WHITE PAPER

Drive-based functional safety
maximizing machine safety, uptime and productivity

Safer machines with **drive-based functional safety**

In industrial automation variable speed drives are commonly used to control the speed and torque of motors. Their use helps to improve the energy efficiency, productivity, and efficiency of many applications. Because of their ubiquitous nature in today's industrial landscape, ensuring that drives perform to the highest functional safety standards is essential to prevent accidents, protect personnel, and avoid damage to products and equipment. Drive-based functional safety can boost the productivity of machinery in many ways. For example, cleaning operations can be performed without stopping the machine and equipment and wiring costs can be reduced.

Industrial applications are inherently hazardous. From conveyor belts to bottling machines, anywhere that humans and machines interact holds risks Functional safety solutions minimize or eliminate risks to people, to equipment and to environment.

This whitepaper, updated in 2024, describes some of the functional safety solutions for drives available today.

What is drive-based **functional safety?**

Traditionally, functional safety enables reliable stopping and prevents unexpected startup of the machine. Functional safety can be extended to safely monitor movement and, when necessary, take control of the machine applications to ensure safe operation. Bringing machinery to a safe state quickly and efficiently is a critical aspect of functional safety.

Once stopped, ensuring that a machine does not start unexpectedly is crucial to prevent accidents and protect operators, maintenance personnel, and the surrounding environment. Depending on the application and its work cycles, machines may also need to operate at safely limited speed during specific procedures such as maintenance and repair. Drive-based safety functions cover a wide range of tasks, from those responsible for safely stopping the drive, to those that monitor motion parameters such as speed, position, or torque.

Implementing a machine safety system has become easier today due to several factors that have evolved with advancements in technology and industry standards. For example, drive-based functional safety enables safety functions to be integrated into a drive. Also, modularity provides a wide range of configurable safety features that can be adapted to the specific needs of any given application.

—

Functional safety involves preventing malfunctions, failures and hazardous situations.

Drive-based functional safety solutions in industrial systems

Drive-based functional safety refers to the integration of functional safety features within variable speed drives (VSDs). Functional safety in this context involves implementing measures to ensure that the drive operates in a safe manner, particularly when it comes to preventing or mitigating the impact of malfunctions or failures that could lead to hazardous situations.

All machinery supplied in the European Union must meet the essential health and safety requirements (EHSR) of the EU Machinery Directive 2006/42/EC. Using certified drive-based safety solutions according to IEC61800-5-2, IEC62061 and ISO13849, will reduce the compliance work required on the machinery. For more information, please see ABB drives Technical guide No. 10: Functional safety.

Examples of **Functional safety implementation**

In this section, four examples of functional safety implementation are described:

- **Traditional electromechanical safety solution**
- **Integrated drive-based functional safety**
- **Integrated drive-based functional safety with a safety PLC (STO + SS1)**
- **Integrated drive-based functional safety with a safety PLC**

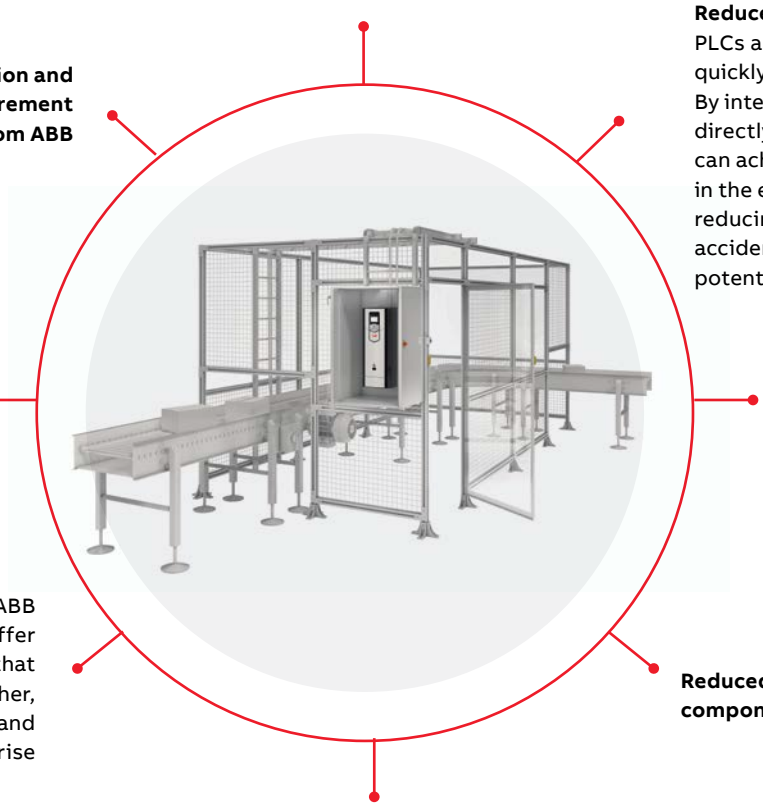
A conveyor belt application has been used as an example because it is an industrial application where functional safety is crucial. People frequently interact with conveyor belts by cleaning, repairing, and placing material on and picking material off them. Based on a safety risk analysis several points need to be considered. Firstly, the motor must remain in a non-torque state during a cleaning or maintenance procedure, because unexpected start-up has been identified as a risk. When a red emergency stop button is pressed, at any time, the conveyor must stop in a safe manner. And when people are near the conveyor inside the protective cage, the conveyor speed must be safely reduced for safe material handling.

