BEI SENSORS

What the new *"Machinery Safety"* regulation means for your company

Specifying encoders for speed monitoring in safety applications according the new EN ISO 13 849-1 is a challenge for most automation engineers or systems integrators developing new machines.

Sensata Technologies

Safety in process automation has always been a point of interest for engineers and system designers. Until now, there was no uniform way to assess and codify a safe system but a new European regulation extends and clarifies the scope of safety. The main question for machine builders or system integrators is:

What do I need to do to place a machine on the market in compliance with this directive?

The European Commission machinery directive stipulates that machinery should not pose any danger. Unfortunately zero risk in technology does not exist, but the aim is to achieve an acceptable residual risk. If safety is dependent on control systems, these must be designed so that the probability of functional faults is sufficiently low. If this is not possible, any faults that occur shall not lead to the loss of the safety function. To meet this requirement, it makes sense to use harmonized standards that have been created in accordance with the European Commission.

In the past, the safety-related parts of a machine control were designed in accordance with EN 954-1 based on the calculated risk. The aim was to assign an appropriate system behavior to each category. Once electronics and programmable electronics in particular, had made their mark on safety technology, safety could no longer be evaluated only in terms of the simple category system and without probability information. EN 62061 and EN ISO 13849-1 were developed to cover this weakness.
Much literature covers this regulation but a few points are key for understanding and making the standards applicable in the field especially in motion and control topics of this article.

Scope of the new Standards EN ISO 13849-1 and IEC/EN 62061

Since 2012 with the application of the new machine directive EN ISO 13849, safety is becoming increasingly significant in machines and plant equipment.

EN ISO 13849-1: This standard may be applied to safety-related parts of control systems and all types of machinery, regardless of the type of technology and energy used. The performance of a safety function is described by the term Performance Level (PL).

IEC/EN 62061: This standard defines requirements and gives recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems for machinery. It does not define requirements for the performance of non-electronic safety-related control elements for machinery. **IEC/EN 62061** represents a sector-specific standard under **IEC/EN 61508**. The performance of a safety function is described by the term **Safety Integrity Level (SIL)**.

The goal of functional safety, as explained above, is to minimize or eliminate risk that can occur during normal or compromised operations of machines or industrial plants. The first approach for achieving an acceptable residual risk is to define an architecture using devices that have already been characterized in terms of safety parameters. These devices require the following safety-related characteristic parameters depending on device type:

- **Category:** Structural Requirement
- **PL / SIL :** Performance Level / Safety Integrity Level
- **PFH or PFD:** Probability of Failure per Hour / Probability of Failure on Demand
- **MTTFd:** Mean Time To Dangerous Failure
- **L10h:** Mechanical Life time
- **DC:** Diagnostic Coverage
- **SFF:** Safe Failure Fraction
- **TM:** Mission Time

PFD (Probability of Failure on Demand)	**PFH** (Probability of Failure per Hour)	**Safety Integrity Level (SIL)** EN 61508 - EN 62061	**Performance Level (PL)** EN ISO 13849-1
$10^{-2} < PFD < 10^{-1}$	$10^{-6} < PFH < 10^{-5}$	1	b, c
$10^{-3} < PFD < 10^{-2}$	$10^{-7} < PFH < 10^{-6}$	2	d
$10^{-4} < PFD < 10^{-3}$	$10^{-8} < PFH < 10^{-7}$	3	e

Basics of a safety procedure approach

A hazard on a machine will result in injury sooner or later if protective measures are not put in place. Protective measures are a combination of the measures taken by the designer and those implemented by the user. Measures taken during the design phase are always preferable to those implemented by the user, and generally they are also more effective.

