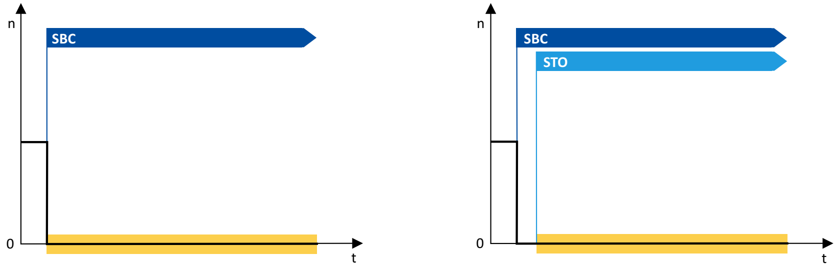
- Possible consequence: Death or severe injuries
- Possible remedy: External measures ensure that the drive only starts after confirmation.

Stop functions

STO | SS1 | SSE | SS2 | SOS | SBC | CAS

Safe brake control (SBC)

SBC enables the safe activation of a spring-applied brake of the drive. By switching off the brake voltage, the brake is applied immediately. To relieve the drive, STO can be activated simultaneously or with a time delay.



Direct activation

This safety function can be activated via a safe input or via a safety bus.

⚠ DANGER!

The power supply is not safely disconnected.

- Possible consequence: Death or severe injuries due to electrical voltage.
- Possible remedy: Turn off the power supply.

Automatic restart can occur if the request of the safety function is deactivated.

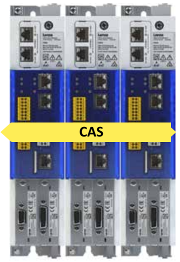
- Possible consequence: Death or severe injuries
- Possible remedy: External measures ensure that the drive only starts after confirmation.

Stop functions

Cascading STO (CAS)

CAS is not a safety function, but the combination of the STO safety function on one signal for several drives.

With this cascading, several drives can be switched off synchronously by triggering an STO message. All affected drives then coast to a stop.



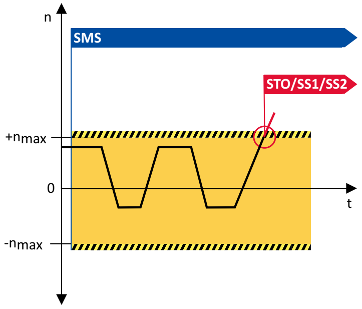
Activation

For cascading, the STO signal must be transferred from a safe output to a safe input of the slave drive. For the restart of the system, the safety function must then be acknowledged for each drive.

Monitoring functions

Safe maximum speed (SMS)

SMS can be used to monitor the maximum speed of the drive.



Direct activation

This safety function is activated by parameterizing the maximum speed.

Response when monitoring limits are exceeded

Triggering the stop functions STO, SS1 or SS2.

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

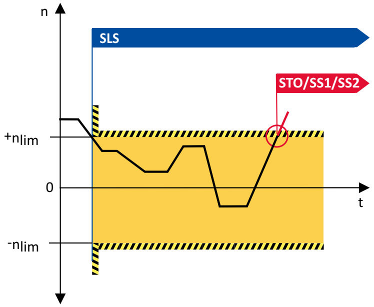
- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Monitoring functions

SMS | SLS | SSM | SLI | SDI | SLP | PDSS | SCA

Safely limited speed (SLS)

With SLS, any operating speed of the machine can be monitored.
Monitoring starts when the actual speed is within the set monitoring limits.



Direct activation

This safety function is activated via a safe input or via a safety bus.

Response when monitoring limits are exceeded

Triggering the stop functions STO, SS1 or SS2.

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Monitoring functions

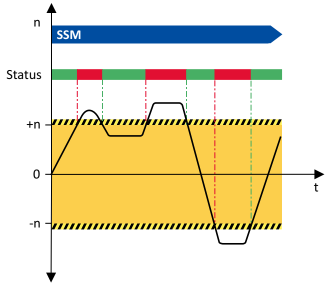
Safe speed monitoring (SSM)

With SSM, the amount of any operating speed of the machine can be monitored. Compliance with the monitoring limits is signaled by a status message.

