Drive-based functional safety

How low voltage AC drives are playing an increasingly important role in machine safety

基于变频器的功能性安全

低压交流变频器如何在确保机器安全方面发挥日益重要的作用

3ABD00039028
生效日期：2015-01-01
版　　本：A

用电力与效率
创造美好世界™

White paper

Drive-based functional safety

Table of Contents

White paper

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

1.1 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 machine safety, 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 Machinery Directive, harmonized standards and national laws) that must be fulfilled when implementing functional machine safety. And the third presents examples of ABB's low voltage AC drive-based functional safety offering and solutions in connection with other safety devices.

1.2 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.

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.

1.3 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.

1.4 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.

1.5 Typical drive-based functional safety functions

Safe torque off (STO)
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) of machinery or for an emergency stop, fulfilling stop category 0 (EN 60204-1).

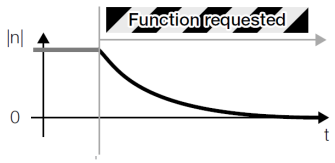

Figure 1. *Upon activation STO immediately switches off the drive output to the motor. Motor speed then coasts to a stop.*

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).

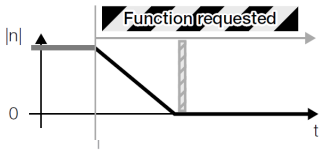

Figure 2. *When activated, SS1 will ramp motor speed down to a standstill and then activate the STO function.*

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.

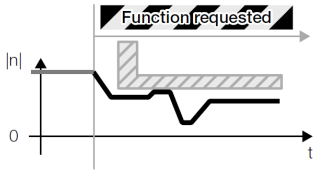

Figure 3. *Upon activation, SLS will monitor that motor speed does not exceed a defined level. If it is exceeded, SLS will activate STO or SSE to stop the drive.*

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.

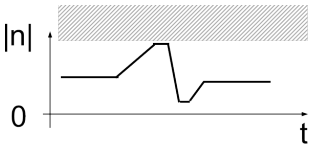

Figure 4. *When SMS is used, it is always active and ensures that the set speed limit is not exceeded (ie. maximum allowed speed).*

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).

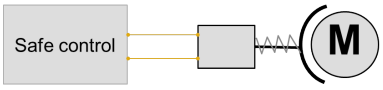

Figure 5. *SBC provides a safe control signal to operate the mechanical brake.*

White paper

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

2.1 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 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.

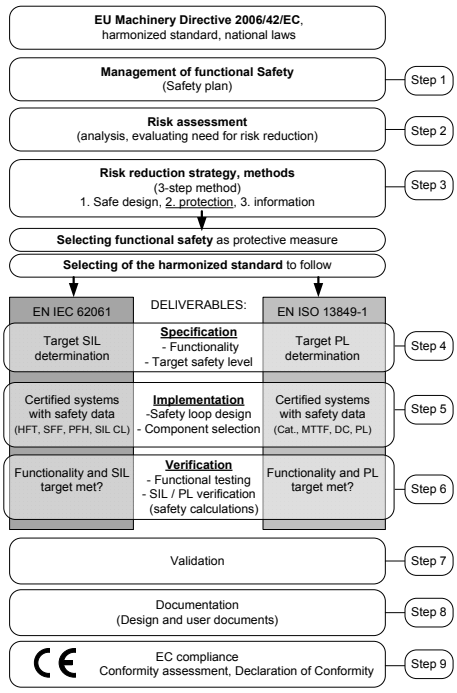

Figure 6. *The roadmap to functional safety*

2.2 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.

2.3 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.

2.4 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.

White paper

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

3.1 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 FSO-11 safety functions module which is compatible with ABB's ACS880 industrial drive series.

3.2 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 industrial 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.

3.3 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 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.

Risk reduction in our examples can be achieved by implementing three machine safety functions:
1. Prevention of unexpected start-up,
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 start-up, 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 examples below.

3.4 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).

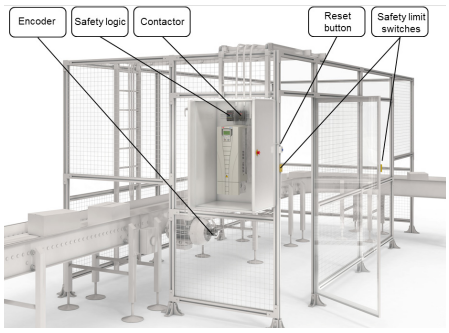

Figure. 7. *Safety monitors receiving and sending safety impulses to the drive. More safety devices and wiring are needed compared to integrated drive-based functional safety (see fig. 8)*

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.