The designer must follow the sequence described below:

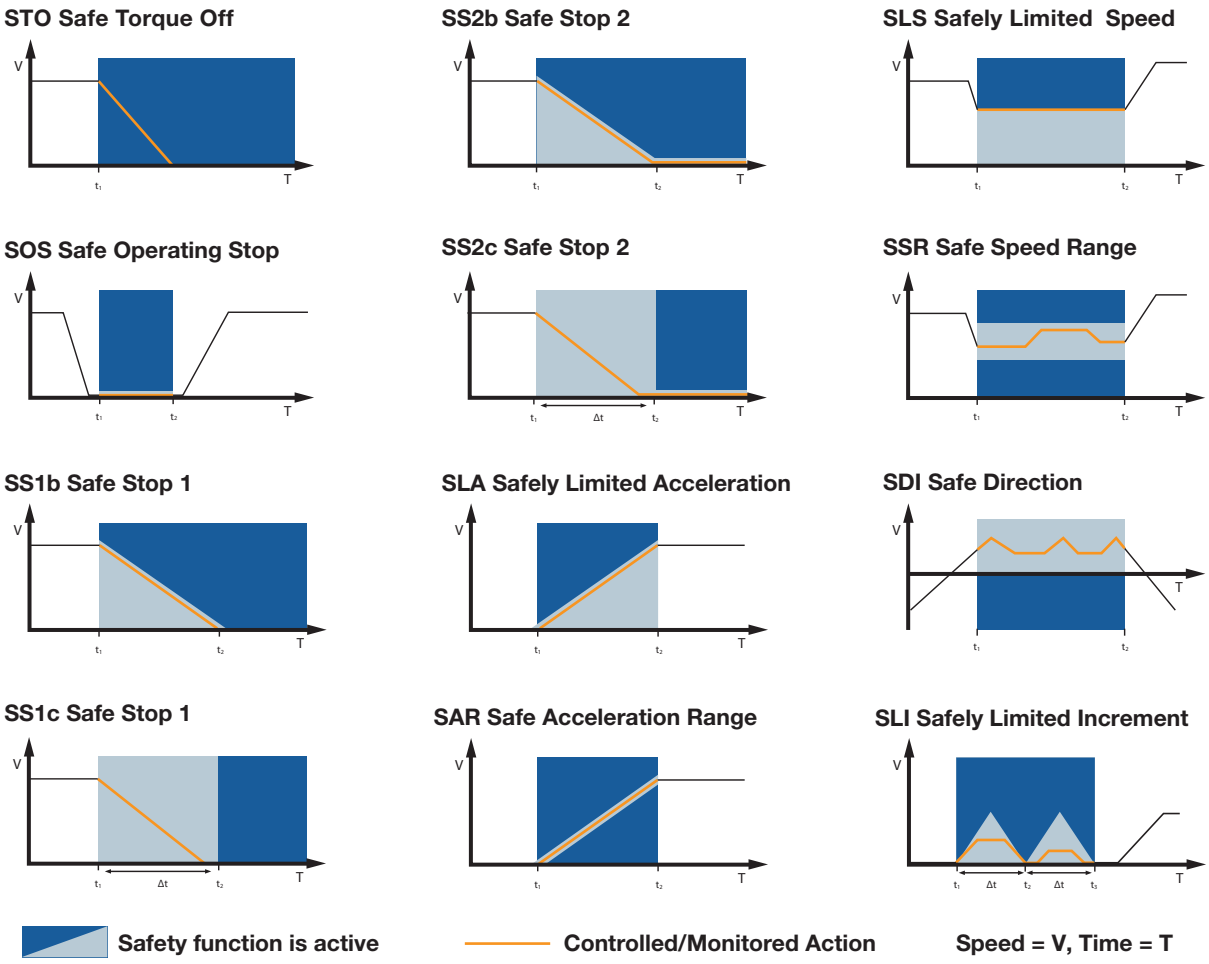
1. Establish the limits and the intended use of the machinery.
2. Identify the hazards and any associated hazardous situations.
3. Estimate the risk for each identified hazard and hazardous situation.
4. Evaluate the risk and decide on the need for risk reduction.

