Motion Control Products

Application note
Machinery safety

AN00209

Rev D (EN)

This documentation is meant only as an introductory guide. It is not meant as a guaranteed procedure that will allow a machine builder to achieve full compliance with the safety requirements of their machine. It is the full responsibility of the machine builder to comply with all relevant standards and safety regulations

Introduction

The purpose of this application note is to provide a guide to machine builders on functional safety and how it can be implemented on ABB motion products. This application note is written to provide background information on the subject of functional safety.

This application note is associated with an additional application note which focusses on detailed methods for the safe stopping of servo drives from ABB motion products:

AN00206 - Implementing safety functions on ABB servo drives

Machine builders legal obligations

The European Union is harmonizing safety regulations across all member countries. It will be necessary for all machine builders to comply with these regulations if they wish to sell equipment into Europe. There are also many similarities between these regulations and those in other regions of the world.

CE marking and functional safety:

When a manufacturer marks a product with the CE mark this means that it complies with all relevant European directives. The Machinery Directive has the following definitions of a machine:

- An assembly of linked parts or components, at least one of which moves, and which are joined together for a specific application.
- An assembly of machines or complex plants (complex plants include production lines and special purpose machinery made up of several machines)
- Safety components, such as light curtains, safety mats etc.
- Interchangeable equipment that can modify the basic functions of a machine.

A machine manufacture (watch use of capital letters – machine manufacturer) is anyone who assembles machines or any parts of machines. It also includes machine users who modify the machine or end users who create an assembly such as a production line of multiple machines. Machinery that has been built for the builders own use must also comply.

The process for fulfilling the Essential Health and Safety Requirements EHSR of the machinery directive may be divided up into 9 separate steps. These steps will be elaborated on further on in this application note:

1. Management of functional safety.
2. Risk assessment.
3. Risk reduction.
4. Establishing safety requirements.
5. Implementing a functional safety system.
6. Verifying functional safety system.
7. Validating functional safety system.
8. Documentation.
9. Compliance.

Machine Directive and safety components:

The Machinery Directive describes a safety component as follows:

- Serves to fulfil a safety function.
- Is independently placed on the market.
- The failure and/or malfunction of which endangers the safety of persons.
- Is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.

Examples of electrical safety components that will often effect the operation of ABB motion products are:

- Electro sensitive devices designed specifically to detect persons in order to ensure their safety, e.g. non-material barriers, sensor mats, electromagnetic detectors.
- Power-operated movable guard switches.
- Emergency stop devices.
- Over-speed limitation devices.
- Electric safety devices in the form of safety switches containing electronic components.

Machine Standards:

The Machinery Directive lists over 600 standards that are harmonized. There are many more that are not. The list below is a short list of the main generic standards that relate to electronic drives for use in machines. Many of the standards are specific to a particular type of machine. These are called C standards. If no relevant C standard is available a generic standard is used. Listed below are the standards discussed in this application note.

EN ISO 13849-1:2008 Harmonised.

Safety of machinery safety-related parts of control systems – Part 1: General principles for design. EN ISO 13849-1 is a generic standard for functional safety and provides presumption of conformity within the EU. The scope is given as the electrical, electronic, programmable electronic, mechanical, pneumatic and hydraulic safety of machinery.
EN 62061:2005 Harmonised safety of machinery functional safety of safety-related electrical, electronic and programmable electronic control systems

EN ISO 14121-1:2007 Harmonised.

Safety of machinery risk assessment – Part 1: Principles

STEP 1: Management of functional safety:

To achieve the required level of functional safety it is first necessary to have the correct management in place. This can be in the form of a safety plan. A safety plan would perform the following functions:

- Identify all relevant activities.
- Describe the policy and strategy for implementing functional safety.
- Identify responsibilities.
- Establish procedures and resources for documentation.
- Describe management of the configuration of the safety system.
- Include a plan for verification and validation.

