Sensata Technologies

WHAT DO INDUSTRIAL ENGINEERS NEED TO KNOW ABOUT FUNCTIONAL SAFETY?

WHITE PAPER

How Functional Safety can improve product reliability, reduce manufacturing downtime and expand your market.

-By Scott Orlosky and Jean-Marc Hubsch, Sensata Technologies

Engineers designing systems for industrial and factory applications are adopting functional safety design practices to reduce the risk of system failures that could result in costly damage or injury. In addition, adhering to functional safety processes can help expand a manufacturer's market and customer base worldwide.

Protecting systems' operators from the potential for major injury is an imperative understood on both sides of the Atlantic. While safety standards are unified under an international umbrella, adoption rates have been slow as manufacturers and system designers consider which set of standards they should follow and which will give them the greatest competitive advantage.

While Functional Safety is mandatory in systems design in the UK and Europe, driven by European Directives EN ISO 13 849-1 and EN 62061, in the US, a different set of safety rules apply. To understand more, it is helpful to explore the European Standards that came into force in 2012.

THE EUROPEAN DIMENSION

The European Commission machinery directive stipulates that machinery should not have unacceptable risk. In the real world, of course, zero risk can never exist, but what the directive endeavors to achieve is a level of acceptable risk given the environment.

Crucially, if safety is dependent on control systems (encoders, sensors etc.), then these systems must be designed so that the probability of functional faults is sufficiently low. If this is not possible, any faults that do occur should not lead to the loss of the safety function.

In the past, the safety-related parts of a machine control were designed in accordance with EN 954-1 based on the calculated risk. However, with the emergence of new and more advanced hardware and software components, the standards of measuring and monitoring safety had to be upgraded. Today, the core Functional Safety standard is IEC/EN61508 and includes several detailed standards relating to specific areas of manufacturing and design, most notably EN ISO 13849 and IEC/EN 62061.

EN ISO 13849-1 (written with specific reference to machinery safety.) 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. These parts may include but are not restricted to relays, valves, position switches, PLCs, motor control units, pressure sensors etc. The

performance of a safety function is described by the term Performance Level (PL), with a safety rating categorized between the low “a” and highest rating “e”.

IEC/EN 62061 (written with specific reference to electrical/electronic components.) This standard defines the requirements and provides the recommendations for the design, integration and certification of safety-related electrical, electronic and programmable electronic control systems for machinery. The performance of a safety function is described by the term Safety Integrity Level (SIL), categorized between 1 and 4, where ‘4’ is for the most complex, plant-level systems in the highest risk environments. (For the purposes of this article, we shall satisfy ourselves with

Figure 1 - FUNCTIONAL SAFETY LEVELS IN TERMS OF RISK

PFD (Probability of Failure on Demand)	PFH (Probability of Failures per Hour)	SIL EN 61508 EN 62061	PL EN 13849-1	Risk reduction factor
$10^{-2} < PFD < 10^{-1}$	$10^{-6} < PFH < 10^{-5}$	1	b,c	10 to 100
$10^{-3} < PFD < 10^{-2}$	$10^{-7} < PFH < 10^{-6}$	2	d	100 to 1000
$10^{-4} < PFD < 10^{-3}$	$10^{-8} < PFH < 10^{-7}$	3	e	1000 to 10,000

The concepts of Safety Integrity Level (SIL) and Performance Level (PL) describe the capacity of the control system, in terms of safety, to reduce the risk factor.

BASICS IN SAFETY DESIGN

Levels 1 – 3, as applied to industrial machinery.)

Designing safety into industrial applications is typically a combination of the measures taken by the engineer during design and development, and those implemented by the user once the system is installed and operational.
Measures taken during the initial design phase are always preferable, and usually more effective, than those taken by the machine operator. (That said, the retrospective replacement/refurbishment of control systems with safety-rated/certificated components can now be easily achieved, as we shall see.)

Design Considerations

Whether the measures are taken before the system is designed, or after it has been installed, the design has to take into account the following factors:

- Establishing the limits and the intended use of the machinery.
- Identifying the hazards and any associated hazardous situations.
- Estimating the risk for each identified hazard and hazardous situation.
- Evaluating the risk and deciding on the need for risk reduction.

A key part of reducing risk requires defining the machine’s safety functions. This includes the safety functions of the control system, for example to prevent the machine from starting unexpectedly, over-speeding, running too slow, etc.

It is similarly important to recognize that a machine has different operating states (e.g., automatic and setup modes) and that the protective measures in these different modes may be completely different. Indeed, it might be that to achieve the levels of safety required, one or more safety-relevant control parts and several different safety functions are included, based on the operating mode.

Industry Applications

Consider, for example, a conveyor application, where the initial line of ‘protection’ could be a sensor that detects when a person is within eight feet of the machine. Rather than completely shutting the conveyor down, the controller first reduces the speed of the conveyor to reduce the risk. Production is therefore maintained, without compromising safety.