Design of the Motion Control architecture

A part of the risk reduction process involves the definition of the machine's safety functions. This includes the safety functions of the control system, e.g. to prevent unexpected start-up, overspeed detection, rotation direction change etc. When defining the safety functions, it is always important to consider that a machine has different operating states (e.g., automatic & setup mode) and that the protective measures in these different modes may be completely different (e.g., safely limited

speed in setup mode, two-handed safety stop automatic mode). A safety function may be implemented through one or more safety-relevant control parts and several safety functions.

The safety related drive functions being used for the following tasks according to EN 61 800-5-2 are illustrated below:



The most common “safety” architectures in speed monitoring

Incremental encoders are typical parts used in safety related speed monitoring systems. The speed monitoring architecture may be designed in several different ways to get the targeted safety level.

For example, one could consider using redundant sensors and perform a signal comparison of both in order to achieve the required safety level (see Figure 1, next page). However, this approach may not be the most efficient.

Doubling the mechanical complexity, wiring, monitoring etc. makes the task complicated, and not very cost effective. In addition, the responsibility for the entire

safety loop is dependent upon the builder due to the fact that none of the sub-assemblies are assessed by an external independent notification body.

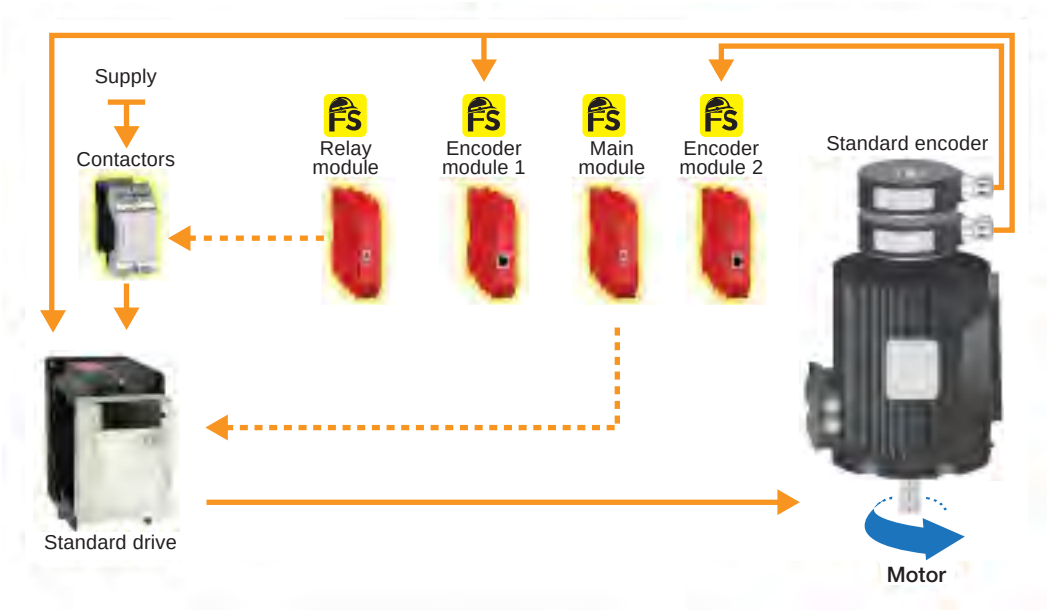
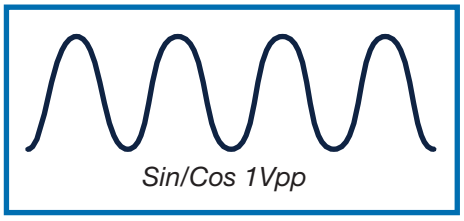


Figure 1: *Safety architecture using redundant sensors adds mechanical complexity and increases installation time and cost.*

Another common approach was to use certified analog encoders with sine cosine signals. This restricted product offer limits the designer's efficiency and technical creativity, as well as the purchaser in sourcing potential suppliers.



