WHITE PAPER

Drive-based functional safety

How variable speed drives are playing an increasingly important role in machine safety

Melbourne
Unit 12/2 Sibthorpe St
Braeside Vic 3195
Ph: 03) 9587 1233
sales@remtron.com.au

Gippsland
1/29 - 31 Eastern Rd
Traralgon Vic 3844
Ph: 03) 5192 5000
gippslansales@remtron.com.au

Albury
444 Wilson Street
Albury NSW 2640
Ph: 02) 6023 1819
alburysales@remtron.com.au.

Tasmania
6 Ferguson Drive
Devonport TAS 7310
Ph: 03) 6422 5000
remtrontasmania@remtron.com.au

Adelaide
22 Marlow Road
Keswick SA 5035
Ph: 08) 8351 2920
sasales@remtron.com.au

Table of contents

Part 1. Functional safety: Safer machines with drive-based functional safety

Introduction
Today, new drive technology is making the previously complicated job of implementing a machine safety system much easier. Recent technical advances make safer operation less complex, while at the same time offering exciting new potential for productivity and uptime gains.

This white paper will look at the way in which new developments in drive-based functional safety contribute to greater overall protection of people, machines and ecosystems. The aim is to help make machines safe, and especially drive-based functional safety, easier for machine safety professionals.

This white paper is divided into three sections. The first covers the new possibilities that integrated drive based functional safety brings to machines and applications. The second part discusses the regulatory requirements (such as the EU Machinery Directive, harmonized standards and national laws) that must be fulfilled when implementing functional machine safety. And the third presents examples of ABB's drive-based functional safety offering and solutions in connection with other safety devices.

Managing machine risks
In any industrial process it is critically important that when something goes wrong the machinery is quickly and safely brought to a safe state, which usually means stopped. Once stopped it must not start unexpectedly. Depending on the application and its work cycles, machines may also need to operate at reduced speed during specific times. Any malfunction in machine control can result in hazardous situations leading to serious injury, or even death, with disastrous effects for the company, its people and its image.

Ultimately, machine builders and system integrators have the responsibility for ensuring that any product or machine they supply is safe. It must be designed by following safety principles and must comply with relevant directives, standards and national laws. The machine's end user has responsibility extending through the entire lifecycle of an industrial system. It is thus vitally important that safety planning is included from the very start of any machine design process. This way safety becomes a natural, functional part of the machinery and not an afterthought.

Drive-based functional safety (which we define as "active machine safety functionality designed to work with drives"), simplifies the task because drive safety functions are certified and integrated into the drive system.

Safety is important in industrial applications involving motors, drives and programmable logic controllers (PLCs). Machine safety is achieved by identifying and reducing risks to an acceptable level. Risk reduction is done by an inherently safe design and by applying risk-reducing protection measures, such as safety functions.

When done correctly, these measures can be flexible, reliable and easy-to-use. They also bring solid economic benefits such as increased productivity and uptime, without generating additional risks.

Towards integrated drive-based functional safety
The job of implementing a machine safety system is today easier thanks to three main factors.

First, modern electronics enable safety functions to be directly integrated into a drive's safety logic, so functional safety is a standard feature of the drive.

Second, legislation has kept pace with these advancements, with new standards that define the requirements and provides guidelines for implementing machinery safety.

Third, engineering companies such as ABB have developed a wide range of safety devices and solutions that are easy to integrate in industrial applications for improved safety, uptime and functionality.

These three factors have enabled safety solutions that can be more effective in preventing accidents, less costly to implement, easier to adapt and more reliable than previous hardwired electromechanical systems.

The result: Electromechanical safety systems can now be replaced with electronic safety functions. Built directly into the drive's safety logic, the safety functions work seamlessly, side-by-side with the drive's normal control functions.

Drive-based functional safety solutions in industrial systems

Drives, simply put, control movements such as motor speed and torque in industrial applications like conveyors and cranes. As levels, complexity and modularity of industrial automation increase, drive-based functional safety is fast becoming an important part of overall safety design for industrial processes.

