

Technical description

How to implement an emergency stop, category 1, with an ACS580 drive



This document presents details how an emergency stop, stop category 1, safety function can be designed and implemented using an ACS580 general purpose drives together with other ABB safety devices. The safety function is implemented according to EN/IEC 62061, EN ISO 13849-1, EN/IEC 60204-1, EN ISO 13850 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 eg, from 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 functions can be implemented with other ABB drives with few modifications.

ACS580 general purpose drives offer a safe torque off (STO) safety function as a standard integrated feature. 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.



ACS580 R1 drive



INCA 1 emergency stop button



RT7 safety timer relay

Effective and reliable emergency stop functionality for drive applications

Emergency stop function details

Requirements according to EN/IEC 60204-1 and EN ISO 13850

Emergency stop

- Overrides all other functions and operations in all modes at all times
- Power to the machine actuators that can cause a hazardous situation should be removed
- Reset must not initiate a restart
- The emergency stop function shall not be applied as a substitute for safeguarding measures and other safety functions but should be designed for use as a complementary protective measure

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 3 (EN/IEC 62061),
PL e (EN ISO 13849-1)

Overview of the safety function

Emergency stop, stop category 1 (Figure 1), stops the drive with a controlled deceleration ramp before disabling the drive's output to the motor. In this example, the deceleration ramp is time monitored. The safety function can be used, for example, in an application where a synchronized stop of multiple axes is required.

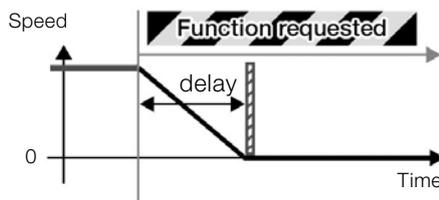


Figure 1: Typical motor speed with a stop category 1 stop.

Design of the safety function

The design of the emergency stop, stop category 1, consists of an emergency stop button as an activating switch, a safety timer relay as a logic unit and a safe torque off (STO) -circuit inside the ACS580 drive. The drive acts 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 emergency stop button is pressed, the safety relay detects the button signal and opens its non-delayed contacts to inform the drive to

decelerate. Simultaneously, the relay's timer for the time delay contacts starts counting. After the time delay has elapsed, the contacts open, activating the STO function, which disables the drive's power output to the motor.

To continue drive operation after an emergency stop, the emergency stop button is released (pulled up), which causes the contacts of the relay to close. This deactivates the STO function. The drive is restarted by a separate start command. The drive is configured not to start automatically.

The safety relay is used because it provides diagnostics for the emergency stop button wiring. The relay 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:

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

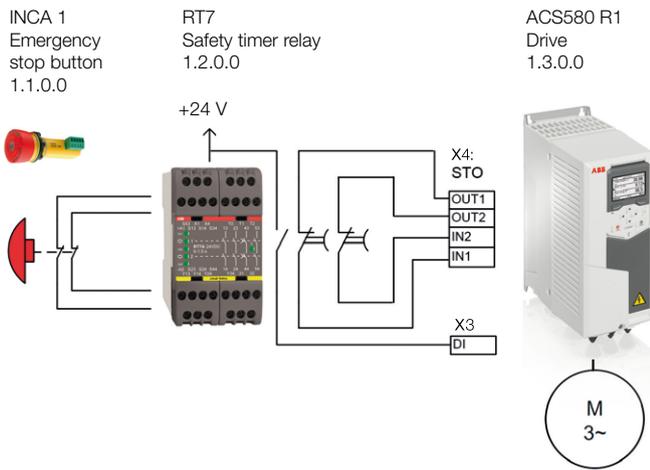
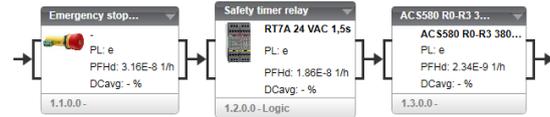


Figure 2: Connection example of the emergency stop function with ACS580. Emergency stop reset button is not used in this example.



Properties of: Emergency stop, stop category 1, with STO

Target PL: e Current PL: e Total PFHd: 5.25E-8 1/h

Breakdown by subsystems:

Component ID	Name	PL	PFHd	Cat	MTTFd	DCavg	Contribution to total PFHd	Lifetime
1.1.0.0	Emergency stop button	e	3.16E-8 1/h	4	-	-	60.14 %	20 years
1.2.0.0	Safety timer relay	e	1.86E-8 1/h	4	-	-	35.4 %	20 years
1.3.0.0	ACS580 R0-R3 380-480V	e	2.34E-9 1/h	3	-	-	4.45 %	20 years

Figure 3: Safety calculation and design for the emergency stop 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 (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 emergency stop with ACS580 drives. The emergency stop function in this document achieves PL e (SIL 3). 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 ISO 13850, EN/IEC 61800-5-2 and EN/IEC 60204-1) and local laws and regulations. ABB does not take any responsibility for 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

© Copyright 2016 ABB. All rights reserved.
Specifications subject to change without notice.



Drive-based functional
safety web page

3AUJ0000192908 REV A EN 17.2.2016 *12939