Benefits of ABB drive-based functional safety with a safety PLC solution

One wire: The network can be used for process control, monitoring and safety control/status

Seamless integration and streamlining procurement of safety devices from ABB

Reduced response time: Safety PLCs are designed to respond quickly to safety-critical events. By integrating safety functions directly into the drive system, you can achieve faster response times in the event of an emergency, reducing the likelihood of accidents and minimizing potential damage



Easier maintenance and support

Safety monitoring and diagnostics: This allows for monitoring of safety information (e.g., safe motor speed information) and provides feedback to the control system in case of faults or failures

Faster troubleshooting: ABB safety PLC and ABB drives offer integrated safety functions that work seamlessly together, making it easier to identify and resolve issues when they arise

Reduced number of components

Cost savings: While the initial implementation of safety features may require an investment, the enhanced safety and reliability provided by drive-based functional safety with a safety PLC can lead to cost savings in the long run by reducing the risk of accidents, improving productivity, and minimizing downtime

Example 1.
Traditional electromechanical safety solution

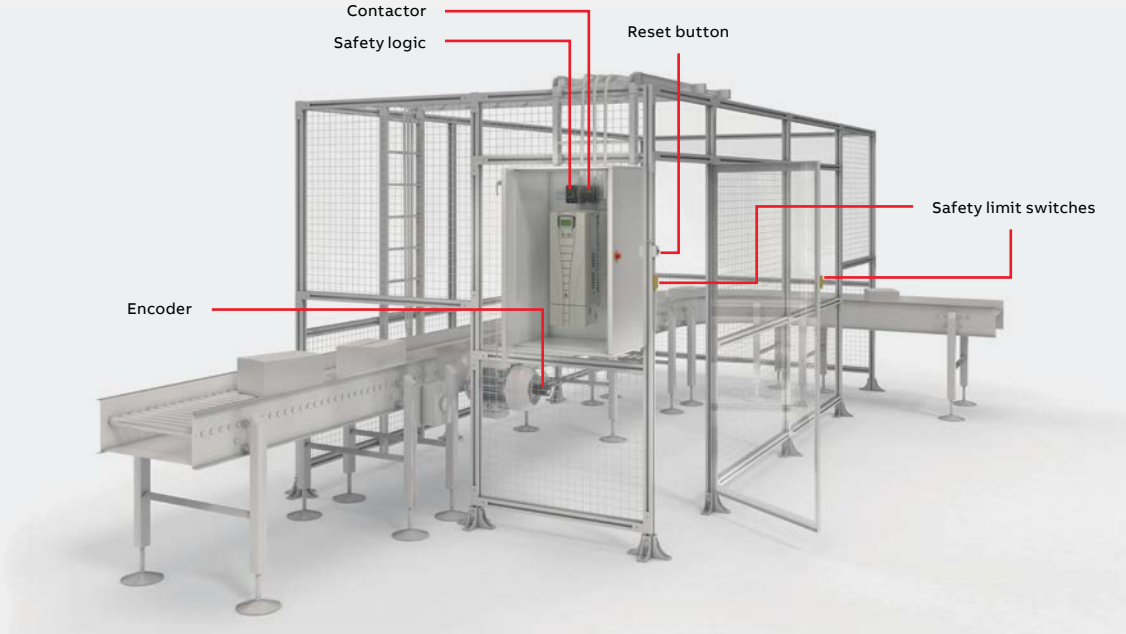
The traditional way of building a safety system includes connecting safety limit switches, relays, external safety monitoring devices and contactors together with the drive. The drive itself has no safety functionality.

When the protective cage door to the conveyor is opened the safety door switch detects the open door. This sends signals to the drive to decelerate. At the same time the signal is sent to an external safety monitoring device (safety logic), which, together with an encoder speed measurement, enables safe speed monitoring.

Traditional electromechanical safety solutions bring extra equipment costs, wiring, and maintenance needs compared to drive / safety – PLC-based safety functions.

Example 1

—
Additional safety devices and wiring are needed compared to integrated drive-based functional safety.



Example 2.
Integrated drive-based functional safety

Integrated drive-based functional safety includes the same functionality as the traditional electromechanical safety solution. The functionality of the drive and safety features are combined simplifying the overall design process.

The most basic functionality is the STO in the drive which eliminates the need for a motor contactor to stop the motor safely. SS1 enhances motor control by providing a controlled ramp to stop. With SLS the motor speed can be reduced for maintenance activities and thus maintain productivity instead of stopping completely.

The complexity of configuration and installation is reduced in several ways:

Fewer components: Single device integration. Integrated drive-based functional safety combines the functionality of the drive and safety features into a single device. This eliminates the need for externally wired discrete safety devices such as safety logic contactors or encoders.