When sensing a hazardous situation a drive-based functional safety system can react in several ways. It might, for example, initiate an emergency stop based on user input. Or if it detects an out of control situation such as system overspeed, it can stop a process in a controlled and orderly way.

In larger systems with several drives, control of the overall safety system can be done using a safety PLC, which activates drive-based safety functions when required in the whole system.

Typical drive-based functional safety functions

Safe torque off (STO) is the required basic foundation for drive-based functional safety, since it brings a drive safely to a no-torque state. STO is typically used for prevention of an unexpected startup (EN 1037/ISO 14118) of machinery or for an emergency stop, fulfilling stop category 0 (EN/IEC 60204-1).

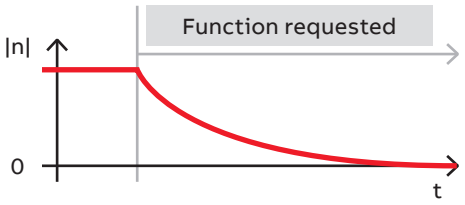


Figure 1. Upon activation STO immediately switches off the drive output to the motor. Motor speed then coasts to a stop.

Safe stop 1 (SS1) stops the motor safely, using a controlled ramp stop and then activates the STO function. SS1 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 stop category 1 (EN 60204-1).

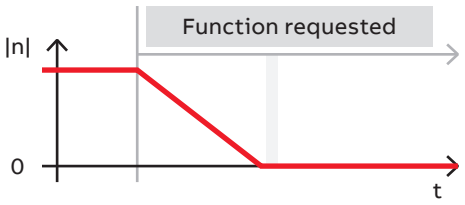
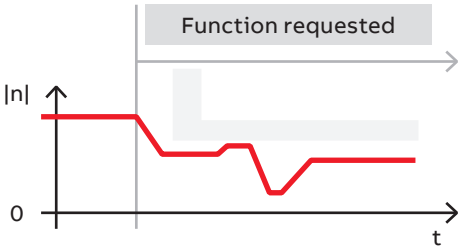


Figure 2. When activated, SS1 will ramp motor speed down to a standstill and then activate the STO function.

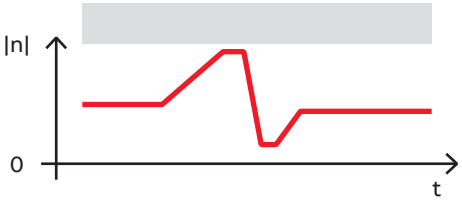
Safe stop emergency (SSE) is a safety function specifically designed for emergency stops. SSE can be configured to execute either STO or SS1 depending on which emergency stop is suitable for the system. For examples of this functionality see Fig. 1 or 2.

Safely-limited speed (SLS) prevents motors from exceeding a defined 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 ie. maintenance or cleaning operations.



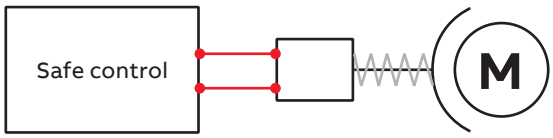
—
Figure 3. Upon activation, SLS will monitor that motor speed does not exceed a defined level. If it is exceeded, SLS will activate STO or SSE to stop the drive.

Safe maximum speed (SMS) is a variant of the SLS-safety function. It provides continuous protection against a motor exceeding a defined maximum speed limit.



—
Figure 4. When SMS is used, it is always active and ensures that the set speed limit is not exceeded (ie. maximum allowed speed).

Safe brake control (SBC) provides a safe output signal to control a mechanical holding brake. Drills, cranes, winches, hoists, vertical conveyors and elevators that need external brake solutions require this type of safety function. Typical use for SBC is when a drive is switched off with STO function and there is an active load affecting the motor (eg, a hanging load on a crane/winder).



—
Figure 5. SBC provides a safe control signal to operate the mechanical brake.