3.5 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 9) can be eliminated.

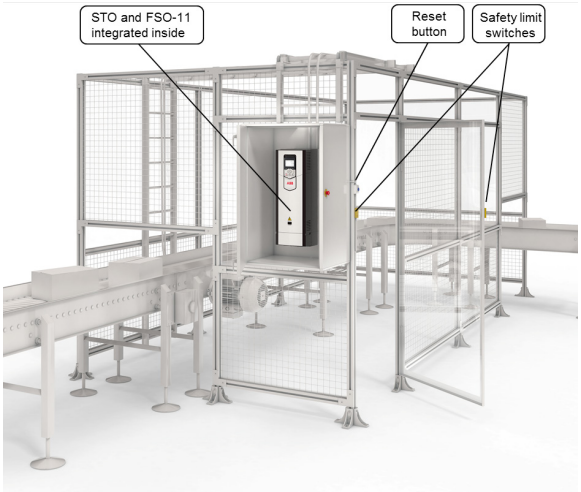

Figure 8. *Safety logic integrated into the drive for effective safety monitoring. Less safety devices and wiring needed compared to a traditional drive-based functional safety solution (see fig. 7).*

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 low voltage AC drives with STO as a standard feature includes ACS880, ACS580, ACS850, ACS355, ACQ810, ACSM1 and MicroFlex e150. 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-11 is perfectly suited for the ACS880 drives.

The FSO-11 works seamlessly with the all-compatible ACS880 drives and can be used in systems up to SIL 3/PL e. This compact safety module offers several safety functions including: Safe stop 1 (SS1), Safe stop emergency (SSE), Safe brake control (SBC), Safely-limited speed (SLS), Safe maximum speed (SMS) and prevention of unexpected start-up.

Using the FSO-11 eliminates the hassle of figuring out how to hook up and wire the logic with relays, reset signals and contactors, as the drive safety functions are pre-designed 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 start-up, 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 FSO-11 is easy to install and commission (only for ACS880 drives)
- The FSO-11 has several safety functions in one compact module
- With the FSO-11 encoderless mode all safety monitoring for movement is done inside the drive. No additional logic or design is needed.

3.6 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. 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.

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 safety fieldbus adapter module that provides PROFIsafe connectivity.

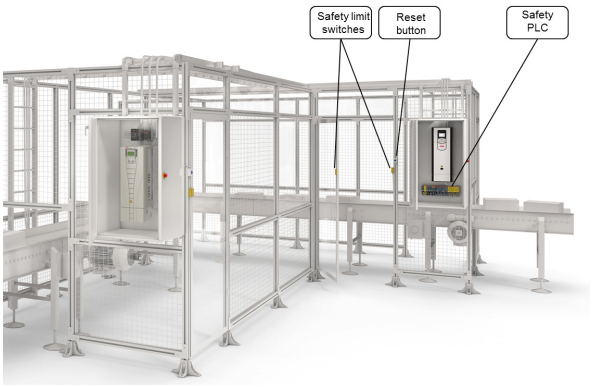

Figure 9. *Safety system with traditional and integrated drive-based safety functions, controlled by a safety PLC.*

In integrated drive-based functional safety the PLC controls the overall safety system via the FSO-11 safety functions module inside each (ACS880) drive, 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 start-up prevention 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 safety fieldbus, such as PROFIsafe (FENA-11) is used
- Safety functions module (FSO-11) in ACS880 drives supports the safety PLC with diagnostics and safety information (ie. safe motor speed information)
- 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

3.7 Easy programming 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 built-in libraries. With these it is then verified that the required SIL/PL for the machine 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 Machinery Directive 2006/42/EC and the harmonized standards under this directive. For machine builders outside of EU the IEC/ISO versions of the EU's harmonized standards provide the necessary requirements and guidance.

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.

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

Get in touch to learn more

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

To learn more go to www.abb.com/drives

Contacts

Ere Jääskeläinen
Market manager
ABB Finland
P.O. Box 184
FI-00381 Helsinki
Finland
ere.jaaskelainen@fi.abb.com

Pasi Pohjalainen
Market manager
ABB Finland
P.O. Box 184
FI-00381 Helsinki
Finland
pasi.pohjalainen@fi.abb.com

Mikko Ristolainen
Functional safety manager
ABB Finland
P.O. Box 184
FI-00381 Helsinki
Finland
Mikko.ristolainen@fi.abb.com

White paper

Disclaimer

This document is an informative guide intended to assist the users, specifiers and manufacturers of machinery and related people 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. The information and examples in this guide are for general use only and do not offer all of the necessary details for implementing a safety system.