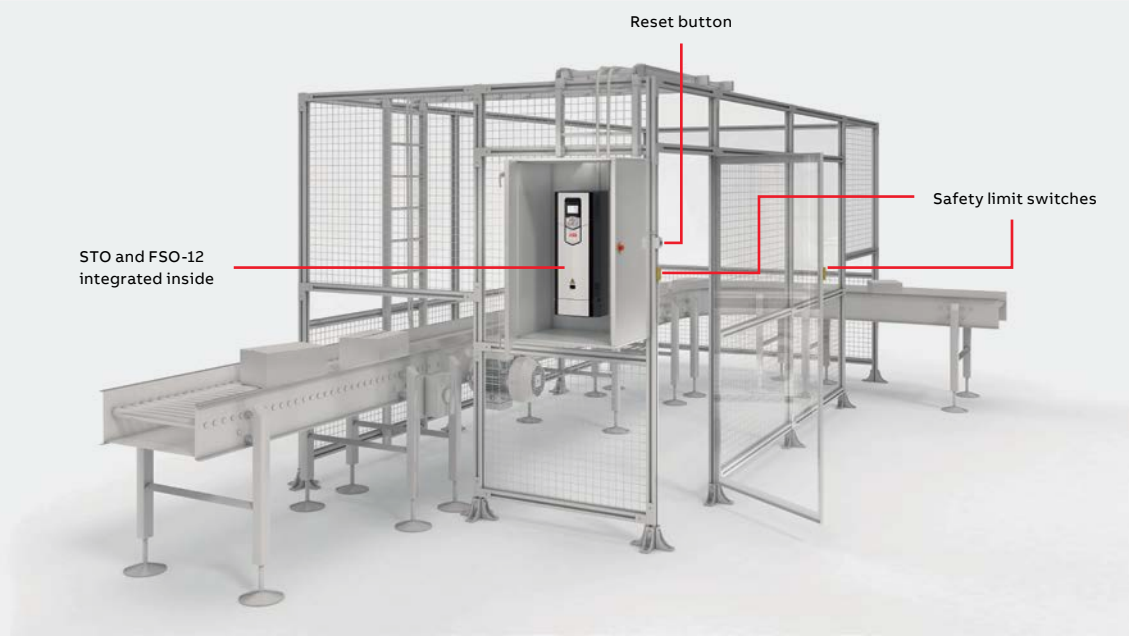
Less wiring: Reduced wiring complexity. With integrated safety features, the need for additional wiring is significantly reduced. Safety signals and functions are communicated internally within the integrated drive, leading to a simplified wiring scheme.

Space and cost savings with the capability for safe speed monitoring without an encoder for applications without external accelerative loads such as hanging loads.

Ease of configuration: Plug-and-play integration. Integrated drive-based safety often supports standardized communication protocols (e.g., PROFISAFE and CIP Safety), making it easier to integrate with other automation components. This plug-and-play capability simplifies the configuration process.

Reduced installation time: The simplified wiring, streamlined configuration, and reduced need for external components contribute to a faster and more straightforward installation process.

Example 2



—
Safety logic integrated into the drive for effective safety monitoring. Less safety devices and wiring needed compared to traditional safety solution).

Example 3.
Integrated drive-based functional safety with a safety PLC (STO+SS1)

In industrial applications it is typical to have several drives/ motors working together. For such cases a safety PLC (E.g. AC500-S) can be used for controlling drives and machines safely from a common source to provide synchronized control. Commonly, safety is achieved by safely stopping the machine in case of maintenance or emergency. For this purpose, ABB drives are optimized by providing safety functions STO and SS1 over PROFIsafe (FSPS-21) and CIP Safety (FSCS-21) which enables safe stop over network with a safety PLC.

Simplicity: Simple safety functions do not require any safety parameters in a drive. Without safety parameters neither safety password protection/management is required on a drive level.

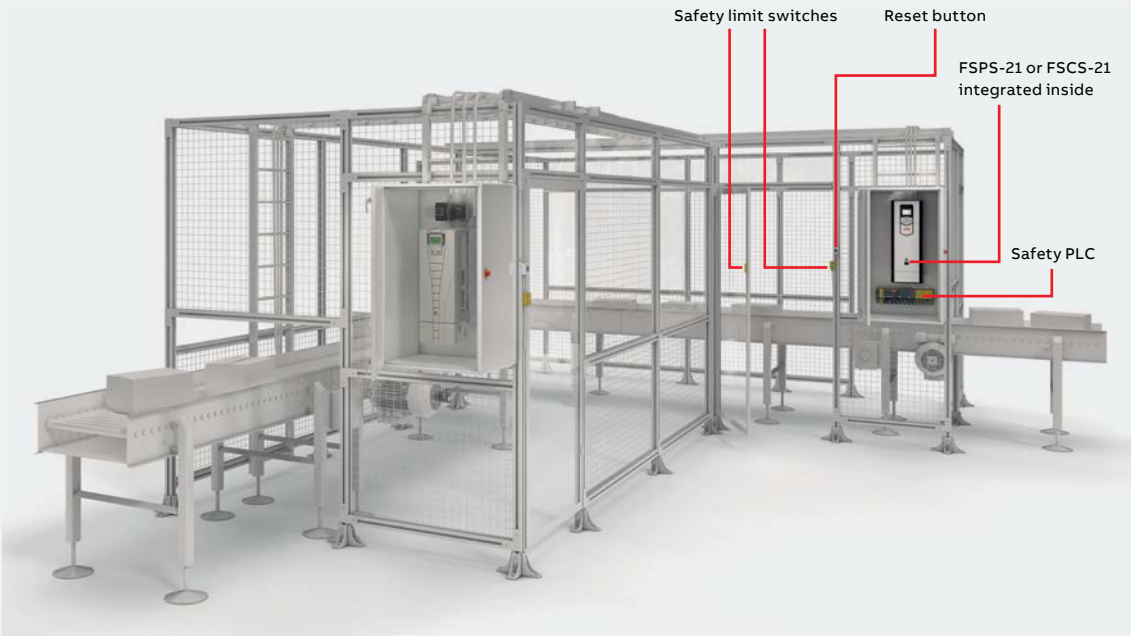
Less wiring: Single ethernet cable for motor control and functional safety.