Part 2. Laws, Standards and a Roadmap to drive-based functional safety

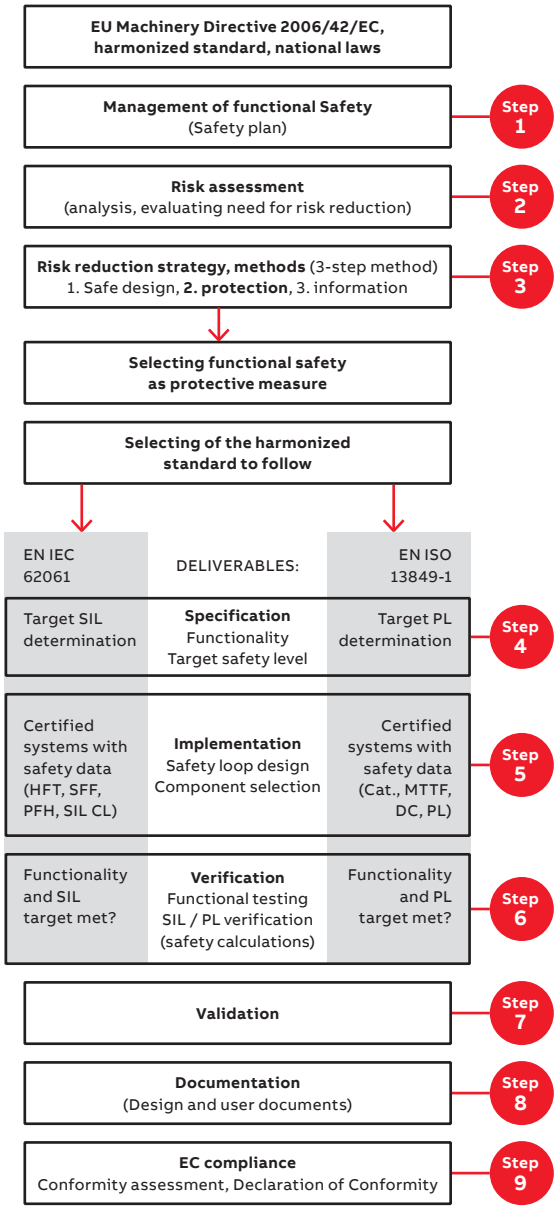
EU Machinery Directive, relevant harmonized standards and national laws
Under the directives, national and regional laws, end users, machine builders and system integrators are generally responsible for safety of machines and systems. The text in this section will mainly refer to EU (European Union) legislation, which however is based on IEC/ISO standards that are globally applicable.

All machinery supplied in the European Union must meet the essential health and safety requirements (EHSR) of the EU Machinery Directive 2006/42/EC. To fulfill these requirements it is sensible for the machine builder to follow a roadmap of set safety design steps. This helps both to meet legal requirements for the CE compliance marking and also to generate the necessary technical documentation.

Functional safety regulations in the EU consist of two parts; the EU Machinery Directive and the harmonized safety standards. The harmonized standards provide the technical means and procedures to fulfill the Machinery Directive requirements.

European Standardization organizations CEN, CENELEC and ETSI have harmonized certain international IEC/ISO standards as means to fulfill the legal requirements of the Machinery Directive. Product standard EN/IEC 61800-5-2 specifically focuses on drive-based functional safety and defines the standardized safety functions such as safe torque off, STO; safe stop 1, SS1; and safely-limited speed, SLS.

The same international IEC/ISO standards that are harmonized in Europe, are widely applied in outside European Union as well. But it should be noted that different market areas also have their own local safety legislation, for example in US, Brazil, and South Korea.



—
Figure 6. The roadmap to functional safety

Harmonized standards:
Relevant for safety design including drives
The harmonized safety standards are a collection of ISO, IEC and European standards listed under the EU Machinery Directive. A harmonized standard, identified by the prefix EN, is an agreed norm in the EU member states and basis for national laws. Outside the EU the same standards, in IEC/ ISO versions, provide a global requirement framework that machine design should comply with.

In the following chapter we list the most commonly-used harmonized standards, which are relevant for safety experts at machine builders and system designers.