Application examples:

- Safe speed monitoring.

Despite excessive speed, no immediate machine standstill may occur. The operating personnel is only informed safely.



Direct activation

This safety function is activated by parameterizing the monitored operating speed.

Response when monitoring limits are exceeded

- Safety bus: Status bit is reset
- Safe output: active/inactive

⚠ DANGER!

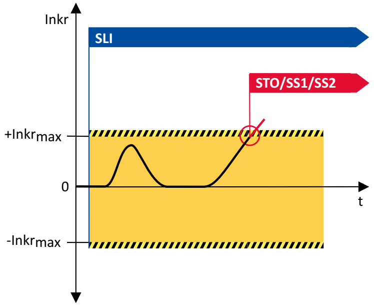
Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Monitoring functions

Safely limited increment (SLI)

SLI can be used to monitor the amount of a maximum permissible position change.



Direct activation

This safety function is activated via a safe input or via a safety bus.

Response when monitoring limits are exceeded

Triggering the stop functions STO, SS1 or SS2.

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

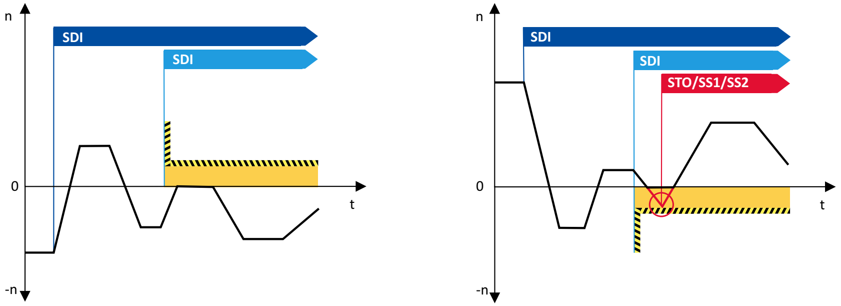
- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Monitoring functions

Safe direction (SDI)

With SDI, the direction of rotation of the machine can be monitored.

A tolerance window can be used to define the number of increments that the drive may move in the blocked direction.



Direct activation

This safety function is activated via a safe input or via a safety bus. A delay time for monitoring can be set.

Response when monitoring limits are exceeded

Triggering the stop functions STO, SS1 or SS2.

DANGER!

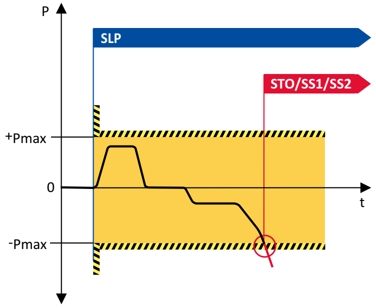
Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Monitoring functions

Safely limited position (SLP)

With SLP, the absolute position limits of a permissible movement range can be monitored.



Direct activation

This safety function is activated via a safe input or via a safety bus.

Response when monitoring limits are exceeded

Triggering the stop functions STO, SS1 or SS2.

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Monitoring functions

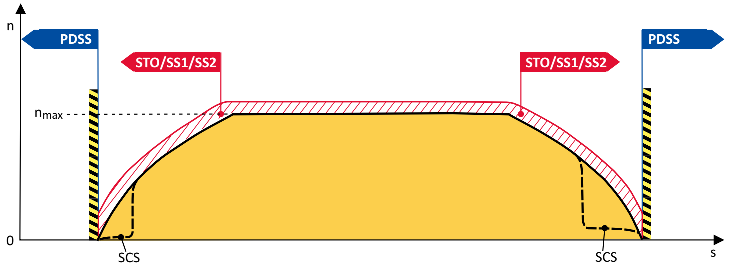
Safe position-dependent speed (PDSS)

PDSS can be used to monitor the speed of a drive as a function of the absolute position along a physically limited range of motion. e.g. a storage and retrieval machine between the end positions.