—

ABB drive-based solutions provide easier maintenance and support, faster troubleshooting, and cost savings.

Example 3

—
Safety system with traditional and integrated drivebased safety functions, controlled by a safety PLC.



Example 4.
Integrated drive-based functional safety with a safety PLC

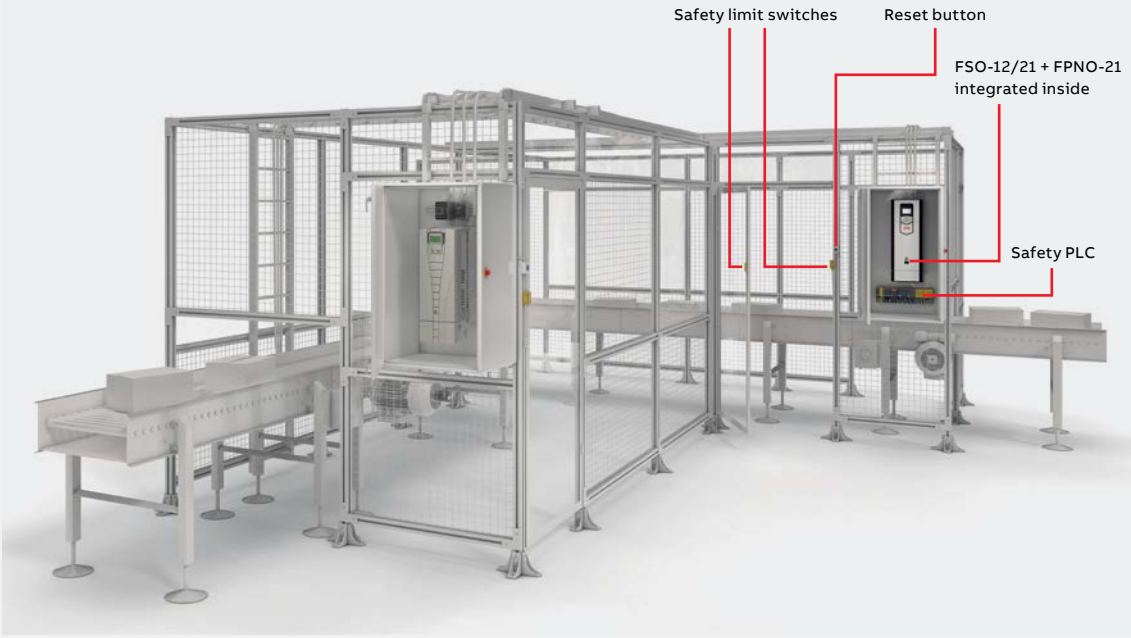
In industrial applications safe stopping is not always the preferred or allowed reaction. Monitoring motor safe speed using integrated drive-based functional safety together with a safety PLC enables synchronous reactions to emergency situations as well as activating SLS instead of STO.

In integrated drive-based functional safety the PLC controls the overall safety system by activating or deactivating drive-based safety functions. The drives perform local safety monitoring by controlling motor speed, torque and stopping. Additionally, the drive can be used as a safety sensor. In this case the drive generates safe data (e.g., motor speed) and sends it over the safety fieldbus to a safety PLC that can utilize the data for safe monitoring.

Drive groupings according to the safety zones in the application is also possible. For example, an overspeed of any drive on a conveyor line may require all drives to stop, which is possible by activating the STO in all drives. Similarly, an emergency stop command can typically stop all drives, whereas a prevention of unexpected start up may be divided into smaller groups.

Where safe stopping is not the preferred action, integrated drive-based functional safety with a safety PLC provides alternative solutions.

Example 4



Safety system with traditional and integrated drive-based safety functions, controlled by a safety PLC.

Ensuring the safety of your machinery **and processes with ABB solutions**

ABB offers various safety devices and tools for designing safer machines and processes that utilize drives. Our drive-based functional safety offering includes drives that come with integrated safety features and extended safety functionality all in one package. Safe connection between drive and PLC is established using safety communication protocols PROFIsafe or CIP Safety connectivity. ABB's functional safety design tool (FSDT-01) speeds up the design process when building safety solutions.

ABB all-compatible drives have Safe Torque Off (STO) as standard. A wide range of functional safety modules are available as options. All drive-based safety functions are pre-certified and mostly conform to the highest safety levels SIL3 and Ple.