Roadmap for achieving conformity
The Machinery Directive requires machine manufacturers (or their representatives) to perform and document a risk assessment. The machine design must then take these results into account, with any risks reduced to an acceptable level. This is done either via risk-reducing machine design changes or by applying appropriate safeguarding techniques such as drive-based functional safety.

After the risks have been reduced to acceptable level, measures to control any residual risks have to be documented in user documentation (ie. warnings, instructions etc.).

A common way to design a safe machine and ensure conformity is to follow suitable harmonized standards when implementing the safety system. By fulfilling requirements of harmonized standards, it is presumed that the machine conforms to EHSR of the Machinery Directive.

Certified safety devices greatly simplify the design and validation process of a safety system. This is a big advantage since certified devices already have the necessary safety capability to achieve a given safety level, and the necessary supporting safety data for safety integrity level (SIL) / performance level (PL) verification calculations.

Usually a third party certification is not necessary for machines. Manufacturers can ‘self-declare’ conformity to the Directive based on proper design and documentation, a conformity assessment and achievement of CE marking (see Figure 6, roadmap to functional safety including the main steps).

Harmonized standards provide unified guidelines for hazard and risk assessment, and also outline the approach for reducing risks to acceptable level (EN ISO 12100). Designing machine safety functionality is most effectively achieved by following the harmonized standards for the specific machine types, if they exist, and/or the harmonized generic machinery application standards EN/IEC 62061 or EN ISO 13849-1.

More information on harmonized standards
For those wanting more detailed information regarding the roadmap to functional safety via harmonized standards, ABB Drives technical guide no. 10 “Functional Safety” is an excellent source.

Part 3. ABB's drive-based functional safety solutions

Drive-based functional safety
Functional safety can be easily achieved with safety devices that are, themselves, already certified to the most relevant functional safety standards. ABB drives include many certified safety functions either as standard, or are offered as options. A good example is the TÜV-certified safety functions module (the FSO-12 or FSO-21 variant) which is compatible with ABB's ACS880 drive series.

Safe torque off (STO) as the foundation
ABB has put great emphasis on building safety functionality into its drives. We offer cost-efficient safety solutions with our drives and PLCs, as well as a full range of safety relays and contactors, emergency stop switches and other safety devices. Depending on the needed machinery safety, our solutions can range from one drive to an entire system of drives.

As mentioned in part 1, Safe torque off (STO) is the foundation of drive-based functional safety. Several ABB's drives therefore have STO built-in as a standard feature, while some drive series offer it as an option.

The all-compatible ACS880 drives with STO (as standard) are the best-equipped, most-modern example of integrated drive-based functional safety. They provide highest machinery safety capability, complying with SIL 3 and PL e safety level.

STO can be supplemented with additional safety functions like safely-limited speed (SLS), to ensure a specific speed level in the drive, and machine, is not exceeded. Safety functions that are integrated inside the drive eliminate the use of costly external safety add-ons like contactors, safety relays, etc. Using integrated drive-based functional safety results in cleaner installation and lower costs, with fewer components needed to reach the required SIL or PL.

Three examples
In this section three different ways of implementing ABB drive-based functional safety solutions are shown, using the example of an industrial conveyor belt.

In our imaginary example we assume people are frequently interacting with a conveyor belt by placing on and picking off material from it. Based on a risk analysis made for the conveyor, it should remain safely powerless when stopped eg, for cleaning. This means that the motor must be in a non-torque state when stopped, because unexpected startup 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.

Risk reduction in our examples can be achieved by implementing three machine safety functions:
1. Prevention of unexpected startup (POUS)
2. Emergency stop
3. Safely-limited speed (SLS)

This is done by using two drive-safety functions: safe torque off (STO) and safely-limited speed (SLS). STO is used for both emergency stopping with an emergency stop device and prevention of unexpected startup, to keep the motor from starting with eg, a lockable on/off switch connected to the STO.

The machine safety system can be built using ABB safety devices for maximum control, as presented in the following examples.