ABB Oy Drives does not accept any liability for direct or indirect injury or damage caused by the use of information found in this document. The manufacturer of the machinery is always responsible for the safety of the product and its suitability under the applicable laws. ABB hereby disclaims all liabilities that may result from this document.

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.

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

白皮书

基于变频器的功能性安全

目录

白皮书

第1部分. 功能性安全：基于变频器的功能性安全使机器更安全

1.1 引言

现在，借助全新传动技术，先前复杂的机器安全系统实现工作变得容易多了。最新的技术进步使得安全操作不再那么复杂，同时，还展现了令人振奋的新潜力——提高生产率和延长正常运行时间。

本白皮书的着眼点是，基于变频器功能性安全方面的新进展，如何为人员、机器和生态系统提供更出色的整体保护。其目的是保证机器的安全性，特别是基于变频器的功能性安全，让机器安全方面的专业人员可以更轻松地实现机器的安全性。

本白皮书分为三个部分。第一部分涉及内容是，基于变频器的功能性安全为机器和应用带来新的可能性。第二部分讨论的是，在实现功能性机器安全时必须满足的监管要求（比如，机械指令、协调标准和国家法律）。第三部分介绍基于 ABB 低压交流变频器的功能性安全所涵括的功能举例和与其他安全装置联用的方案实例。

1.2 管理机器风险

在工业过程中，至关重要的是，在出现问题时，使机器快速安全地进入安全状态，这通常是指机器停下来。一旦停下来，就不得被意外启动。根据具体应用及其工作周期，机器可能还需要在特定时间内减速工作。机器控制方面的任何故障，都可能导致危险情况，造成严重伤害，甚至死亡，对公司、员工和公司形象造成灾难性的影响。

最终，机器制造商和系统集成商有责任确保他们供应的产品或机器是安全的。机器必须按照安全原则进行设计，并且，必须遵守相关指令、标准和国家法律。机器的最终用户有责任将其贯穿工业系统的整个生命周期。因而，至关重要的是，在机器设计流程一开始就要纳入安全规划。这样，安全成为机器固有的功能性部分，而不会是后期问题。

基于变频器的功能性安全（我们将其定义为“旨在使用变频器的主动式机器安全功能”），可简化相关工作，因为变频器安全功能通过认证，集成到了变频器系统中。

安全在涉及电机、变频器和可编程逻辑控制器（PLC）的工业应用中十分重要。通过识别风险并将风险降至一个可接受的水平，可实现机器的安全性。通过固有的安全设计和应用降低风险的保护举措，可降低风险。

如果操作得当，这些举措可以十分灵活可靠且易于使用。它们也能带来实实在在的经济效益，譬如，提高生产率和延长正常运行时间，而不会产生额外风险。

1.3 迈向基于变频器的集成式功能性安全

得益于三个主要因素，机器安全系统的实现工作现在变得更容易了。

首先，现代电子产品能将安全功能直接集成到变频器的安全逻辑中，所以，功能性安全是变频器的标准功能。

其次，立法与这些技术进步并驾齐驱，并有新标准明确需求和提供实现机器安全的准则。
第三，像 ABB 这样的工程公司已开发了各种安全装置和解决方案，它们易于集成到工业应用中，用来改善安全性、延长正常工作时间和增强功能性。

这三个因素使得安全解决方案能更有效地防止事故发生，实施成本更低，更易于适应，并且，比先前的硬连线机电系统更可靠。

结论：机电安全系统现在可被电子安全功能所取代。安全功能直接内置到变频器的安全逻辑中，能以无缝方式发挥作用，与变频器的正常控制功能并行工作。

1.4 工业系统中基于变频器的功能性安全解决方案

简单地说，变频器控制运动，譬如，传送带和起重机等工业应用中的电机转速和转矩。随着工业自动化水平的提高、复杂性的增加和模块化程度的提升，基于变频器的功能性安全正迅速成为工业过程总体安全设计的一个重要组成部分。

当感觉到危险情况时，基于变频器的功能性安全系统以多种方式作出反应。譬如，可能根据用户输入启动急停。或者，如果检测到系统超速等失控情况，能以可控的有序方式使过程停止。