Until recently, functional safety encoders on the market have been limited to only sine/cosine signals.

Example of a "safety encoder" implementation

Let's imagine there is a requirement to achieve a SIL3/PLe Category 4 system integrating speed monitoring.

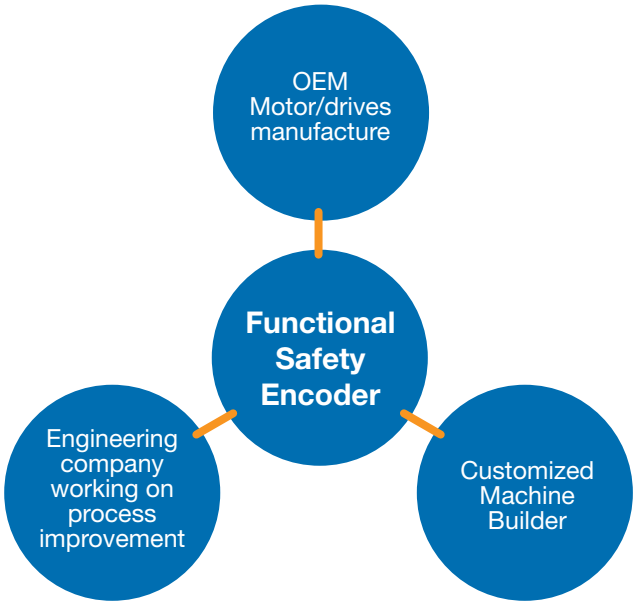
The following are three examples of how a safety rating of SIL3/PLe can be achieved integrating existing equipment.

BEI SENSORS

Example 1

The encoder is a part of the system; it must be backwardly compatible with the legacy products mounted on the motors and connected to the safety drive or PLC.

Key needs: Mechanical interface, signals and wiring should be identical to the standard installation in order to use common parts for safety and non-safety speed monitoring loops on the same equipment.



Example 2

The encoder is a part of existing equipment; it must be compatible to avoid major mechanical changes on the motor and continue to use the current drive and PLC.

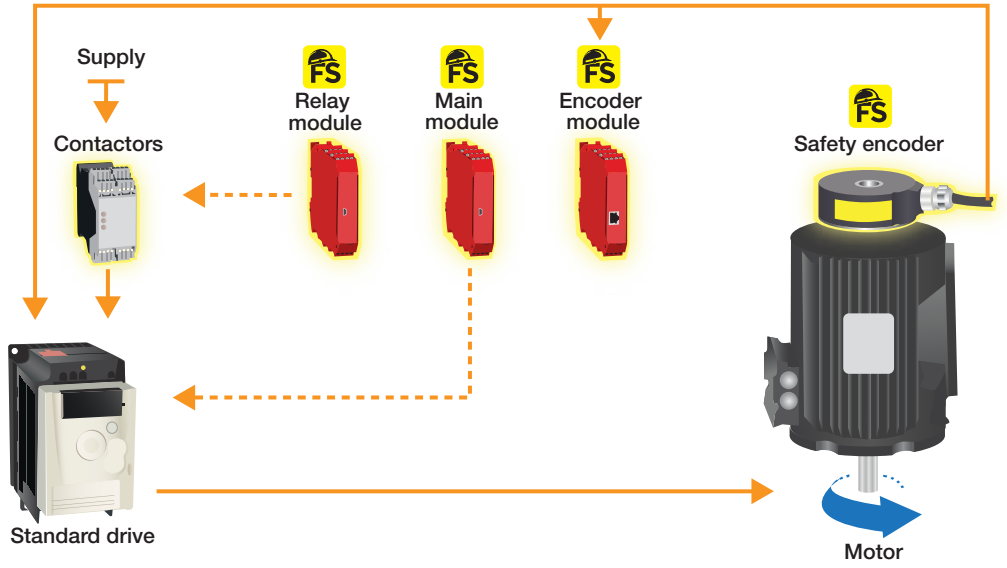
Key needs: Must find additional safety devices such as overspeed controllers integrating safety relays in order to bring the machine into a safe state and maintain the devices currently in place.

