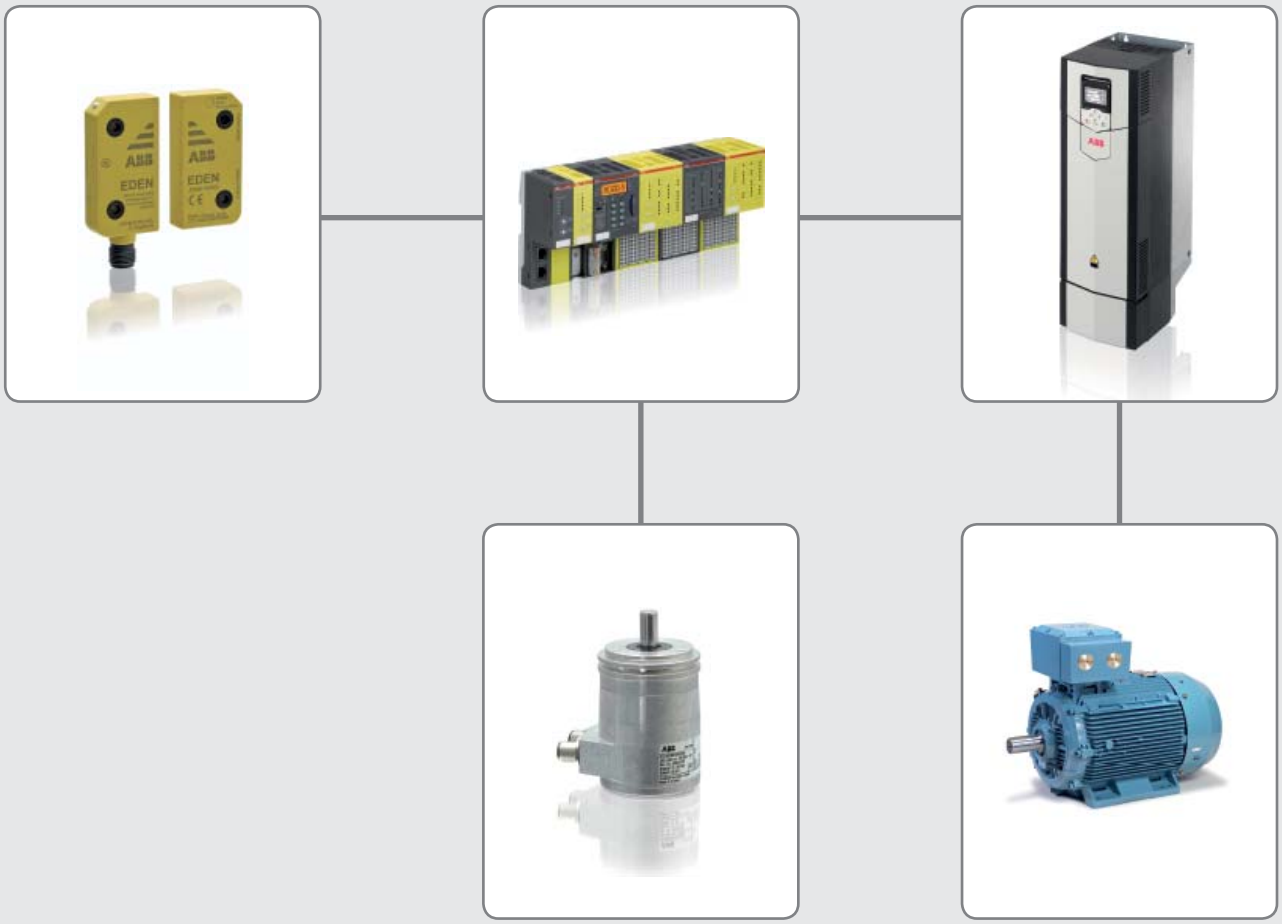
Technical description
How to implement a safe stop 1 function, with an ACS880-01 and an AC500-S safety PLC



This document presents details how a safe stop 1 (SS1) safety function can be designed and implemented using ACS880-01 industrial drives and a AC500-S safety PLC together with other ABB safety devices. The safety function is implemented according to EN/IEC 62061, EN ISO 13849-1, EN/IEC 60204-1 and EN/IEC 61800-5-2 machinery standards. Necessary SIL/PL calculations are presented using ABB's Functional safety design tool.