在配备多台变频器的大型系统中，可利用安全 PLC 来控制整体安全系统，安全 PLC 会在整个系统中根据需要激活基于变频器的安全功能。

1.5 基于变频器的功能性安全的典型功能

安全力矩中断（STO）
STO 是实现基于变频器的功能性安全的必要基础功能，因为 STO 能安全地使变频器切换到无转矩状态。STO 通常用于防止机器的意外启动（EN 1037），或者用于紧急停车，实现 0 类急停（EN 60204-1）。

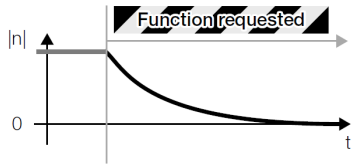

图 1. *一经激活，STO 立即关闭变频器向电机的输出。然后，电机自由停车。*

安全停车 1（SS1）利用斜坡停车功能，使电机安全地停下来，然后激活 STO 功能。SS1 通常用于轧机等应用，在这些应用中，必须以受控方式使运动停下来，然后切换到无转矩状态。此外，SS1 还可用于实施紧急停车，实现 1 类急停（EN 60204-1）。

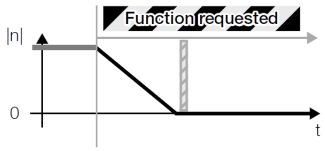

***图 2.** 激活后，SS1 将使电机斜坡停车，然后激活 STO 功能。*

紧急安全停车（SSE）是专为实现紧急停车而设计的安全功能。SSE 可配置为执行 STO 或 SS1，具体取决于哪种紧急停车方式适用于该系统。关于该功能的示例，请参阅图 1 或图 2。

安全限速控制（SLS）防止电机超过规定限速。SLS 安全功能可用于分离机、搅拌

机、传送带或造纸机等应用，在这些应用中，在维护或清洁操作期间超速是很危险的。

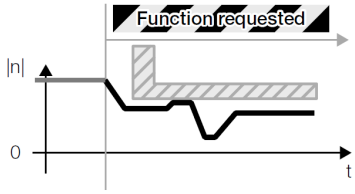

图 3. *激活后，SLS 将进行监控，确保电机转速不超过设定级别。如果超过设定级别，SLS 将激活 STO 或 SSE，使变频器停下来。*

最高安全限速（SMS）是 SLS 安全功能的一个变体。SMS 提供连续保护，防止电机超过设定的最高限速。

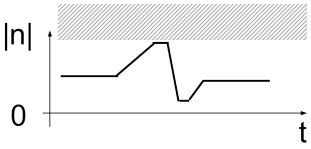

图 4. *使用 SMS 时，始终启用，并确保不超过设定的限速（即允许的最大速度）。*

安全制动控制（SBC）提供安全输出信号来控制机械抱闸。需要外部制动解决方案的钻机、起重机、绞车、提升机、垂直升降机和电梯，需要这种安全功能。SBC 的典型用途是，当变频器由 STO 功能关闭输出时，加一个有效的负载来影响电机（譬如，起重机/卷绕机上的悬停负载）。

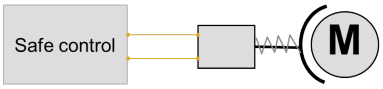

图 5. *SBC 提供安全控制信号，操控机械抱闸。*

第 2 部分. 基于变频器的功能性安全相关法律、标准和路线图

2.1 机械指令、相关的协调标准和国家法律

根据机械指令、国家和地区法律，最终用户、机械制造商和系统集成商通常负责确保机器和系统的安全。本节正文将主要涉及欧盟法律法规，不过，这些法律法规基于全球适用的 IEC/ISO 标准。

在欧盟地区提供的所有机器，必须符合欧盟机械指令 2006/42/EC 的基本健康和安全要求（EHSR）。为满足这些要求，对于机械制造商而言，明智的做法是遵照规定安全设计步骤的路线图。这不仅有助于符合 CE 合规标志的法律规定，也有助于生成必要的技术文档。

欧盟地区的功能性安全法规由两部分组成：机械指令和协调安全标准。协调标准提供符合机械指令各项规定的技术手段和流程。

欧洲标准化组织CEN、CENELEC和ETSI现已统一某些国际IEC/ISO标准，作为满足机械指令法律规定的方法。产品标准EN/IEC 61800-5-2特别注重基于变频器的功能性安全，并定义了标准化安全功能，比如：安全力矩中断（STO）；安全停车 1（SS1）以及安全限速控制（SLS）。