First example: Traditional safety solution using a drive, safety monitoring device, safety encoder and contactors

The traditional way of building a safety system includes connecting safety limit switches, relays/ external safety monitoring devices and contactors together with the drive (see figure 7).

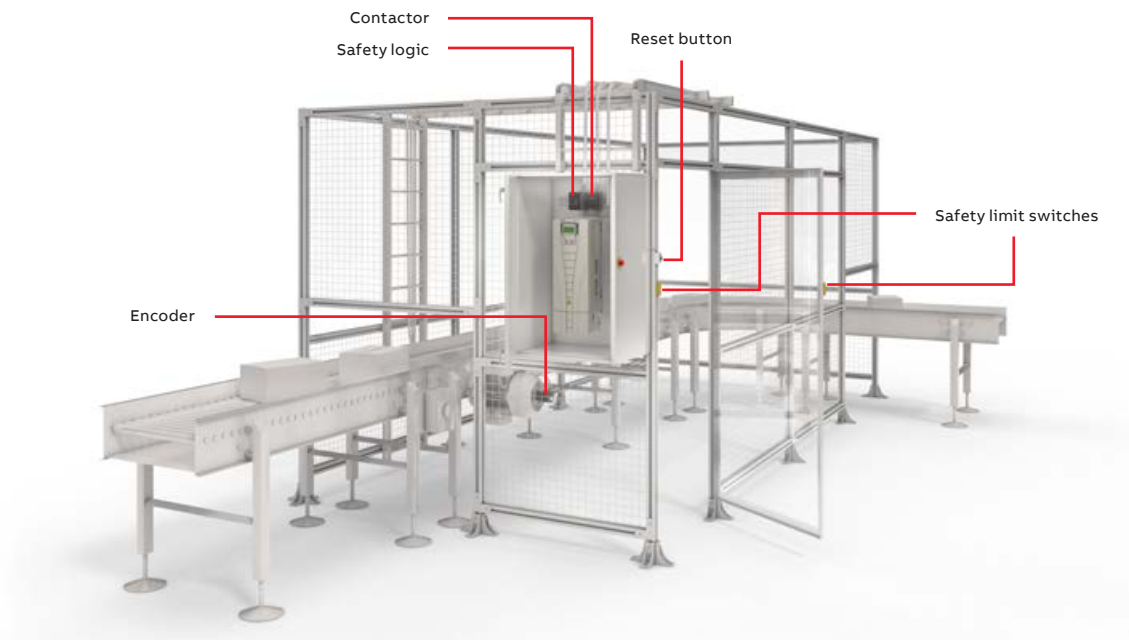
Once the protective cage door to the conveyor has been opened the safety limit switch detects the open door. This sends signals to the drive to decrease speed. At the same time the signal is sent to an external safety monitoring device (safety logic), which together with an encoder speed measurement, creates a safety function SLS, for safe speed monitoring.

People can now interact safely with the slowly moving conveyor and perform their task. After leaving the conveyor and closing the protective cage door, the safety monitor has to be reset with a button, before the conveyor is allowed to increase back to normal speed.

If, for some reason during the safe speed phase when SLS is active, there is a malfunction that causes the conveyor belt to suddenly increase speed, the safety monitor will detect the overspeed and activate the motor contactor that interrupts the drive's output to the motor, thus stopping the conveyor.

Benefits of traditional electromechanical safety solutions:

- Safety solutions can be built together with drives that do not have safety functionality integrated into them



—
Figure. 7. Safety monitors receiving and sending safety impulses to the drive. More safety devices and wiring are needed compared to integrated drive-based functional safety (see fig. 8).

Second example:
Integrated drive-based functional safety
With integrated drive-based functional safety, the safety functions are implemented into the machine via the drive. As a result, the use of externally wired discrete safety devices such as safety monitors, wiring, an encoder (see figure 8) can be eliminated.