Step 2: Risk assessment:

This is a process where each risk associated with the machine is identified and evaluated. Any risk assessed as being high should ideally be eliminated by design changes. If this is not possible the risk may be reduced by implementing a safety function. As a last resort any residual risk should be clearly documented in the user manual. Clear signs should be fixed to the machine to alert to the hazard.

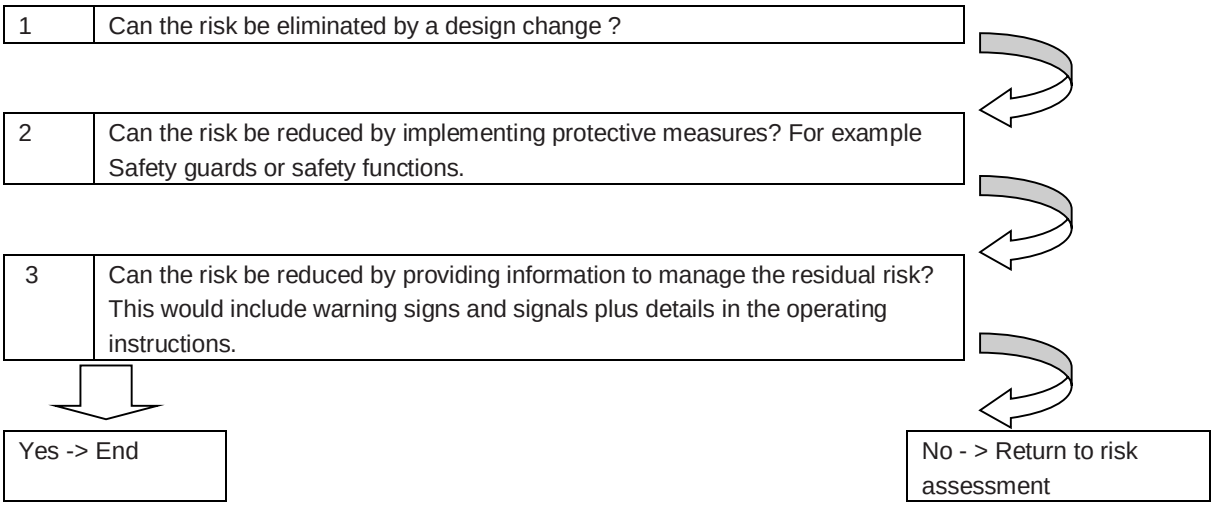
Standards EN ISO 14121-1:2007 and EN ISO 12100-1:2003 explain the process of risk analysis and minimization. There is much repetition between standards but the basic risk assessment procedure contains the following steps:

Step 1	Determine the limits and intended use of the machine. These limits can be listed in sub categories such as: – Limits of use. – Spatial limits. – Environmental limits – Life cycle and life time limits – etc.
Step 2	Identify the hazards associated with the machine.
Step 3	Estimate the risks identified one by one. The level of risk is a product of two attributes. The *Severity* of the risk and the probability of it occurring.
Step 4	Evaluate the level of risk. Is the level low enough ?
Yes -> End	No - > Risk reduction

Document this process for each hazard individually. If the result of this analysis reveals that the risks are acceptable then the process ends here. If the risks remain unacceptable then move on to step 3

Step 3: Risk reduction:

If the risk cannot be eliminated then standard EN ISO 12100-1 recommends 3 steps for reducing the risk.



There will inevitably be some residual risk that cannot be reduced further by technology or design changes. These must be documented in the operating instructions. Further risk reduction measures may be suggested in the documentation. These would include:

- Introducing safe working procedures.
- Work supervision.
- Permit to work systems.
- Use of personal protective equipment.
- User training.

The remaining steps in this application note describe implementing a safety function (option 2 of the risk reduction procedure) in further detail.

Step 4: Establish safety requirements:

The process of risk reduction described above will attempt to reduce all risks to an acceptable level. Inevitably some safety function will be required to reduce the risk still further. The safety function reduces the likelihood of an accident occurring during exposure to a hazard. The safety function is not part of the normal operation of the machine. If the safety function fails the machine will still operate. The performance of the safety function must be assed for each identified hazard.

