Technical description
How to implement a prevention of unexpected startup safety function, with an ACS850 drive

This document presents details how the prevention of unexpected startup (POUS) safety function can be designed and implemented using an ACS850 machinery drive together with other ABB safety devices. POUS in this document is implemented according to EN/IEC 62061, EN ISO 13849-1, EN/IEC 60204-1, EN 1037, ISO 14118 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.

The prevention of unexpected startup safety function can be implemented using a ACS850 drive with integrated safe torque off (STO) function. STO eliminates the need to use contactors, which means that the drive is not disconnected from the power during safe stopping. This again enables fast restart of the drive and the machine. STO is also offered as standard in many ABB drive types for easy integration of functional safety.

ACS850-04 frame A drive

C2SS1-10B-02 selector switch

BT50 safety relay

Effective and reliable prevention of unexpected startup functionality for drive applications

Prevention of unexpected startup function details	
Requirements according to EN/IEC 60204-1, EN 1037 and ISO 14118	**Prevention of unexpected startup** Machines shall be provided with means intended for isolation and energy dissipation: – Isolating the machine from all power supplies – Locking, if necessary, all the isolating units in the "isolated" position – Dissipating or restraining any stored energy which may give rise to a hazard **Isolation devices shall:** – Ensure a reliable isolation – Have a reliable mechanical link between the manual control and the isolating elements – Be equipped with clear and unambiguous identification of the state of the isolation device
Safety integrity level	SIL 3 (EN/IEC 62061), PL e (EN ISO 13849-1)

Overview of the safety function

Prevention of unexpected startup (POUS) prevents the drive from generating the torque required to rotate the motor. This is achieved by activating the STO safety function in the drive. The POUS safety function ensures that the machine does not start, for example during short-time maintenance on the non-electrical parts of the machinery (as STO does not provide electrical disconnection). Restart of the drive is also faster when the drive does not need to be switched off.

Design of the safety function

The design of the POUS consists of a selector switch as an activating switch, a safety relay as a logic unit and safe torque off (STO) -circuit inside the ACS850 drive as an actuator to keep the motor in a non-torque state. POUS Indication (eg. lamp) connected to safety relay indicates the status (whether it is on or off) of POUS function. Indication is not required by the POUS related standards ISO 14118 or EN 1037 and therefore is not included in this design example. See circuit diagram (Figure 1) for connection details.

Operation of the safety function

When the selector switch is turned to the POUS On-position, the safety relay detects the switch signal and opens its contacts to activate the safe torque off (STO) safety function. After STO is activated, it disables drives power output to the motor.

To disable the POUS function, the POUS switch is turned to the Off-position, which causes the relay contacts to close. This deactivates the STO safety function. The ACS850 drive is started by a separate start command. The drive is configured not to start automatically after a POUS function.

The safety relay is used because it provides diagnostics for the switch wiring. The relay also enables the use of a separate reset button (reset button is not shown in this example since it is not required by the standard). POUS indication might be required by other standards than EN/IEC 62061, ISO 13849 or EN 1037 and needs to be added to the design procedure if so.

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:

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

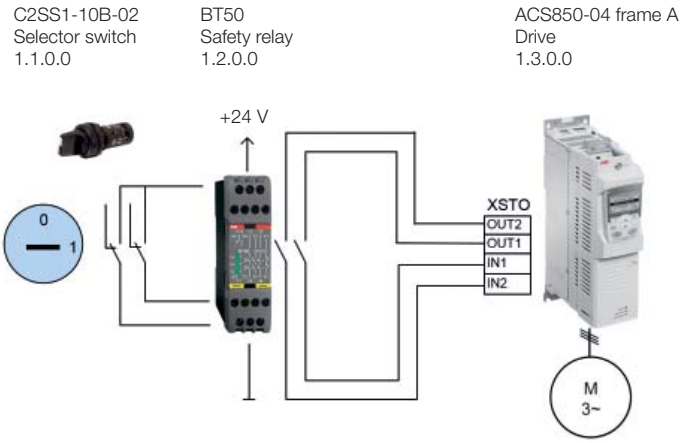
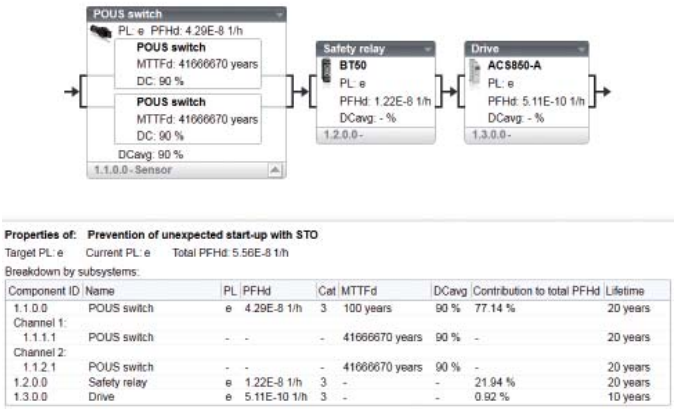


Figure 1: Connection example of the POUS safety function with ACS850. POUS indication is not used in this example.



Properties of: Prevention of unexpected start-up with STO
Target PL: e Current PL: e Total PFHd: 5.56E-8 1/h
Breakdown by subsystems:

Component ID	Name	PL	PFHd	Cat	MTTFd	DCavg	Contribution to total PFHd	Lifetime
1.1.0.0	POUS switch	e	4.29E-8 1/h	3	100 years	90 %	77.14 %	20 years
Channel 1:								
1.1.1.1	POUS switch	-	-	-	41666670 years	90 %	-	20 years
Channel 2:								
1.1.2.1	POUS switch	-	-	-	41666670 years	90 %	-	20 years
1.2.0.0	Safety relay	e	1.22E-8 1/h	3	-	-	21.94 %	20 years
1.3.0.0	Drive	e	5.11E-10 1/h	3	-	-	0.92 %	10 years

Figure 2: Safety calculation and design for the POUS 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.

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 2 shows the design of the POUS function with the ACS850 drive. The POUS function in this document achieves PL e (SIL 3). Calculations are made using the default safety data available for the safety devices. The activation frequency of the POUS is 1 time per day in this example.

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 ISO 13850, EN/IEC 61800-5-2, EN 1037, ISO 14118 and EN/IEC 60204-1) and local laws and regulations. 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

3AUA0000172915 REV A EN 22.12.2014 #17362

Power and productivity
for a better world™