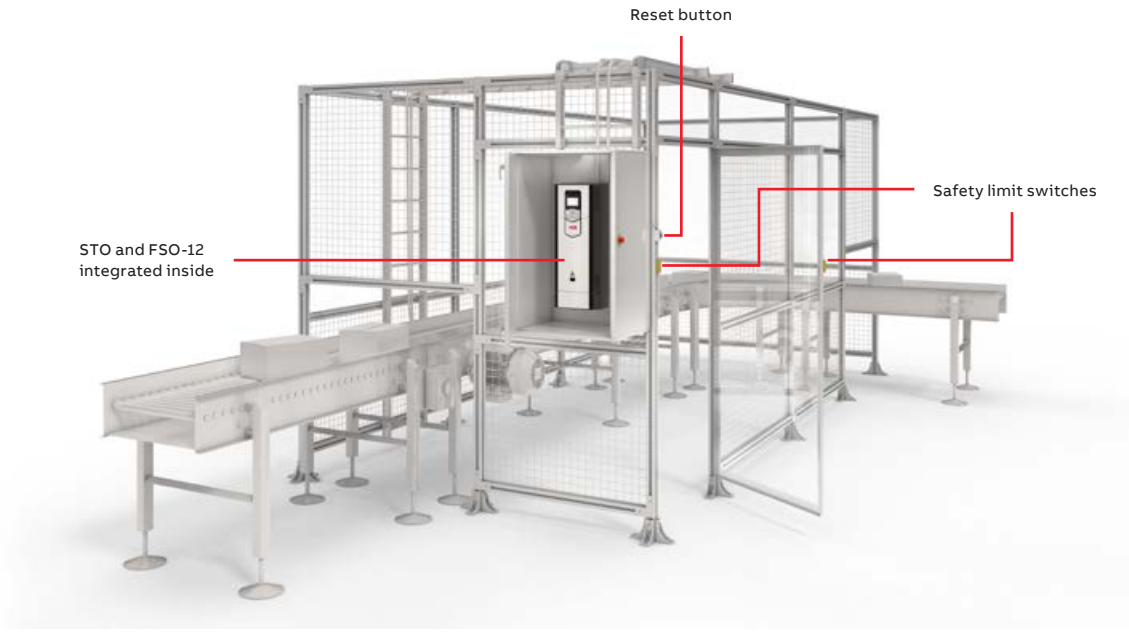
Integrated drive-based functional safety not only simplifies the overall safety design process, but with fewer parts and less wiring, the complexity of configuration and installation is also significantly reduced for a lower total cost.

Compared to the traditional safety solution, integrated drive-based functional safety includes the same functionality but it is simply built into the drive. The most basic functionality level is the STO circuit inside the drive which can safely disable the drive's power stage, thus eliminating any need for a motor contactor.

ABB's offering of drives with STO as a standard feature includes e.g. ACS880, ACS580, ACH580, ACQ580, ACS380, DCS880, ACSM1 and MicroFlex e190. The ACS800 drives have STO built-in as an optional feature.

When additional integrated safety functions are needed, ABB's optional TÜV-certified safety functions module (FSO-12 or FSO-21) is perfectly suited for the ACS880 drives. Alternatively a simpler safety solution is ABB's optional TÜV-certified safety functions fieldbus module (FSPS-21) that is easy to plug into ACS380, ACS580 and ACS880 drives.

The safety functions module (FSO-12 or FSO-21) and safety functions fieldbus module (FSPS-21) can be used in systems up to SIL 3/PL e. The Safety functions module (FSO-12 or FSO-21) offers several 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) and prevention of unexpected startup (POUS). Compared to the FSO-12 the FSO-21 offers additionally Safe direction (SDI) and Safe speed monitor (SSM). Both safety function modules are capable of monitoring safe speed in encoderless mode (in open loop). This is made possible when monitoring is based on a pre-set motor profile, speed profile and speed estimation of the safety functions module. The FSO-21 also supports closed loop safe speed monitoring together with the pulse encoder interface module (FSE-31).



—
Figure 8. Safety logic integrated into the drive for effective safety monitoring. Less safety devices and wiring needed compared to traditional safety solution (see fig. 7).