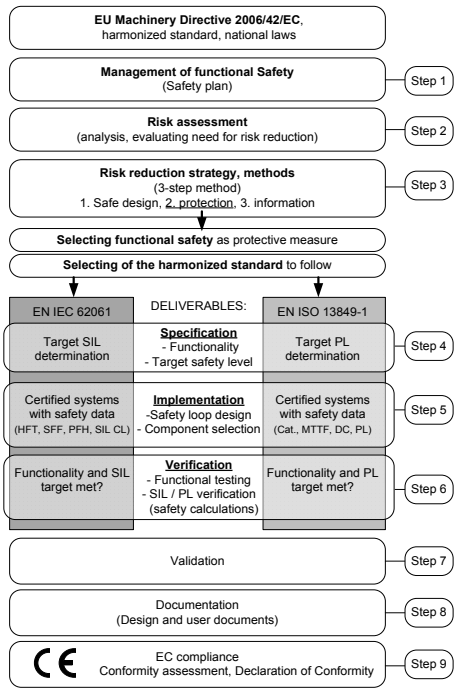

图6. *实现功能性安全的路线图*

2.2 协调标准：与包括变频器在内的安全设计相关

统一安全标准是根据欧盟机械指令列出的一些 ISO、IEC 和欧洲标准 。统一标准通过前缀 EN 确定，是欧盟各成员国达成一致的标准，是国家法律的依据。 在欧盟以外地区，IEC/ISO 版本的相同标准提供了机器设计应遵从的全球规定框架。

在下一节，我们将列出最常用的协调标准，这些标准为机械制造商和系统设计商中负责安全设计的专业人员提供参考。

2.3 合规路线图

机械指令要求机械制造商（或其代表）进行风险评估，并进行相关文档记录。然后，机器设计必须考虑这些结果，将一切风险降至可接受的水平。这可以通过降低风险的机器设计变动，或者通过应用适当的安全保障技术（如，基于变频器的功能性安全）来实现。

在将风险降至可接受的水平后，控制任何剩余风险的举措必须在用户文档（即，警告、说明等）中记录下来。

设计安全机器与确保符合规范的一种常见方式是，在实施安全系统时遵循适当的协调标准。通过满足协调标准的各项要求，推断机器符合机械指令的基本健康和安全要求。

通过认证的安全装置大大简化了安全系统的设计和验证过程。这是一个很大的优势，因为通过认证的装置现已具备达到给定安全级别的必要安全功能，以及用于安全完整性等级（SIL）/性能等级（PL）相关验证计算的必要支持安全数据。

通常，机器没必要进行第三方认证。根据适当的设计和技术资料、CE合规评估和CE标志，制造商可“自行声明”符合该指令（参阅图6，包括主要步骤在内的功能性安全路线图）。

统一标准提供进行危害和风险评估的统一准则，同时，还概述将风险降至可接受水平的方法（EN ISO 12100）。通过遵照针对特定机器类型的统一标准（如存在），和/或统一的通用机械应用标准EN/IEC 62061 或 EN ISO 13849-1，将能以最有效的方式实现机器安全功能的设计。

2.4 关于统一标准的更多信息

关于通过统一标准实现功能性安全的路线图，如果想要获得更详细的信息，可以参考 ABB 变频器技术指南 10“功能性安全”。

第 3 部分. ABB 基于变频器的功能性安全解决方案

3.1 基于变频器的功能性安全

借助本身已通过相关功能性安全标准认证的安全装置，可轻松实现功能性安全。ABB 变频器具备许多通过认证的标配或可选的安全功能。典型范例就是 TÜV 认证的 FSO-11 安全功能模块，该模块兼容 ABB 的 ACS880 工业级变频器系列。

3.2 安全力矩中断（STO）作为基础

ABB 一直十分注重在变频器中置入安全功能。我们凭借 ABB 变频器和可编程逻辑控制器以及全系列安全继电器和接触器、急停开关等安全装置，提供经济划算的安全解决方案。根据机器安全性的需要，我们的解决方案可以是一台变频器，或包括多台变频器的整套系统。

如第 1 部分所述，安全力矩中断（STO）是基于变频器的功能性安全的基础。因此，一些 ABB 变频器已将 STO 内置为标配功能，而另一些变频器系列则将其作为可选功能。

标配 STO 功能的全能型 ACS880 工业级变频器，是基于变频器的集成式功能性安全的最新范例。其具备最高级的机械安全性能，符合 SIL 3 和 PL e 安全级别。