Safer machines with drive-based functional safety

Drive-based safety functions are used in applications that require risk reduction from eg. unexpected and hazardous movement. The aim is to design machines that are safe to use. This safety function example is presented for specific drive and safety devices, but the function can be implemented with other ABB drives with few modifications.

ACS880-01 industrial drives can be connected with AC500-S safety PLC to implement an encoderless safe stop 1 (SS1) safety function. This function brings the machine to a controlled stop and uses the safe torque off (STO) safety function integrated in the ACS880-01 drive. STO eliminates the need for using contactors. This results in the drive not being disconnected from the supply during safe stopping. As a result, the drive and machine restarts are fast.

ACS880-01 R5 drive

Eden OSSD non-contact safety sensor

AC500-S safety PLC

PROFIsafe encoder

Effective and reliable safe stop 1 function for drive applications

Safe stop 1 function details	
Requirements according to EN/IEC 60204-1 and EN/IEC 61800-5-2	**Safe stop 1** initiates and monitors or controls the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit. **Stop category 1:** a controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved.
Safety integrity level	SIL 2 (EN/IEC 62061), PL d (EN ISO 13849-1)

Overview of the safety function

The SS1 safety function (Figure 1) is a stop category 1 function that stops the drive with a controlled deceleration ramp before disabling the power output from the drive to the motor. In this example, the function monitors the deceleration ramp. SS1 can be used, for example, in applications where the machine movement has to be brought to a stop in a controlled way before switching to a non-torque state.

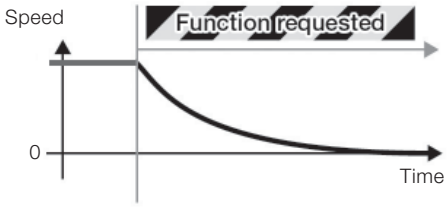


Figure 1: SS1 safety function using ramp monitoring method.

Design of the safety function

The design of the safe stop 1 (SS1) safety function consists of a non-contact safety sensor as an activating switch, safety PLC as a logic unit with an encoder providing speed feedback and a safe torque off (STO) -circuit inside the ACS880-01 drive as an actuator to bring the motor into a non-torque state after the deceleration. See circuit diagram (Figure 2) for connection details.

Operation of the safety function

When the Eden sensor is activated, the PLC detects the sensor signal and commands the drive to stop the motor using a deceleration ramp. The PLC monitors the deceleration using the PROFIsafe encoder, and after the motor has stopped the PLC activates the STO function to bring the motor into a non-torque state.

To continue operation after a safe stop, the Eden sensor is returned to the stand-by position. This deactivates the SS1 safety function in the safety PLC, causing PLC to deactivate the STO function. The drive is restarted by a separate command. The drive is configured not to start automatically.

The safety PLC provides diagnostics for the activating sensor wiring. The PLC also enables the use of a separate reset button, if required (reset button is not shown in this example since it is not required by the standard).

Ensuring the required safety performance

The safety function has to fulfil the required safety performance determined by a risk assessment. ABB's Functional safety design tool (FSDT-01) is used to design the desired safety function. This is carried out according to the following steps:

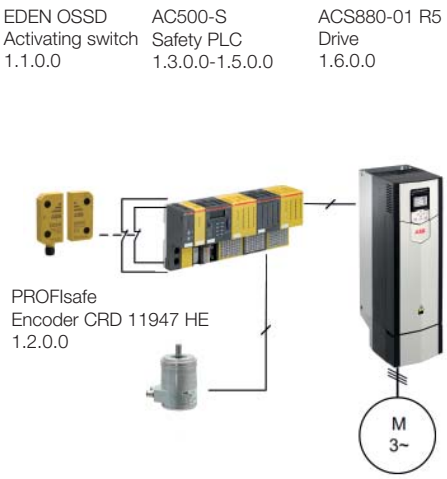
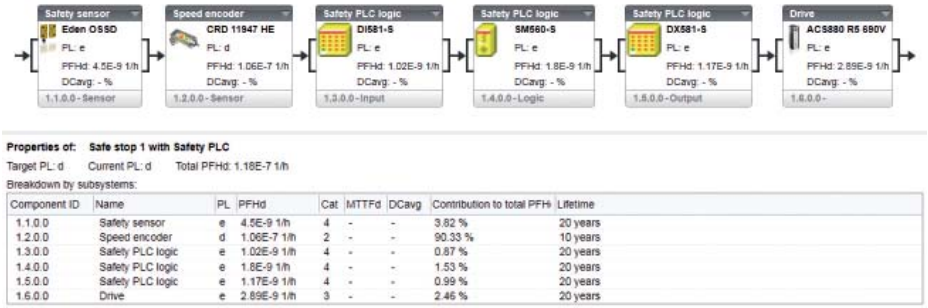


Figure 2: Connection example of the safe stop 1 (SS1) safety function with ACS880-01 and AC500-S safety PLC. Reset button is not used in this example.