The Safety functions fieldbus module (FSPS-21) offers Safe torque off (STO), Safe stop 1 (SS1-t) and prevention of unexpected startup (POUS).

Using the safety functions module eliminates the hassle of figuring out how to hook up and wire the logic with relays and contactors, as the drives safety functions are predesigned in the module, waiting to be commissioned. In addition, it is easy to commission and configure the drive system using Drive composer pro, the common PC tool for the ACS880 drive series.

Benefits of integrated drive-based functional safety:

- No wearing parts needed to be changed or maintained
- Less wiring saves costs and time.
- Safety functionality seamlessly integrated into the drive operation.
- Using STO as the motor switch off path, instead of a contactor, is fast and saves money, space, and wear/ maintenance
- With STO there is no need to power off the drive or use an output contactor for prevention of unexpected startup, enabling faster restarts and eliminating any need for resetting a position referenced etc.
- Cost and space savings with the capability for safe speed monitoring without encoder for applications without active loads (motor slows down when the drive is shut down)
- The safety functions module is easy to install and commission (only for ACS880 drives)
- The safety functions module (FSO-12 or FSO-21) has several safety functions in one compact module
- With the safety functions modules, safety monitoring of movements is integrated to the drive. No additional logic or design is needed.

Third example: System safety monitoring solutions using drives and a safety PLC for multiple drive control

When a safety system includes several drives, a safety PLC can be used for controlling drives and machines from a common source (see figure 9). System safety monitoring can, of course, be designed using a traditional safety solution combined with a safety PLC (such ABB's AC500-S safety PLC). In this way different safety functions can be performed with the application being controlled by one common safety PLC.

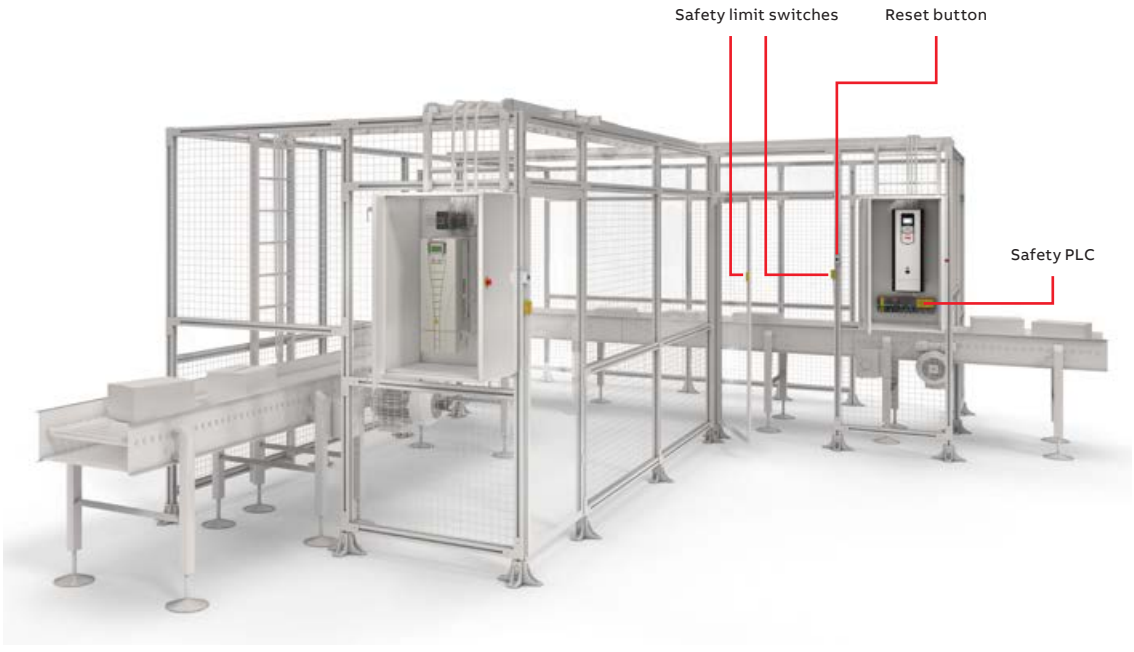


Figure 9. Safety system with traditional and integrated drivebased safety functions, controlled by a safety PLC.