Using the parameterized values for the maximum speed, for the decelerations and for the absolute end positions, PDSS calculates the maximum speed at each position to ensure timely standstill at the position limits. In addition, two creep speeds can be parameterized to approach the position limits more slowly.

As a result, mechanical buffers can be dimensioned smaller or mechanical buffers and limit switches can be dispensed with altogether. A suitable safety-rated mechanical braking system may be required.

From the end positions, the drive can travel with maximum acceleration.



Direct activation

This safety function is activated via a safe input or via a safety bus.

Response when monitoring limits are exceeded

Triggering the stop functions STO, SS1 or SS2.

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

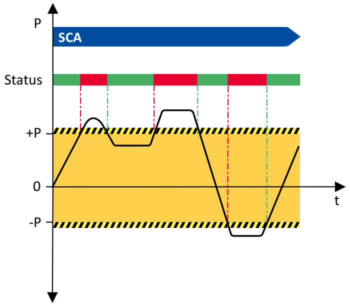
Monitoring functions

Safe cam (SCA)

With SCA the amount of any position can be monitored. Compliance with the monitoring limits is signaled by a status message.

Application examples:

- Monitoring the parking position of a storage and retrieval machine.
- Collision avoidance for an X-Y-Z gantry when there is a fixed obstacle in the travel range.



Direct activation

This safety function is activated via the parameterization of the cam values (position values).

Response when monitoring limits are exceeded

- Safety bus: Status bit is reset
- Safe output: active/inactive

⚠ DANGER!

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

Help and maintenance functions

Safe homing (SHOM)

Safety functions based on absolute positions require an absolute reference point to calculate and monitor the position. The definition of the absolute reference point is required because the encoder systems used for position evaluation do not provide a safe absolute position after the system is switched on for the first time.

Activation

SHom is activated by a control signal. The home position is taken over by a second control signal, which must follow the first control signal in a defined time interval.

Response in the event of errors

A faulty reference run triggers the STO stop function.

⚠ **DANGER!**

Uncontrolled rotation of the motor possible if no safety rated encoder system is used.

- Possible consequence: Death or severe injuries
- Possible remedy: Use a safety rated encoder system to use this function.

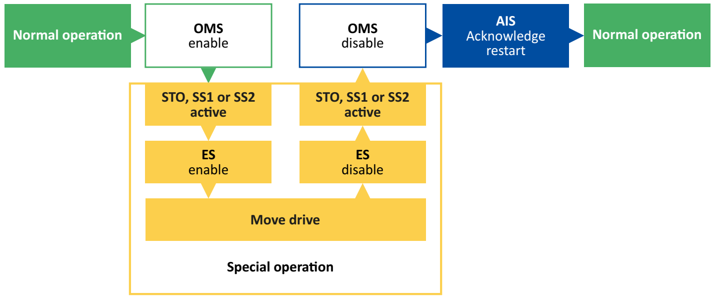
Help and maintenance functions

Operation mode selector (OMS)

OMS is not a safety function per se, but is used to commission the system. In this way, the corresponding safety functions can be activated or deactivated.

After switching to OMS, one of the configurable stop functions STO, SS1 or SS2 is active. The enable switch is used to override the active stop function and the control functions can be tested.

Separate motion functions SLI and SLS can be defined for OMS.



Direct activation

The operation mode selector (OMS) can be activated via a safe input or via a safety bus.

Help and maintenance functions

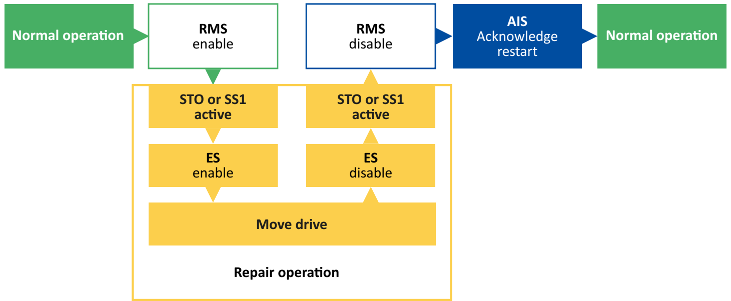
Repair mode selector (RMS)

If the drive is completely blocked by a faulty encoder system ("deadlock"), this function can be used to remove the blockage and move the drive.