A safety function consists of an action (What is done to reduce the risk) and a safety performance (A measure of how effective the action has to be). For example if the hazard was a rotating shaft the action might be to stop the motor in one second when the safety gate is opened.

The required safety performance must then be determined. There are two standards that can be used to do this. They use different methods. EN 62061determines the Safety Integrity Level (SIL) of the safety function. EN ISO 13849-1 determines the Performance Level (PL). Either can be used and both can be found to be equivalent.

Choosing which standard is used depends on the choice of technology, experience and customer requirements. EN62061 has a strong bias towards control systems. EN ISO 13849-1 is more generic.

Determining the required SIL (EN62061)

The steps to determine the SIL are as follows:

1. Determine the severity of the consequence of the hazard.
2. Determine the frequency and duration that someone is likely to be exposed to the hazard.
3. Determine the probability of a hazardous event occurring when exposed to it.
4. Determine the possibility of avoiding harm.
5. These are demonstrated in the table below.
6. Adding the frequency (Fr), probability of occurrence (Pr) and probability of avoidance (Av) gives the class (Cl).
7. The class and the severity (Se) are then used to determine the required SIL.

Probability of occurrence of harm					
Fr		**Pr**		**Av**	
Frequency, Duration		**Probability of hazardous event**		**Avoidance**	
<= Hour	**5**	Very high	**5**		
> 1h <= Day	**4**	Likely	**4**		
> Day <= 2 Weeks	**3**	Possible	**3**	Impossible	**5**
> 2 Weeks <= 1 Year	**2**	Rarely	**2**	Possible	**3**
> 1 Year	**1**	Negligible	**1**	Likely	**1**

Severity of harm	
Se	
Consequences (severity)	
Death, losing an eye or arm	4
Permanent, losing fingers	3
Reversible, medical attention	2
Reversible, first aid	1

SIL Class				
Class Cl				
3-4	5-7	8-10	11-13	14-15
SIL2	SIL2	SIL2	SIL3	SIL3
OM	OM	SIL1	SIL2	SIL3
OM	OM	OM	OM	SIL1
OM = Other Measures				OM

In this example, Class **Cl = Fr + Pr + Av** = 5 + 3 + 3 = 11. With an **Se** of 3 this gives **SIL2**.

Determining the required PL (ISO13849-1)

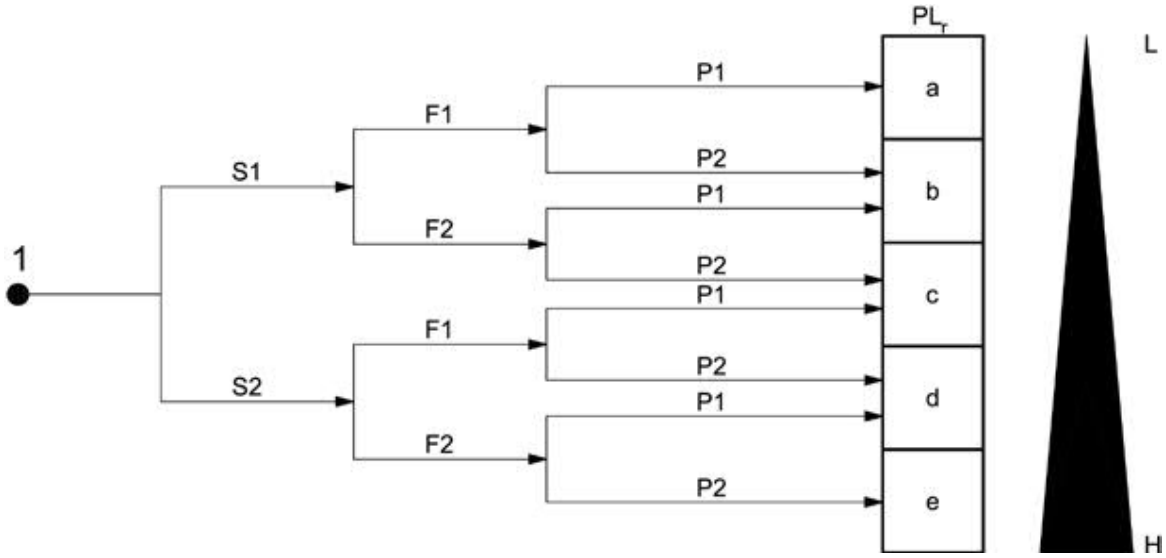
The steps to determine the PL are as follows:

1. Determine the severity of the damage.
   S1 is for slight, reversible injury
   S2 is for severe irreversible injury or death.

2. Determine the frequency and duration of exposure to the hazard.
   F1 is from rare too often or short periods of exposure
   F2 is for continuous or long periods of exposure.

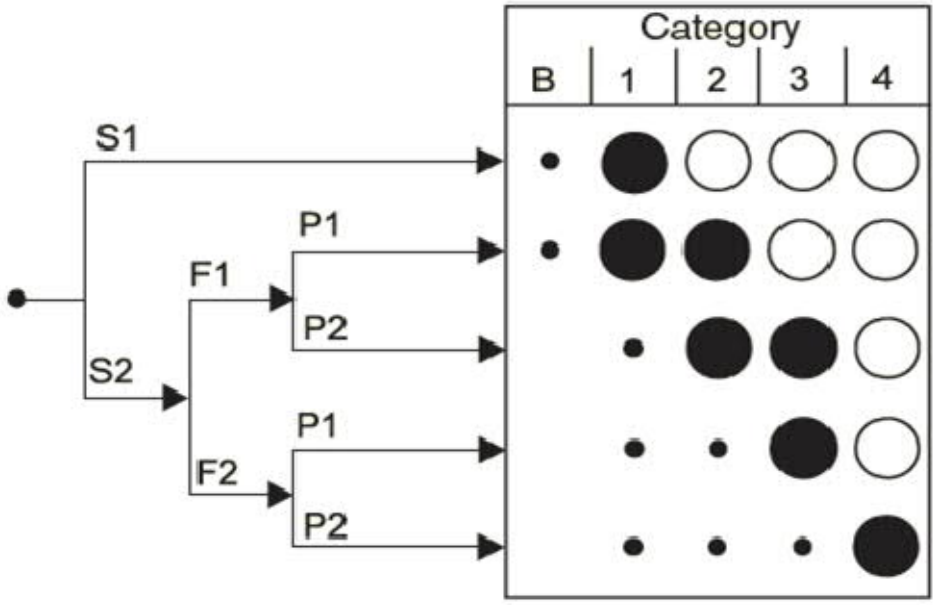
3. Determine the probability of avoiding the hazard or limiting the damage caused.
   P1 Possible under some conditions
   P2 Hardly possible.

   These steps are illustrated in the diagram below:



A note on Safety Categories for safety systems:

EN 954-1 defined control categories after consideration of the risk parameters. The diagram for determining the correct category is shown below:



Method for selecting a safety category for safety-related parts of control system. Annex B (informative) of standard EN 954-1.

standard EN 954-1.

The shaded circles represent recommended categories. The clear circle means that the measure is over dimensioned.

EN ISO 13849-1 supersedes EN 954-1 and introduces performance levels (PL). Performance level takes residual probability into consideration. The PL grades are selected so that they comply with the so-called safety integrity levels (SILs) from IEC EN 61 508 and also allow reference back to the control categories from EN 954-1.

The safety categories determine the required behaviour of the safety-related parts of a control system in respect to their resistance to faults. Categories B, 1,2,3 and 4 are described below.