Properties of: Safe stop 1 with Safety PLC

Target PL: d Current PL: d Total PFHd: 1.18E-7 1/h

Breakdown by subsystems:

Component ID	Name	PL	PFHd	Cat	MTTFd	DCavg	Contribution to total PFH	Lifetime
1.1.0.0	Safety sensor	e	4.5E-9 1/h	4	-	-	3.82 %	20 years
1.2.0.0	Speed encoder	d	1.06E-7 1/h	2	-	-	90.33 %	10 years
1.3.0.0	Safety PLC logic	e	1.02E-9 1/h	4	-	-	0.87 %	20 years
1.4.0.0	Safety PLC logic	e	1.8E-9 1/h	4	-	-	1.53 %	20 years
1.5.0.0	Safety PLC logic	e	1.17E-9 1/h	4	-	-	0.99 %	20 years
1.6.0.0	Drive	e	2.89E-9 1/h	3	-	-	2.46 %	20 years

Figure 3: Safety calculation and design for the safe stop safety function according to EN ISO 13849-1 (can also be made according to EN/IEC 62061). The design is made with the Functional safety design tool.

1. **Evaluate the risks** to establish target safety performance (SIL/PL level) for the safety function.

2. **Design** the safety function loop and **verify** the achieved performance level (PL) or safety integrity level (SIL) for the safety function loop (according to EN ISO 13849-1 or EN/IEC 62061, respectively), utilizing the device safety data and the application specific characteristics.

3. **Generate a report** for the machine documentation. Report should contain all the calculation results as well as all assumptions made during the application design.

Figure 3 shows the design of the safe stop 1 function with the ACS880-01 drive. The safe stop 1 function in this document achieves PL d (SIL 2). Calculations are made using the default safety data available for the safety devices.

Safety function verification and validation

In addition to the safety calculations for the achieved safety performance (SIL/PL), the safety function needs to be functionally verified as well.

Finally the implemented safety function is validated against the risk assessment to ensure that the implemented safety function actually reduces the targeted risk.

General considerations

Achieving machinery safety requires a systematic approach beyond the physical implementation of a safety function. The overall machinery safety generally covers the following areas:

- **Planning** for and managing functional safety during the lifecycle of the machine
- **Assuring compliance** to local laws and requirements (such as the Machinery directive/CE marking)
- **Assessing machine risks** (analysis and evaluation)
- **Planning the risk reduction** and establishing safety requirements
- **Designing** the safety functions
- **Implementing and verifying** the safety functions
- **Validating** the safety functions
- **Documenting** the implemented functions and results of risk assessment, verification and validation

For more information concerning functional safety and the Functional safety design tool, see **www.abb.com/safety** and ABB's Technical Guide no. 10.

Abbreviations

Abbr.	Reference	Description
DC_{avg}	EN ISO 13849-1	Diagnostic coverage
$MTTF_d$	EN ISO 13849-1	Mean time to dangerous failure
PFH_d	EN/IEC 62061	Probability of dangerous failures per hour
PL	EN ISO 13849-1	Performance level: corresponds to SIL, Levels a-e
SIL	EN/IEC 62061	Safety integrity level

Note: This is an indicative example. Relevant installation, design and safety calculations need to be specifically completed for each system implementation according to machinery safety standards (EN/IEC 62061, EN ISO 13849-1, EN/IEC 60204-1 and EN/IEC 61800-5-2). ABB does not take any responsibility of the accuracy of the data used in this document and reserves right to make changes without further notice. For detailed safety function implementation please contact your local ABB representative.

Contact us

www.abb.com/drives
www.abb.com/drivespartners

Drive-based functional safety web page

3AUA0000172919 REV A EN 22.12.2014 #17366

Power and productivity for a better world™