More information can be found through this link.
ABB drives functional safety option modules FSO-12 and FSO-21 functional safety modules provide an easy way to extend safety functions in the ACS880 and DCS880 series drives. These plug-in modules are installed and cabled inside the drive, enabling different safety functions and diagnostics in one compact and reliable module.

FSO-12 and FSO-21 offer several open loop control (encoder less) safety functions including:

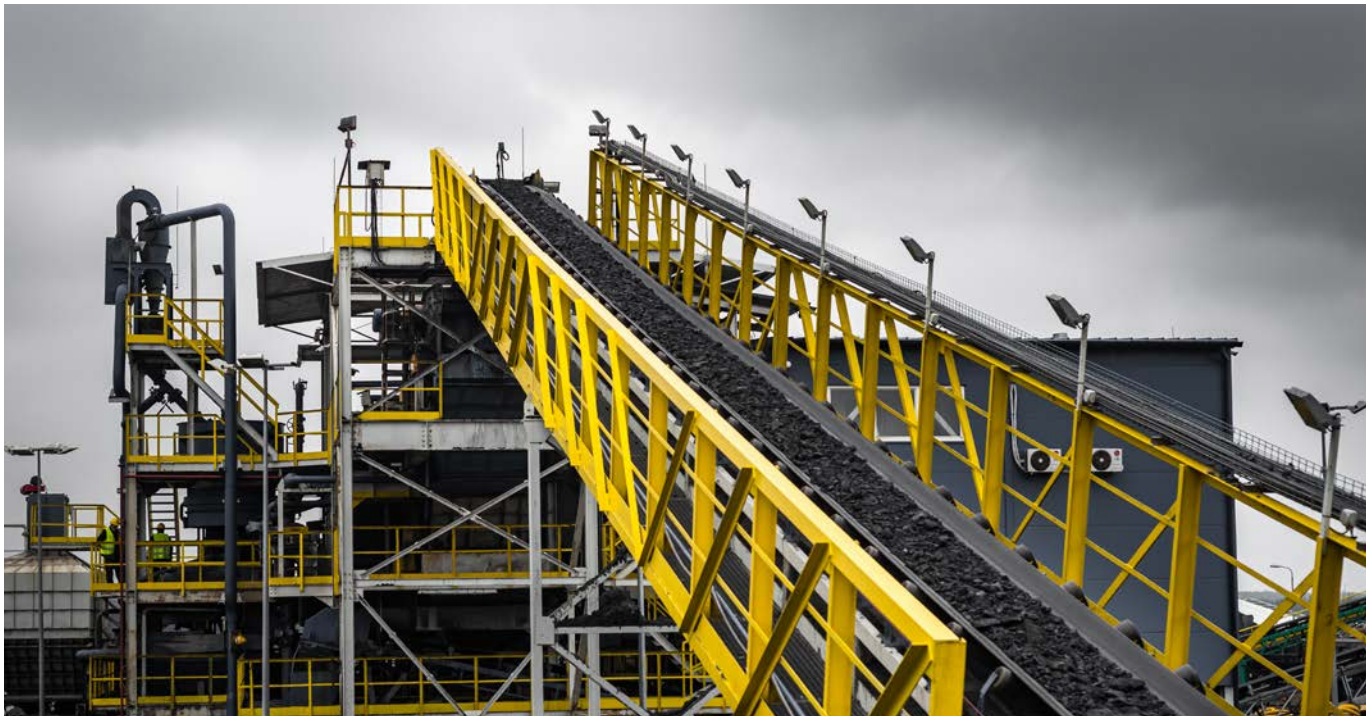
- Safe Stop 1 (SS1, as SS1-r and SS1-t implementations)
- Safe Stop Emergency (SSE)
- Safe Brake Control (SBC)
- Safely Limited Speed (SLS)
- Safe Maximum Speed (SMS)
- Prevention of Unexpected Start-up (POUS).
- The highest safety levels: SIL3/PLe (Safety Integrity Level / Performance level).

FSO-21 offers additional functions with closed loop control (with safety HTL encoder feedback) functions:

- Safe Speed Monitoring (SSM)
- Safe Direction (SDI), requires the pulse encoder interface module (FSE-31)
- The highest safety levels: SIL3/PLe Safety Integrity Level/Performance level

Both FSO-12 and FSO-21 are capable of monitoring safe speed in encoder less mode (in open loop). This is made possible by having motor basic data and drive internal measurement capabilities The FSO-21 also supports closed loop safe speed monitoring together with the pulse encoder (HTL) interface module (FSE-31).

FSO offers safety speed (e.g. SLS) functionality without an external speed measurement system, thereby greatly reducing system complexity and cost.



The CIP Safety™ functions module FSCS-21 and PROFIsafe safety functions module FSPS-21 are easy to use, cost-efficient and compact modules that enable safe machine control and seamless safety communications between the drive and the programmable logic controller (PLC) in a wide range of machines from conveyors to grinders. This is enabled through the PROFIsafe over the PROFINET IO communication protocol (FSPS -21) and CIP Safety over EtherNet/IP protocol (FSCS-21)

Modules are easy to install and configure and are suitable for ensuring the safety of equipment that reduces the risk of accidents for people working with a variety of applications.