After switching to "RMS", one of the configurable stop functions STO or SS1 is active. The enable switch is used to override the active stop function and the drive can be moved out of the "deadlock".

Please note the following:

- The connected encoders are not evaluated safety-related.
- Only the stop functions configurable for RMS and the enable switch ES are active.
- All other safety functions are deactivated.



Direct activation

The repair mode (RMS) can be activated via a safe input or via a safety bus.

Response in the event of errors

If the current positions are outside parameterized tolerance windows after returning from repair mode, the STO stop function is triggered.
A new reference run is required.

⚠ DANGER!

Unexpected motions with unexpected speed.
Violation of the permissible movement limits.

- Possible consequence: Death or severe injuries
- Possible remedy:
  - Use RMS exclusively to free a drive from a "deadlock".
  - If necessary, take additional safety measures to ensure that no persons can be endangered, since all monitoring functions are deactivated except for the ES enable switch.
  - Use other functions to move the drive when it is not in a "deadlock"!

Help and maintenance functions

SHom OMS RMS ES MUT

Enable switch (ES)
ES overrides the stop function active in special mode OMS or RMS. The stop function is deactivated without delay. The drive can then be moved freely as long as the enable switch is active. If the enable switch is deactivated, the stop function for special operation is activated again without delay.

Direct activation
The enable switch can be activated via a safe input or via a safety bus.

Help and maintenance functions

Safe Muting (MUT)

MUT is used during commissioning or maintenance of the system.

With MUT, individual safe inputs and outputs and/or the safety bus can be deactivated for a short period of time.

Activation

As this function may only be used for commissioning and maintenance of the system, the Engineering Tool EASY Starter or PLC Designer is required for activation.
Activation is only possible with your own safe muting password.
Safe muting is active for a maximum of 30 minutes and is automatically deactivated after this time has elapsed. The drive immediately switches back to monitored operation.

Response in the event of errors

If the Safe Muting function is cancelled by an error, the monitored operation is immediately reactivated.
All previously deactivated safety functions are active again.

⚠ **DANGER!**

Activating the Safe Muting function deactivates safety functions!

- Possible consequence: Death or severe injuries
- Possible remedy:
  - Only authorized personnel may activate the Safe Muting function.
  - An emergency stop measure must be available that cannot be deactivated by Safe Muting.

Safety bus

PROFIsafe FSoE

PROFIsafe

PROFIsafe is the certified safety protocol for the transmission of safety-related data via PROFINET® or PROFIBUS®.

This safety bus supports the transmission of safe information via the PROFIsafe protocol according to the specification "PROFIsafe Profile for Safety Technology", version 2.0, of the PROFIBUS User Organization (PNO). The general data definitions of PROFIsafe apply.

The inverter must be equipped with a PROFINET or a PROFIBUS module. The inverter forwards the PROFIsafe information for safe evaluation.

Addressing

A unique PROFIsafe destination address is required so that a data telegram reaches the correct device. The safety address is adopted as the PROFIsafe target address. This address must match the corresponding configuration of the safety PLC.

Safety bus

PROFIsafe FSoE

FSoE

Fail-safe-over-EtherCAT (FSoE) PROFIsafe is the certified safety protocol for the transmission of safety-related data via EtherCAT®.

This safety bus enables the transmission of safe information via the FSoE protocol according to specification ETG.5100 S, version 1.2.0 of the EtherCAT user organization (ETG). The general data definitions of the EtherCAT apply.

The inverter must be equipped with an EtherCAT module. The inverter forwards the FSoE information for safe evaluation.

Safety over EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.

Safety over EtherCAT®

Addressing

A unique FSoE destination address is required so that a data telegram reaches the correct device. The safety address is taken as the FSoE target address. This address must match the corresponding configuration of the safety PLC