A better strategy might be to build the safety monitoring solution using integrated drive-based functional safety together with a safety PLC. In this alternative the safety PLC (AC500-S) is connected to the drive with a fieldbus adapter module that provides PROFIsafe connectivity. This can be applied using the safety functions module (FSO-12 or FSO-21) together with a fieldbus adapter module (FENA-21 or FPNO-21) or the safety functions fieldbus module (FSPS-21), which doesn't require a separate fieldbus module to work.

In integrated drive-based functional safety the PLC controls the overall safety system via the safety functions modules inside ACS880 drives, thus providing different safety functions and key diagnostics information. The drives perform local safety monitoring by controlling motor speed, torque and stopping.

Grouping of the drives 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 typically can stop all drives, whereas a prevention of unexpected start-up grouping may be divided into smaller groups.

Benefits of drive-based functional safety with safety PLC:

- Reduced wiring between the PLC (such as AC500-S) and drive(s) when a fieldbus adapter module (FENA-21 or FPNO-21) is used
- Safety functions module (FSO-12 or FSO-21) in ACS880 drives supports the safety PLC with diagnostics and safety information (ie. safe motor speed information)
- Safety function fieldbus module (FSPS-21) reduces the need for components to ensure PROFIsafe over PROFINET connectivity
- Single supplier for safety devices simplifies the ordering process and brings cost efficiency
- Common support for reducing machine downtime
- Possibility to group drives according to the need of the specific functions

Functional safety design tool, FSDT-01

ABB's functional safety design tool FSDT-01 helps the designer create safety function documentation to support the safety design of their machine. The tool is easy-to-use and guides the user to select the right devices, such as drives, PLC's and other safety devices, from pre-made libraries. With these it is then verified that the required SIL/PL for the safety function is achieved. The necessary safety functionality and SIL/PL is defined based on the risk assessment performed by the machine designer.

Summary

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.

Safety for machines is achieved by complying with relevant safety directives and standards. In the EU, the EHSR which machine builders must comply with are defined in the EU Machinery Directive 2006/42/EC and the harmonized standards under this directive.

In other market areas, there is their own local safety legislation (for example US, Brazil & South Korea). In the market areas, other than EU, it is necessary to check the local safety legislation and use global IEC and ISO standards, which provide the necessary safety requirements and guidance.

For machine builders outside of EU the IEC/ISO versions of the EU's harmonized standards provide the necessary requirements and guidance. Different market areas also have their own local safety legislation, for example in US, Brazil, and South Korea.

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. Drive-based functional safety means providing drive-based motion control that protects people, property and ecosystems.

Get in touch to learn more

ABB drives offer many features that can help the safety designers achieve the required level of safety in a cost effective way.

Drive-based functional safety offers a vast world of possibilities to machine builders, designers and safety professionals.

To learn more go to **abb.com/safety**

Disclaimer

This document is an informative guide intended to assist the users, specifiers and manufacturers of machinery in achieving a better understanding of the requirements of the EU Machinery Directive, and the measures required to achieve conformity with the directive and the harmonized standards under it.

This document is not intended to be used verbatim, but rather as an informative aid only.

The information and examples in this guide are for general use only and do not offer the necessary details for implementing a safety system.

In no event shall ABB Oy Drives be liable for any loss or damage, whether direct or indirect resulting from or related to the use of this document or information found in it.

Reference

1. ABB Technical guide No. 10 – Functional safety

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.

—

Contact

Joonas T. Saarela
Technical Product Manager - Functional Safety
joonas.t.saarela@fi.abb.com

Ilpo Kangas
Product Compliance Manager
ilpo.kangas@fi.abb.com

Mikko Ristolainen
Functional Safety Manager
mikko.ristolainen@fi.abb.com

3AUA0000181817 REV C EN 8.12.2017 *20550