Example 3

The encoder needs dedicated features for indoor or outdoor harsh environments. The basic course, the basics of mounting and wiring should match existing assembly procedures.

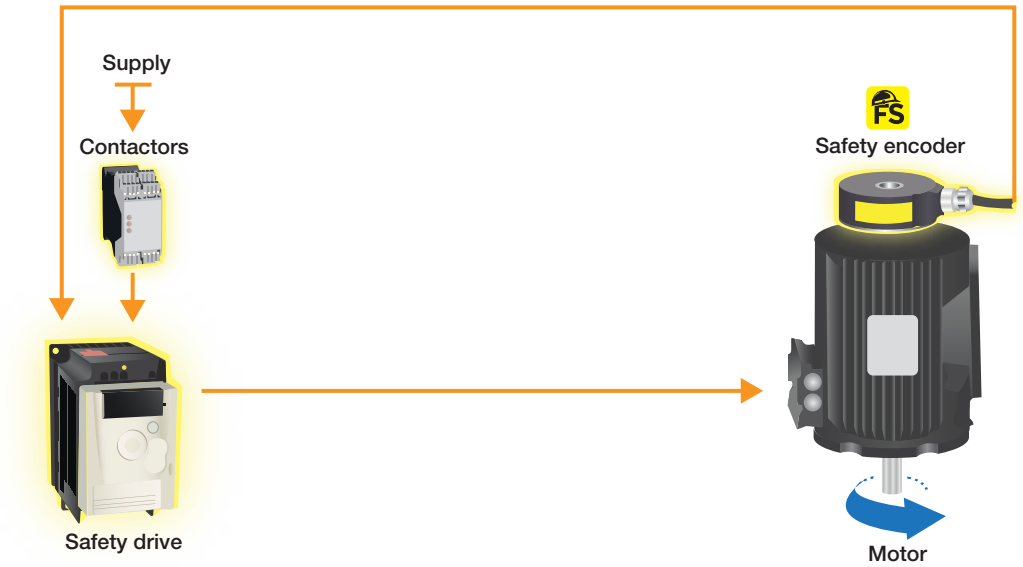
Key needs: Find a supplier offering an extensive range of mechanical, electrical and connection options that cover a large area of industrial and heavy duty applications.

Solution for safety implementation with the fewest changes to the existing system



Modular safety solution: *Legacy drive, PLC and motor are left in place. Only the remaining legacy components are replaced with safety-rated encoder and modules.*

Solution with safety integrated devices



Built-in safety solution: *Fully integrated safety components*

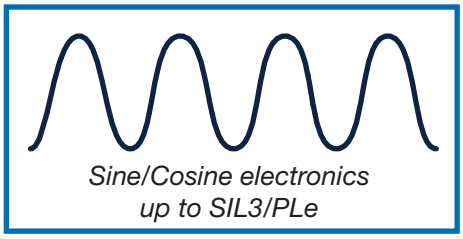
Advantages of a comprehensive digital safety encoder range for speed monitoring

The incremental “safety encoder” offers available on the market have been quite limited and are based on an optical redundancy technology with signal monitoring constructed by an analog (Sine/Cosine) equation calculation ($Sin^2+Cos^2=1$).

In reality, most customers are using and are most familiar with standard digital encoders. Despite the ease of integration issues with a purely digital approach, the availability of good replacement encoders that match to a legacy system is quite limited. The new functional safety digital encoders offer a number of benefits.

Electronics ease of use
Working with a current and familiar communication interface makes the technical approach easy, reduces the risk of signal interpretation errors, limits wrong connections and saves time from the electronics designer up through the wiring technicians.