STO 可以用安全限速控制（SLS）这样的额外安全功能来补充，以确保不超过变频器和机器中的特定速度级别。

通过在变频器内部集成安全功能，可以不必使用费用高昂的接触器、安全继电器等外部安全附件。利用基于变频器的集成式功能性安全，可以使安装工作更简洁，成本更低，同时，达到规定 SIL 或 PL 所需的器件也最少。

3.3 三个实例

在本节中，将介绍实施 ABB 基于变频器的功能性安全解决方案的三种不同方式，以工业传送带为例。

在虚构示例中，我们假定人员与传送带之间通过取放物料进行频繁互动。根据针对传送带所做的风险分析，停下来时，譬如进行清洁时，应保持安全的断电状态。这意味着，停下来后，电机必须处于无转矩状态，因为意外启动已被确定为风险。

当随时按下红色的急停按钮时，传送带必须以安全方式停下来。并且，当人员靠近防护栏内的传送带时，必须安全降低传送带的速度，以便安全地搬运物料。

通过实施三种机器安全功能，在我们的示例中可降低风险：

1. 防止意外启动
2. 紧急停车
3. 安全限速控制（SLS）

这通过利用两个变频器安全功能来实现：安全力矩中断（STO）和安全限速（SLS）。STO 用于借助急停装置实现紧急停车，并防止意外启动——借助连接到 STO 的可锁定开关。

可利用 ABB 安全装置打造机器安全系统，实现最大限度的控制，如下例所示。

3.4 例 1：利用变频器、安全监控设备、安全编码器和接触器的传统安全方案

打造安全系统的传统方式包括，将安全限位开关、继电器/外部安全监测装置和接触器与变频器连接在一起（见图 7）。

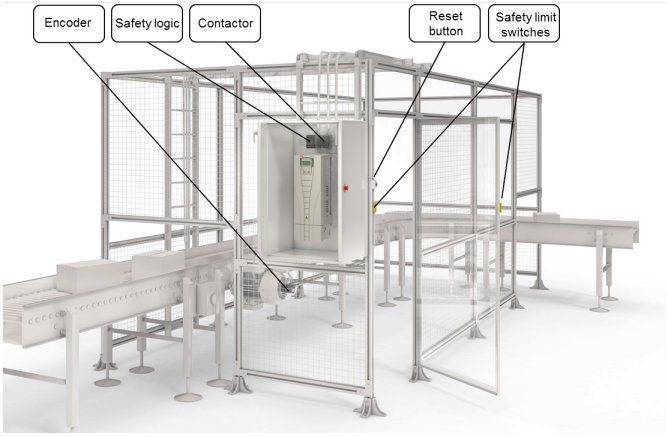

图7. *安全监控器接收并向变频器发送安全脉冲。较之基于变频器的集成式功能性安全，需要更多的安全装置和布线（见图 8）*

一旦将传送带的防护栏门打开，安全限位开关就会检测到打开的门。这会将信号发送至变频器，降低速度。与此同时，信号被发送至外部安全监测装置（安全逻辑器），该装置与编码器速度测量装置一起，创建安全功能 SLS，用于安全速度监控。

操作人员现在可与缓缓移动的传送带安全互动，执行任务。在离开传送带和关闭防护栏门后，安全监控器必须通过一个按钮进行复位，然后允许传送带恢复至正常速度。

如果在 SLS 启用时的安全速度阶段，由于某个原因出现故障，导致传送带突然加速，那么，安全监控器将检测到超速，并激活电机接触器，中断变频器向电机的输出，从而使传送带停下来。