Safety category B

The safety-related parts of control systems and/or their safety equipment, as well as their components must be designed, built, selected, assembled, and combined in accordance with the relevant standards so that they can withstand the following:

- Expected operational stress (e.g., reliability with regard to switching capacity and switching frequency)
- Influence in the work process of materials used (e.g., detergents in a washing machine)
- Other relevant external influences (e.g., mechanical vibrations, external fields, power supply interrupts or malfunctions)

For parts that meet safety category B, no special safety measures are used. The occurrence of a fault can lead to the loss of the safety functions.

Safety category 1 (Single-channel control)

The requirements of category B must be met. Proven components and proven safety principles must be used.

The occurrence of a fault can lead to the loss of the safety functions, but the probability that the fault will occur is lower than in category B.

Safety category 2 (Single-channel control and testing)

The requirements of category B and the use of proven safety principles must be met. The safety function must be tested at suitable intervals by the machine control system. Testing of the safety function, whether initiated manually or automatically, must generate a starting point for the initiation of suitable control measures if a fault is present. If it is not possible to achieve a safe shutdown, the output must provide for a warning of the hazard.

The occurrence of a fault can lead to the loss of the safety function between the test intervals. The loss of the safety function is detected by the test.

Safety category 3 (Single-channel control (redundant))

The requirements of category B and the use of proven safety principles must be met. Safety-related parts must be designed so that:

- A single fault in one of these parts does not lead to the loss of the safety function
- Whenever possible, the single fault is detected on or before the next demand of the safety function

When the single fault occurs, the safety function is always performed.

- Some but not all faults are detected.
- An accumulation of undetected faults can lead to the loss of the safety function.

Safety Category 4 (Single-Channel Control (Redundant) and Testing)

The requirements of category B and the use of proven safety principles must be met. Safety-related parts of the control system must be designed so that:

- A single fault in any of these parts does not lead to the loss of the safety function
- The single fault is detected on or before the next demand of the safety function. If this is not possible, then an accumulation of faults must not lead to the loss of the safety function.

When faults occur, the safety function is always performed. The faults will be detected in time to prevent the loss of the safety function.

Step 5: Implementing functional safety system:

In this step the hardware to implement the safety function is chosen. This may consist of several subsystems. Each sub system will have a safety performance (SIL or PL) associated with it. The safety performance of the overall safety function is only as high as the lowest SIL or PL of any subsystem.

If non–certified subsystems are used then the machine manufacture must calculate the achieved SIL or PL for each subsystem. The calculations for these are in the standards EN62061 and ENISO 13849-1. These calculations are complex and require information that may be difficult to acquire. It is best to use certified subsystems as these will already have some of the performance level calculations available already.

The steps to implement the safety function include.

1. Start by defining the required safety performance (SIL or PL) from the previous section.
2. Select the system architecture to be used. EN ISO13849-1 and EN62061 offer basic architectures.
3. Construct the system from safety subsystems such as guards, switches and relays etc.
4. While installing the system make sure that the safety integrity of the system is not compromised by improper wiring.
5. Verify the functional safety of the system, which is described in the next sections.

Step 6: Verifying a functional safety system:

Verification of the functional safety system demonstrates that the safety performance of the safety function meets the required performance from the risk evaluation.

Verification should be carried out together with the implementation process.

In addition to verifying the SIL or PL of the system, the correct operation of the safety system must also be verified by carrying out functionality testing.

Verifying the SIL of a safety system (EN 62061)

This guide assumes that a certified safety sub component is used. The following steps may be used to verify the SIL.

1. Take the Probability of Dangerous Failure per Hour (PFHd) for each subsystem. This should be provided by the manufacturer of the safety sub-system. PFHd is the random hardware failure value.

2. Use the Common Cause Failure (CCF) Checklist to make sure that all necessary aspects of the safety system have been considered. The checklist can be found in Appendix F of EN 62061.

3. Use the PFHd in the table below to determine the SIL for the sub system.

SIL	Probability of dangerous failures per hour (1/h)
SIL 1	>= 10-6 up to < 10-5
SIL 2	>= 10-7 up to < 10-6
SIL 3	>= 10-8 up to < 10-7

4. The SIL Claim Limit (SILCL) represents the maximum SIL value that the subsystem performs to. The SILCL of the whole system cannot be higher than the SILCL of any subsystem. The SILCL should be provided by the manufacturer of the Safety Sub-System.