- Compatible drives: ACS380, ACS580, ACS880
- Safety functions: Safe Torque Off (STO), Safe Stop 1 (SS1)
- The highest safety levels: SIL3/PLe (Safety Integrity Level / Performance level)

AC500-S safety PLC is certified for SIL3 and PL e safety applications, supporting both PROFIsafe F-Host and F-Device functions over PROFINET. The PLC is well-suited for simple or complex functional safety applications such as material handling, robotics, and wind turbines. Optional XC modules provide protection in harsh environments where, for example, harbor cranes and mobile platforms operate. More information can be found here.

ABB Functional safety design tool
The functional safety design tool (FSDT-01) helps you design and calculate safety integrity levels (SIL)/ performance levels (PL) for safety functions and generate safety calculation reports. Running in Windows, it is a support tool for performing functional safety modeling, design, calculations, and verifications for machine functional safety.

The tool simplifies the process of safety function design, verification, and documentation generation. More information can be found here.

Single ethernet cable for safety and control between the drive and the PLC.

Drive-based functional safety functions **supported by ABB**

Safe Torque Off (STO)
STO is the basic requirement for drive-based functional safety since it brings a drive safely to a no-torque state. STO is typically used for a prevention of an unexpected startup of machinery or for an emergency stop, fulfilling uncontrolled stop category 0 (EN 60204-1). When STO is used as an emergency stop function, it also ensures that resetting the emergency stop does not initiate a restart.

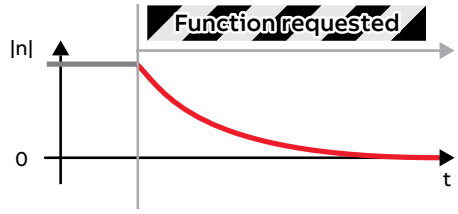


Figure STO: Upon activation STO immediately switches off the drive output thus removing torque to the motor. The Motor then coasts to a stop if there are no other forces accelerating it.

It is important to note that the STO function does not disconnect the voltage of the main and auxiliary circuits from the drive. Therefore, maintenance work on electrical parts of the drive or the motor can only be carried out after isolating the drive from all voltage sources.

Safe Stop 1 (SS1-t – Time monitoring)
This function stops the motor safely using a controlled ramp stop and then activates the STO function. SS1-t is typically used in applications like rolling mills where motion must be stopped in a controlled manner before switching to a no-torque state. In addition to a safe process stop, SS1 can also be used to implement an emergency stop, fulfilling controlled stop category 1 (EN 60204-1).

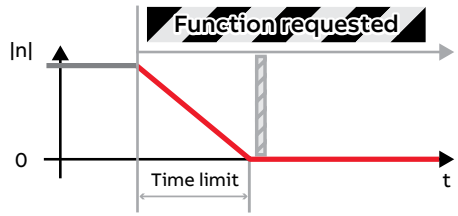


Figure SS1-t: When activated, SS1-t will ramp motor speed to a standstill and then activate the STO function.

Safe Stop 1 (SS1-r – Ramp monitoring)
This function stops the motor safely using a controlled ramp & safely monitors the ramping and then activates the STO function. Compared to SS1-t, SS1-r is used in applications where fast reaction to incorrect ramping is required.

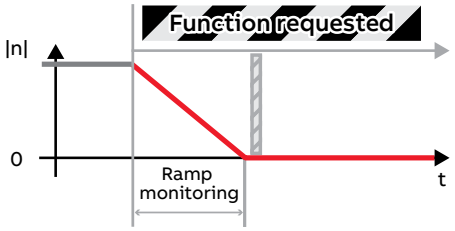


Figure SS1-r: When activated, SS1-r will ramp and monitor motor deceleration to a standstill and then activate the STO function.

Safe Stop Emergency (SSE)
This safety function is specifically designed for implementing emergency machine stops. SSE can be configured to execute either STO or SS1 depending on which emergency stop is suitable for the system. For examples of this functionality see STO and SS1.

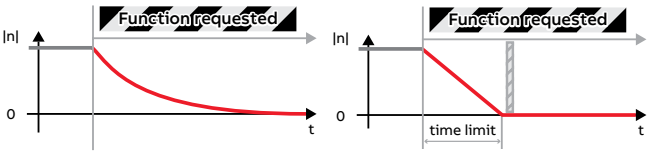
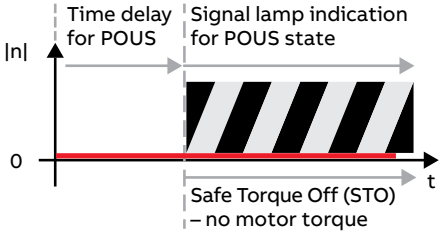


Figure SSE: Safe Stop Emergency can be configured to, upon request, either activate STO instantly, or first initiate motor deceleration and then, once the motor has stopped, activate the STO.

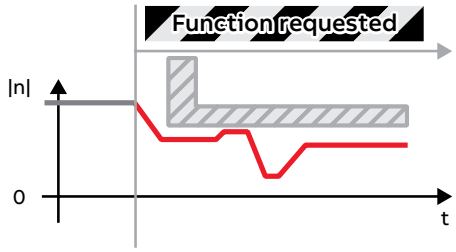
A full range of safety functions ensures immediate response to safety-critical events.