传统机电安全解决方案的优势：

- 安全解决方案可与并未集成安全功能的变频器结合在一起

3.5 例 2：基于变频器的集成式功能性安全

借助基于变频器的集成式功能性安全，安全功能得以通过变频器在机器中实施。结果，可不必使用外部接线的分立安全装置，比如，安全监控器、布线、编码器（见图 9）等。

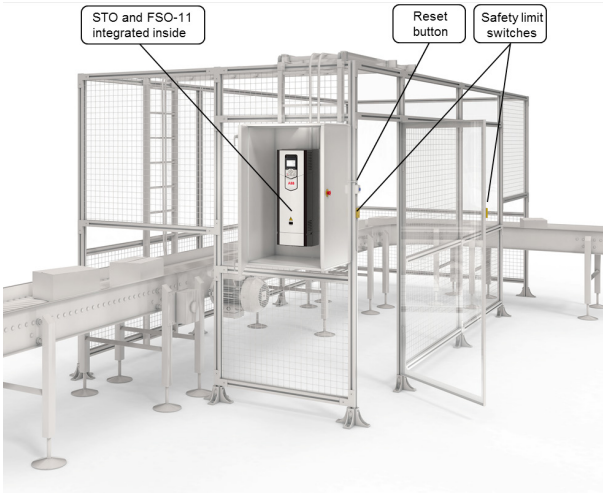

图 8. *安全逻辑集成到变频器中，确保有效的安全监控。较之基于变频器的功能性安全解决方案，需要的安全装置和布线更少（见图 7）。*

基于变频器的集成式功能性安全，不仅可简化总体安全设计过程，而且使用的部件

更少，布线更少，配置和安装复杂程度也显著下降，从而降低了总成本。

较之传统的安全解决方案，基于变频器的集成式功能性安全包括同样的功能，只是内置于变频器中。最基本的功能级别是变频器内部的 STO 电路，可安全地中断变频器的输出，从而不必配备电机接触器。

ABB 标配 STO 的低压交流变频器产品包括：ACS880、ACS580、ACS850、ACS355、ACQ810、ACSM1 和 MicroFlex e150。ACS800 变频器将 STO 作为内置可选功能。

当需要额外的集成式安全功能时，ABB 可选的 TÜV 认证的安全功能模块 FSO-11 非常适合 ACS880 变频器。

FSO-11 无缝支持全能型 ACS880 变频器，并可用于系统（达到 SIL 3/PL e 等级）。该紧凑型安全模块具备多种安全功能，包括：安全停车 1（SS1）、紧急安全停车（SSE）、安全制动控制（SBC）、安全限速控制（SLS）、最高安全限速（SMS）和防止意外启动。

利用 FSO-11，消除继电器、复位信号和接触器之间连接和布线的繁琐性，因为变频器安全功能在模块中进行了预先设计，只需要参数设置即可进行调试。此外，利用 ACS880 变频器系列的通用 PC 工具 Drive composer pro，可以轻松调试和配置变频器系统。

基于变频器的集成式功能性安全的诸多优势：

- 没有需要更换或维护的易损件
- 减少布线，可节约成本和时间
- 安全功能被无缝集成到变频器中。
- STO 取代接触器，用作电机关断路径，速度更快，并能降低成本，节省空间，且减少磨损/维护
- 借助 STO，无需给变频器断电或将输出接触器用于防止意外启动，从而实现更快重启，并且，无需重置参考位置等
- 安全速度监控功能无需编码器（针对不带有功负载的应用），节省成本、节约空间（当变频器关断时，电机自由停车）
- FSO-11 易于安装和调试（仅面向 ACS880 变频器）
- FSO-11 在一个紧凑型模块中具备多种安全功能
- 借助 FSO-11 无编码器模式，针对机器运动的所有安全监控工作可在变频器内部实现。无需额外的逻辑或设计。

3.6 例 3：系统安全监控解决方案利用变频器和安全 PLC 实现多变频器控制

当安全系统包括多台变频器时，安全可编程逻辑控制器可用于从一个共同的源控制变频器和机器。当然，系统安全监控可利用结合安全可编程逻辑控制器（如，ABB 的 AC500-S 安全 PLC）的传统安全解决方案进行设计。通过这种方式，对于通过一个共同的安全可编程逻辑控制器控制的应用，可执行不同的安全功能。

更好的策略可能是，利用配备安全可编程逻辑控制器的基于变频器的集成式功能性安全，打造安全监控解决方案。在这种方案中，安全可编程逻辑控制器（AC500-S）连接到变频器，变频器需配备安全现场总线适配器模块实现 PROFIsafe 连接。

图9. *具备传统和集成式变频器安全功能，通过安全可编程逻辑控制器进行控制的安全系统。*

在基于变频器的集成式功能性安全中，可编程逻辑控制器通过每台（ACS880）变频器内部的 FSO-11 安全功能模块控制整个安全系统，从而提供不同的安全功能和关键诊断信息。变频器通过控制电机转速、转矩和停机来进行本地安全监控。

另外，也可以根据应用中的安全区对变频器进行分组。譬如，传送带上任何一台变频器超速，可能都要求所有变频器停下来，可以通过激活所有变频器的 STO 来实现。类似地，紧急停机命令通常能使所有变频器停下来，而防止启动也可进行更细化的分组。