Only very few manufactures offer an exhaustive encoder range of qualified SIL3/PLe digital electronics with standard features such as 5V or 11-30V power supply, TTL or HTL output, or analog Sine/Cosine output.


Sine/Cosine electronics up to SIL3/PLe


TTL/RS422 or HTL up to SIL3/PLe

Standardized electrical connections
Wiring is always a critical operation that must be done correctly. During the cabinet wiring phase, the technicians familiar with connecting legacy products prefer to stay with the same connection scheme even with safety encoders. Ideally, the cabling of the entire machine including safe and non-safe parts should be the same. Simplicity, cost reduction due to standardization and mis-wiring risk reduction are key for quality and end customer satisfaction.

Mechanical compatibility and safety features
The compatibility with the existing mechanical flange interfaces is key for the mechanical engineers. Most of the technicians and engineers have created, in their CAD tools libraries, and standard mounting interfaces, parts like flanges, bells, fixed hole patterns etc.

The encoder flanges and stator couplings should be completely compatible with legacy products. “Euroflange” 58mm, Synchro flange 58mm, Tacho-flange for

tachometer generator replacement, stator coupling 58mm (hole pattern 63mm and 64mm), stator coupling 90mm are some examples concerning the driving shafts, the standard mandates for the SIL3 and strongly recommends in SIL2 to have positive locks. The better the encoder is coupled to the shaft the less risk for sliding between the shafts occurs. Positive locks provide the best coupling solution for securing the rotating elements, even if a clamping ring, for example, is not properly tightened by an installer or during maintenance operations. Having this redundancy between operators and secured mechanical locks make the mechanical system more secure. Providing an option with a secured insulated reduction sleeve helps to protect the encoder bearing from leakage currents in many motors driven by inverters or heavy DC motors, and increases the operating life.

These encoder safety mechanics including a keyed shaft drive, insulated secure sleeve, and unique positive shaft locks enhance installation reliability.

One part number for a range of safety levels

During the risk assessment of a complete system, different levels of safety areas are defined. A few areas will require the highest rating, but in most areas a SIL2/PLd rating would be sufficient. So, does it make sense to have another part number for each zone? If the encoder has the capability to achieve - regardless of configuration - the highest level, then it is always suitable for a lower level without question – no need to recalculate the safety level. Digital electronics today have the same achievable safety figures (PFH) compared to the prior analog ones. Safety encoders account for less than 1 % of the total admissible PFH value in SIL3 loops. This creates many avenues for achieving the safety architecture targets.

Jean-Marc HUBSCH
Functional Safety Manager
Engineering Manager- Encoders
Sensata Technologies

About BEI Sensors
BEI Sensors specializes in speed and position sensors for extreme applications. With an extensive product offering including optical and magnetic encoders, Hall effect sensors, and potentiometers, BEI Sensors offers standard configurations to completely customized solutions. Through uncompromising quality, performance, and reliability, BEI Sensors upholds a standard of excellence in its products, customer service experience, and commitment to being a global leader in sensor technology.

BEI Sensors is a brand of Sensata Technologies

www.beisensors.com

About Sensata Technologies
Sensata Technologies is one of the world's leading suppliers of sensing, electrical protection, control and power management solutions with operations and business centers in 16 countries. Sensata's products improve safety, efficiency and comfort for millions of people every day in automotive, appliance, aircraft, industrial, military, heavy vehicle, heating, air-conditioning and ventilation, data, telecommunications, recreational vehicle and marine applications.
For more information please visit Sensata's website at www.sensata.com.

Sensata Technologies - BEI Sensors SAS
9 rue de Copenhague
Espace Européen de l'Entreprise-Schiltigheim
BP 70044 - 67013 STRASBOURG Cedex France
Tel: +33 (0)3-88-20-80-80 | Fax: +33 (0)3-88-20-87-87
email: info.beisensors@sensata.com