Verifying the PL of a safety system (EN ISO 13849-1)

This guide assumes that a certified safety sub component is used. The following steps may be used to verify the PL.

1. Use the Common Cause Failure (CCF) Checklist to make sure that all necessary aspects of the safety system have been considered. The checklist can be found in EN ISO 13849-1:2008 Annex I.

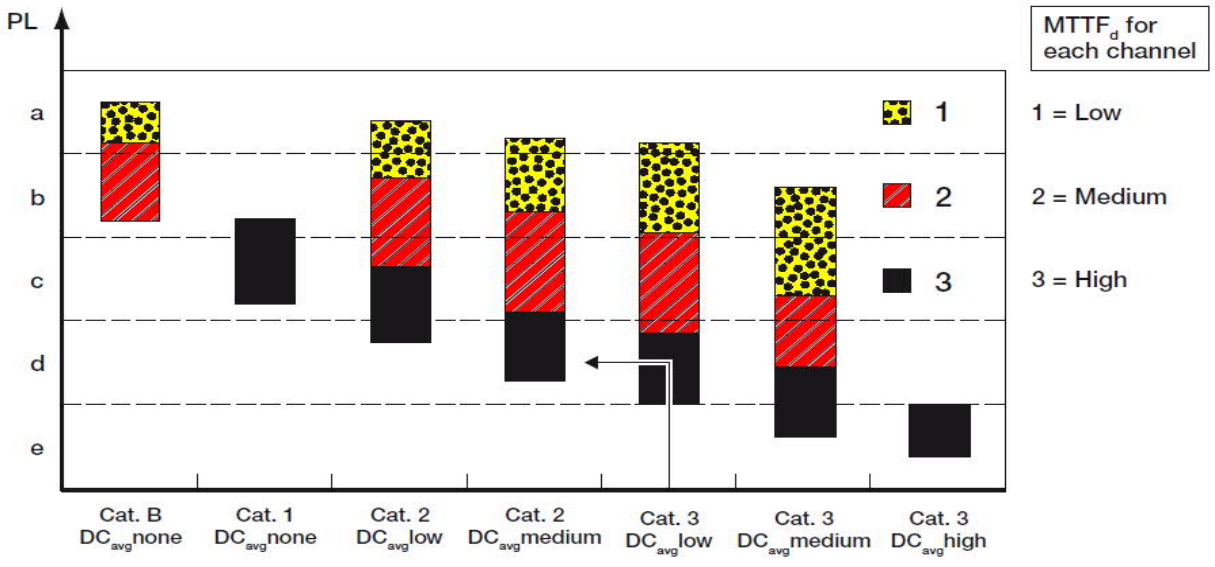
2. The manufacturer of the safety sub system should provide a value for the Mean Time to Dangerous Failure (MTTFd). This is the average time it takes for a dangerous failure to occur. A qualitative value can be read from the table below:

Description of quality	Value range MTTFd
Low	3 Years <= MTTFd < 10 Years
Medium	10 Years <= MTTFd < 30 Years
High	30 Years <= MTTFd < 100 Years

3. The manufacturer of the safety sub system should provide a value for the Diagnostic Coverage (DC). This is the number of dangerous failures that can be detected by diagnostics before they occur. A qualitative value can be read from the table below:

Denotation	Range DC
none	DC < 60%
low	60 % <= DC < 90 %
medium	90 % <= DC < 99 %
high	99 % <= DC

4. The graph below allows the required measures to be determined given the value of PL from the risk assessment. There is some ambiguity in this graph. PL on its own encompasses a band of safety measures so there is a choice. For example if the PL = d you could satisfy this in 3 different ways. You could choose a High MTTFd and choose either Category 2 or a low DC. Alternatively a medium MTTFd could be chosen at the expense of a higher Category or level of DC.