Prevention of Unexpected Start-Up (POUS)
The POUS function prevents the machine from starting unexpectedly. The POUS function activates the Safe torque off (STO) function in the drive. Specially designed for maintenance and repair procedures.



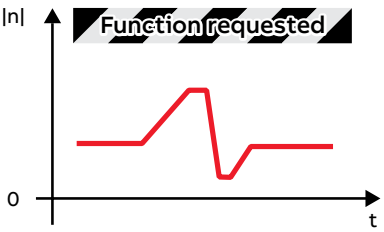
—
Figure Pous: Ensures that the machine remains stopped when people are in the danger area.

Safely-Limited Speed (SLS)
This function prevents motors from exceeding a defined safe speed limit. The SLS safety function can be used in applications such as decanters, mixers, conveyors or paper machines where excess speed can be hazardous during, for example, maintenance or cleaning operations. ABB drives can offer the SLS functionality without an external speed measurement system (such as encoder speed feedback), which greatly reduces system complexity and cost. An external encoder is required in applications with external accelerative loads, for example, hanging loads.



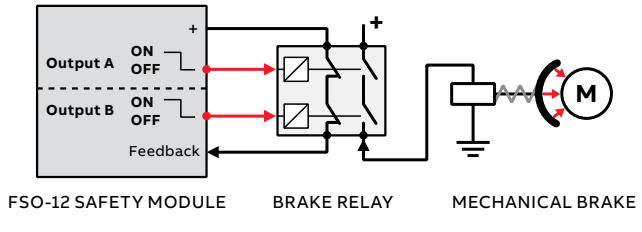
—
Figure SLS: Upon activation, SLS will monitor motor speed. If a defined level is exceeded, the drive will stop the motor using the SSE function.

Safe Maximum Speed (SMS)
This function is a variant of the SLS-safety function. It provides continuous protection against a motor exceeding a defined maximum speed limit. Typically, SMS is used to protect machinery by limiting the maximum speed which the machine can tolerate. ABB drives can offer SLS functionality without an external speed measurement system (such as encoder speed feedback), which greatly reduces system complexity and cost. An external encoder is required in applications with external accelerative loads, for example. hanging loads.