配备安全 PLC 的基于变频器的功能性安全具备诸多优势：

- 当使用 PROFIsafe（FENA-11）等安全现场总线时，减少 PLC（如，AC500-S）与变频器之间的布线
- ACS880 变频器中的安全功能模块（FSO-11）借助诊断和安全信息（即，安全电机转速信息）为安全可编程逻辑控制器提供支持
- 单一的安全装置供应商，可简化订购流程并降低成本
- 共同支持缩短机器的停机时间
- 可以根据需要的特定功能，对变频器进行分组

3.7 简易编程工具 FSDT-01

ABB 的功能性安全设计工具 FSDT-01 有助于设计人员创建安全功能文档，以支持机器的安全设计。该工具易于使用，可引导用户从内置资源库中选择适合的设备，譬如，变频器、可编程逻辑控制器及其他安全装置等。借助上述设备，即可验证机器所需的 SIL/PL 是否实现。必要的安全功能和 SIL/PL 根据机器设计人员进行的风险评估进行定义。

小结

在工业环境中，有许多运动的机器零件，可能导致危险情况，造成严重的并且往往是永久性的伤害。功能性安全的作用就是，使人员、财产和生态系统免受可避免的意外事故的损害。因此，确保所提供产品的安全，是设备供应商、机械制造商和系统集成商的终极责任。

通过遵守相关的安全指令和标准来实现机器安全。在欧盟地区，机械制造商必须遵守的基本健康和安全要求（EHSR），在机械指令 2006/42/EC 和根据该指令制定的统一标准中进行了定义。对于欧盟地区以外的机械制造商，欧盟统一标准的 IEC/ISO 版本为其提供必要的要求和指导。

变频器现已在许多工业应用中使用了几十年。在自动化系统安全一度需要配备许多外部附加设备的情况下，工业领域日益提高的自动化水平，加上许多现代变频器和安全可编程逻辑控制器的电子技术能力，意味着变频器系统目前能极大地提升系统的总体安全性。

白皮书

现在，经改进的全新安全解决方案与标准，使得安全成为变频器功能的组成部分。基于变频器的功能性安全意味着，提供基于变频器的运动控制，确保人员、财产和生态系统的安全。

ABB 变频器具备许多功能，可帮助安全设计人员以经济划算的方式达到所需的安全级别。

了解更多

基于变频器的功能性安全为机械制造商、设计人员和安全专家创造了无限可能。

如需了解更多信息，敬请访问：
www.abb.com/drives

联系方式

Ere Jääskeläinen
市场经理
ABB芬兰
P.O. Box 184
FI-00381 Helsinki
Finland
ere.jaaskelainen@fi.abb.com

Pasi Pohjalainen
市场经理
ABB芬兰
P.O. Box 184
FI-00381 Helsinki
Finland
pasi.pohjalainen@fi.abb.com

Mikko Ristolainen
功能性安全经理
ABB芬兰
P.O. Box 184
FI-00381 Helsinki
Finland
Mikko.ristolainen@fi.abb.com

白皮书

免责声明

本文作为指南，旨在帮助机器用户、说明书编写人员和机器制造商及相关人员更好地了解欧盟机械指令的各项要求，以及遵从该指令及相关统一标准所需的举措。

本文并非为了逐字逐句使用，而是提供有用的帮助。本指南中的信息和示例仅作一般用途，并不涉及实施安全系统的所有必要细节。

对于使用本文中信息所造成的直接或间接伤害或损坏，ABB Oy Drives 不承担任何责任。机械制造商永远负责依据适用法律的产品安全及其适用性。因此，ABB 不承担可能因本文而产生的一切责任。

参考

1. ABB 技术指南 10——功能性安全

术语表

基于变频器的功能性安全
与变频器协同应用的主动式机器安全功能

基于变频器的安全功能
安全设计原则（机械指令）中声明的用于确保机器安全的变频器安全功能。安全功能包括：STO、SLS、SS1；SMS、SBC、SSE。

功能性安全
功能性安全是总体安全性的一部分，依赖于系统或设备针对输入进行正确响应。

统一标准
根据欧洲委员会或欧洲自由贸易联盟秘书处的要求拟定的欧洲标准，其目的是支持指令的基本要求，并且，根据欧盟法律具备有效的强制性。

危害
潜在的危害源。

PL，性能等级
级别（a、b、c、d、e）用于规定安全系统在可预见情况下执行安全功能的能力。

风险
发生伤害的可能性以及伤害的严重程度的结合。

安全功能
专为增加机器安全而设计的功能，如果发生故障可能导致风险迅速增加。

SIL，安全完整性等级
级别（1、2、3、4）用于规定电气安全系统在可预见情况下执行安全功能的能力。机器设备中仅使用1到3级。