Example verification of PL

Comparison of SIL vs. PL

Although methods of evaluation differ between the two standards, the evaluation results can be compared on the basis of random hardware failure.

Safety Integrity Level SIL	Performance Level PL
No correspondence	a
1	b
1	c
2	d
3	e

Step 7: Validating the functional safety system:

Each safety function must be validated in order to ensure that it reduces risk as required in the risk assessment phase.

In order to determine the validity of the functional safety system, the system must be inspected against the risk assessment process carried out in step 2. The system is valid, if it truly reduces the risks.

Step 8: Documenting the functional safety system:

The design of the machine must be documented and relevant user documentation produced before the machine fulfils the requirements set in the Machinery Directive.

Documentation has to be accurate and concise, but at the same time informative and easy for the user to understand. All residual risk must be documented in the user documentation with proper instructions on how to operate the machine safely. The documentation must be accessible and maintainable. The user documentation is delivered with the machine.

Step 9: Proving compliance:

Before a machine may be placed on the market the manufacturer must ensure that it fulfils the relevant essential health and safety requirements defined by the Machinery Directive. This conformity can be assured by following relevant harmonized standards as described in this document.

It will be necessary to provide an up to date technical file supporting this compliance. The file should describe the design, manufacture and operation of the machinery. See Annex VII of the directive 2006/42/EC for more information.

To sell in the EU an EC declaration of conformity must be produced and delivered with the machine. CE marking is then affixed.

Safe stop functions:

Stop functions are found on almost all machines. EN 60204-1 defines 3 categories of stop function for the various functional requirements:

A category 0 stop leads to an immediate removal of power to the machine actuators. Activation of the mains isolating device automatically triggers a category 0 stop, as power is no longer available to generate the movement.

With a category 1 stop, power to the actuators is maintained to enable a controlled stop.

Stop category 2 is used if power is required even in a stop condition, as power is maintained after the controlled stop.

EN 61800-5-2 assigns stop functions to the stop categories listed in EN 60204-1. EN 61800-5-2 divides safety functions into stop functions and other motion safety functions. These are listed below:

Safe Torque Off (STO)

This corresponds to a category 0 stop. Power is removed from the motor and it comes to an uncontrolled stop. It is not necessary to monitor the motor at standstill. This is often used as a backup for one of the other stop categories.

Safe Stop 1 (SS1)

This corresponds to a category 1 stop. The method of motor braking is defined. Implements an STO function at standstill. The run down function is monitored inside the drive which reduces stop times and thereby reduces safety distances from the hazard.

Different implementations:

Monitored time delay: Non-safety drive technology implements the motor ramp down and then power is safely removed from the drive after a safely monitored time delay.

Automatic standstill detection with monitored time delay: Non-safety drive technology implements the motor ramp down and then power is safely removed from the drive after a safely monitored time delay OR if a safety monitoring function detects motor standstill first.

Monitoring of the braking ramp: The drive position is continually monitored by a safety function during ramp down. If it deviates beyond a threshold value an STO is implemented.

Safe Stop 2 (SS2)

This corresponds to a category 2 stop. The method of motor braking is defined. Implements a Safe Operation Stop (SOS) function at standstill. This means that closed loop control is still implemented after stopping to hold the motor at standstill. The run down function is monitored inside the drive which reduces stop times and thereby reduces safety distances from the hazard. Because the drive is still under closed loop control it does not lose its position with reference to the process and so it can be started with little delay.

Different implementations:

Monitored time delay: Non-safety drive technology implements the motor ramp down and then a SOS function is implemented after safely monitored time delay.

Automatic standstill detection with monitored time delay: Non-safety drive technology implements the motor ramp down and then a SOS function is implemented after safely monitored time delay OR if a safety monitoring function detects motor standstill first.

Monitoring of the braking ramp: The drive position is continually monitored by a safety function during ramp down. If it deviates beyond a threshold value an STO is implemented. If the drive successfully reaches the idle speed and position a SOS function is implemented.