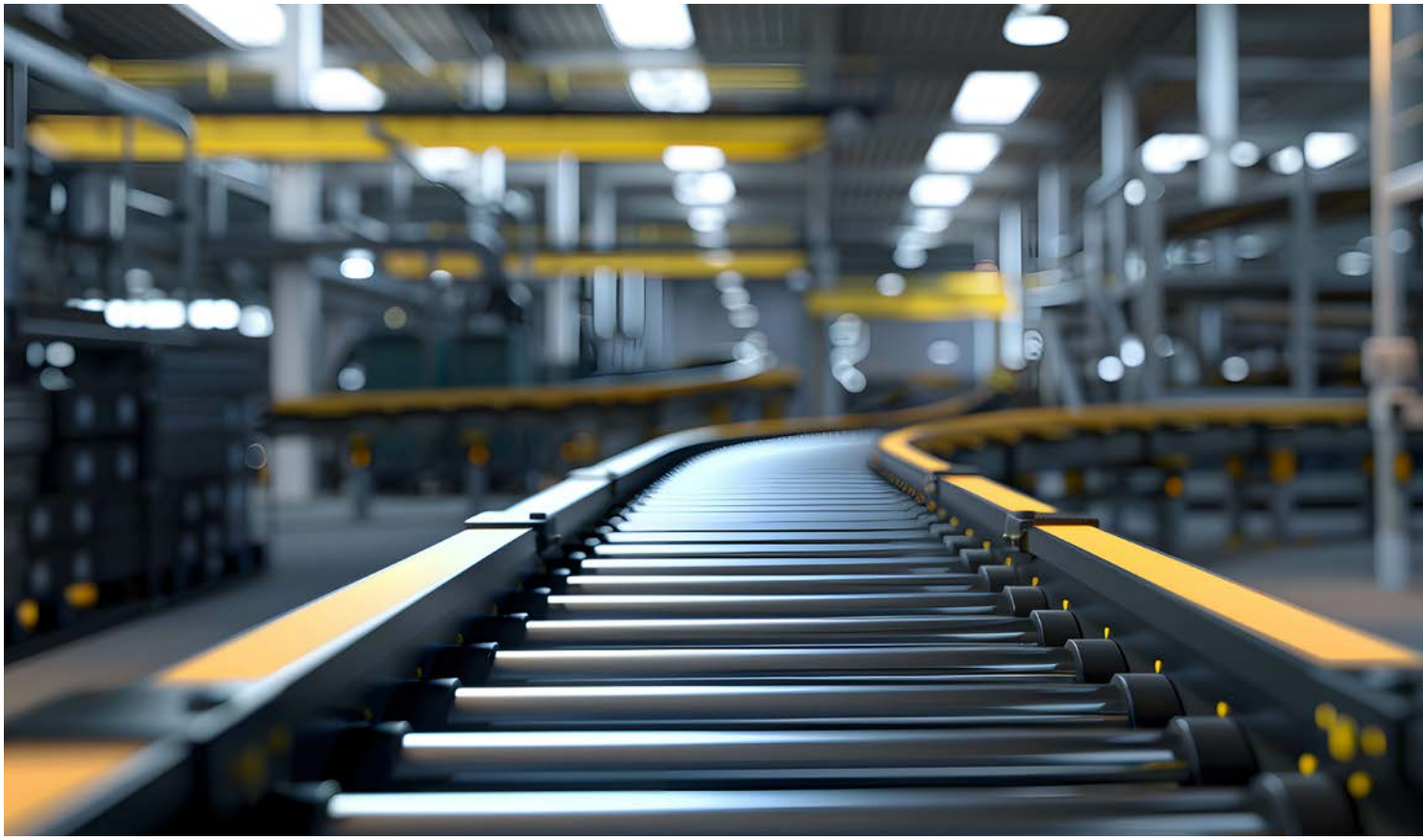


—
Figure SMS: When used, SMS is always active and ensures that the maximum allowed speed is not exceeded. If the level is exceeded, the drive will stop the motor using the SSE function.

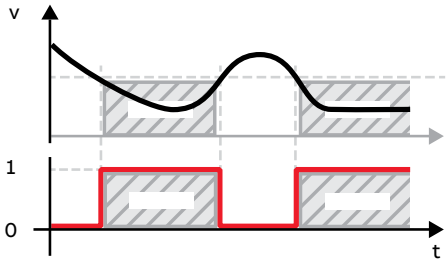
Safe Brake Control (SBC)
This function provides a safe output signal to control a mechanical holding brake. Drills, cranes, winches, hoists, vertical conveyors, and elevators are typical applications needing Safe Brake Control. A typical use for SBC is when a drive is switched off with the STO function and there is an active load affecting the motor, such as a hanging load on a crane or winder. The function allows operators to work near hanging loads and temporarily below the load if necessary. Please refer to sector standards for requirements regarding hanging loads.



—
Figure SBC: SBC provides a safe control signal to operate the mechanical brake.

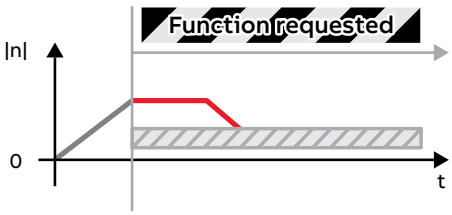


Safe Speed Monitor (SSM)
This function provides a safe output signal, for example to a safety PLC. A typical use for SSM is when there is a need to monitor motor speed, but the reaction is done from a safety PLC to, for example, synchronize the stopping of multiple drives. SSM output can also be used in signaling lamps to indicate if the motor is running or not.



—
Figure SSM: Upon activation, the drive will safely indicate if speed is above or below the defined speed limit.

Safe Direction (SDI)
This position function ensures that a motor will not turn in an unwanted direction. Typical use cases with are found with escalators or conveyors as well as operation near end limit switches in crane applications.



—
Figure SDI: When active, the SDI monitors that the motor does not rotate in an unwanted direction. If movement is detected in an unwanted direction, the motor will be stopped using SSE function.

Conclusion

The industrial environment is full of moving machine parts which can cause hazardous situations and lead to severe and often permanent injuries. The role of functional safety is to protect people, property, and ecosystems from often preventable accidents. It is therefore the ultimate responsibility of device suppliers, machine builders and system integrators to ensure that the products they deliver are safe.

Drives have been used for decades in many industrial applications. Where safety in automation systems once required many external add-on devices, the ever-increasing levels of automation employed in industry combined with the electro-technical capability of many modern drives and safety PLCs mean drive systems now contribute greatly to the overall safety of a system.

Today, new and improved safety solutions and standards enable safety to become an integrated part of drive functionality.

—

The ever-increasing level of automation in industry means drive systems are vital to the overall safety of a system.

Useful links

- Functional safety webpage
- Technical guide No. 10: Functional Safety
- FSO-12/21 flyer
- FSPS-21 flyer
- FSCS-21 flyer

Glossary

Drive-based functional safety
Active machine safety functionality designed to work with drives.

Drive-based safety functions
Safety functions, stated in the principles of safety design (machinery directive) added on the first level safety functions (STO) to perform a certain safety functions with the drive, towards the machine. Safety function include: STO, SLS, SS1, SMS, SBC, SSE, SMS, SDI and POUS.

Functional safety
Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

Harmonized standard
A European standard that has been prepared under the mandate of the European Commission or the EFTA Secretariat with the purpose of supporting the essential requirements of a directive and is effectively mandatory under the EU law.

Hazard
Potential source of harm.

PL, Performance Level
Levels (a, b, c, d, e) for specifying the capability of a safety system to perform a safety function under foreseeable conditions.

Risk
A combination of how possible it is for harm to happen and how severe the harm would be.

Safety function
A function designed for adding safety to a machine whose failure can result in an immediate increase in risk(s).

SIL, Safety Integrity Level
Levels (1, 2, 3, 4) for specifying the capability of an electrical safety system to perform a safety function under foreseeable conditions. Only levels 1 to 3 are used in machines.

—

For more information, please contact
your local ABB representative or visit

new.abb.com/drives/functional-safety
new.abb.com/drives

3AUA0000181817 REV D EN 6.6.2024