Safe motion functions

Safe encoder systems:

The implementation of safety-related monitoring is heavily dependent on the sensor technology used within the system. The sensor technology used within the drive technology is generally not safety-related and must be monitored in case of a malfunction. The table below shows the reliability of different sensor technologies.

Solution	Description	Safety integrity
Standard encoder	Evaluation of two signal tracks on a common lens.	Low
Two encoders	Two totally separate channels, expensive.	Very high
One encoder and initiator	Two totally separate channels, expensive, imprecise.	Average
Safe encoder	Two independent encoder systems in one housing without safe pre-processing.	High
Safe encoder	Two independent encoder systems in one housing with safe pre-processing.	High
Safe encoder	Dual-channel diverse structure in one encoder housing with safe pre-processing.	High
Standard encoder and motor signals	Two totally separate and diverse channels.	Very high

Safe Operating Stop (SOS)

This means that closed loop control is still implemented after stopping to hold the motor at standstill. Because the drive is still under closed loop control it does not lose its position with reference to the process and so it can be started with little delay.

Safety Limited Acceleration (SLA) and Safe Acceleration Range (SAR)

Ferraris sensors are used to detect acceleration only in special applications of machine tools or printing machinery. Standard drives cannot process these signals in their control loops.

Safely Limited Speed (SLS)

This safety function serves to safely reduce the motor speed from its operating speed to a speed deemed safe. This function can be used to prevent unwanted motor start-up. If the motor deviates from this reduced speed an SS1 stop function is usually implemented.

Safe Speed Range (SSR)

This safety function serves to prevent the motor from dropping below a minimum speed as well as reducing the speed. This would be used when a speed reduction might indicate a potentially dangerous event in a process. Where there are multiple axes in a system it may be hazardous for one axes to suddenly slow down as this may cause crushing or other damage to the machine.
The response to this error may be more complicated than simply stopping the axes. At a minimum it may mean stopping multiple axes.

Safely Limited Torque (SLT) and Safe Torque Range (STR)

Due to the lack of suitable sensor technology, the motor torque cannot safely be monitored externally to the drive. The torque can be monitored indirectly as it is proportional to the motor current. This means that a safety function integral to the drive is necessary to limit the torque.

Safely Limited Position (SLP)

This safety function serves to prevent the motor moving beyond a positional threshold. Some safe stop function will be needed if the threshold is reached. Physical limitations on how fast the motor can be stopped will dictate the threshold value. Absolute position measurement is required for this function.

Safely Limited Increment (SLI)

The motor is allowed move after a start command provided a safe limit distance is not reached. If the limit is exceeded a safe stop function is implemented. Relative position measurement is sufficient for this function to work.

Safe Direction (SDI)

This safety function prevents the motor from moving in an invalid direction. This function is often used in combination with speed limiting.

Safe Cam (SCA)

This safety function triggers a safe output signal when the motor is positioned within a specified range. Absolute position measurement is required for this function.

Safe Speed Monitoring (SSM)

This function is very similar to Safely Limited Speed (SLS) except no direct action is taken on the motor if the speed threshold should be exceeded. This function only monitors the speed and sends a safe output signal to other equipment.

Safe brake functions:

Safe Brake Control (SBC)

This safety function controls a safe output to release a mechanical brake before moving a motor. The brake is a “Safety brake” which will engage under the action of a spring if power is removed. Current limiting circuitry may be included to reduce heating of the brake release solenoid. This function is often used on hoists and similar loads that could move under gravity.

Safe Brake Test (SBT)

This safety function allows the holding ability of a mechanical brake to be tested while the axis is stationary. It can detect a defect due to wear and tear and will send a safe output signal to other systems which may for example shutdown production in this area until the problem is addressed.

Contact us

For more information please contact your
local ABB representative or one of the following:

new.abb.com/motion
new.abb.com/drives
new.abb.com/drivespartners
new.abb.com/PLC