In a bottling plant, for example, designing in Functional Safety could enable the speed of the bottling line or the torque to be adjusted to a ‘safe’ level while a brief inspection can take place, or a repair carried out, without production being called to a halt. Similarly, on a printing press, implementing Functional Safety could enable the rollers to be cleaned with little or no real interruption to production and – crucially – little or no risk to the operator.

Within the timber trade, Functional Safety designs are critical to the operation of semi-automated tree harvesting and debarking systems and machinery, and in the speed and positioning of lumber to be sawn. The same is true within steel ,mills, for the safe and accurate pouring of molten steel and the shaping and rolling of ingots and steel plates.

In escalators and moving walkways, speed sensors are vital, and so too in elevators where position control of the

cab and accurately determining weight and maximum loads is essential. In the most recent applications, specifically the emergence of co-operative robots (or 'cobots' as they are sometimes known), the ability for a robot to co-operate effectively with a human counterpart is entirely dependent on safety – notably the ability to register contact and/or reduce the amount of force being applied.

In all of the industries and applications highlighted above, designing in appropriate levels of Functional Safety will help prevent serious injury or even death.

Sensors that detect rotary speed are a common component found in systems that are Functional Safety rated. An incremental encoder that accurately measures the speed and direction of an Automated Guided Vehicle (AGV), for example, for moving product in and around a warehouse or production line, can be part of a system that regulates speed, direction and motor torque and ensures the safety of the people working alongside this equipment.

Using Certified Products

Using components that are themselves certified to a specific Safety Integrity Level (SIL) by one of the recognized certification bodies, such as TUV Rheinland, enables users to achieve the system safety level requirements simply, effectively, and in the quickest possible time. They need only to feed the relevant data into the SISTEMA software (available free on the internet) for a final safety level to be calculated and recorded. Standard products that are not individually safety rated can be used, of course, but may limit the designers to a lower level of safety rating for the system, or require a thorough and independent analysis of the system and slow the speed with which the system can finally be brought to market.

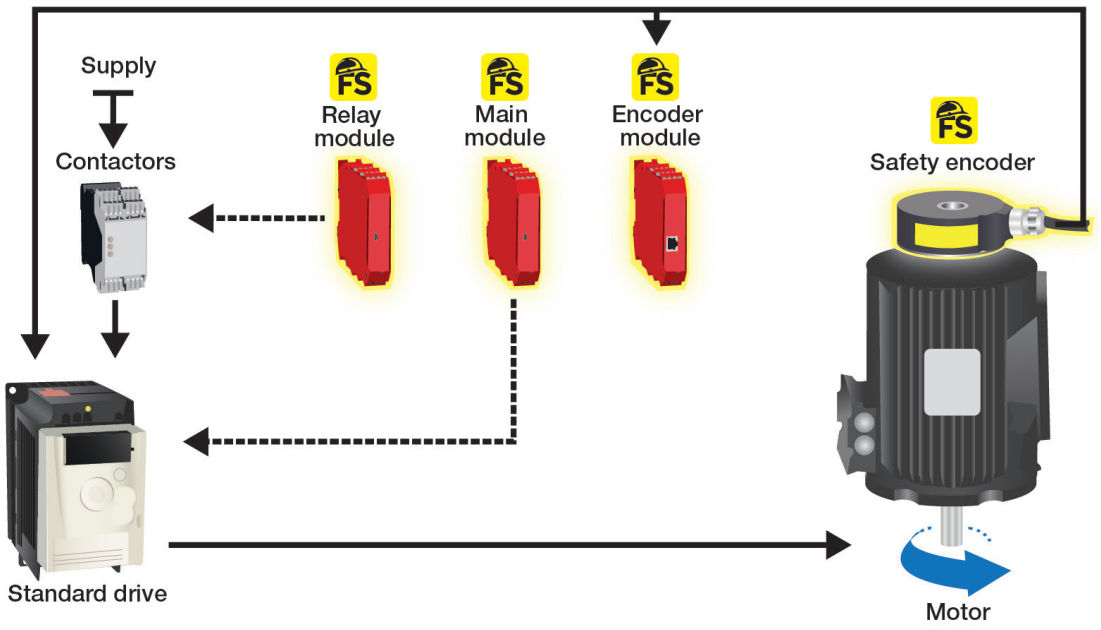
Using certified products makes it easier for engineers to calculate and accurately claim a safety rating for a system overall, as well as providing important data such as a Mean Time to Failure. It also reduces the work (and cost) required of the OEM in designing Functional Safety as a machine upgrade.

Figure 3

Incremental encoders like Sensata's DSM9H which are rated up to SIL3/PLe Cat.4 and offer a wide variety of ouputs, including analog Sin Cos or digital TTL and HTL output, allow for more flexibility in safe system design.

Sensata achieved the highest level of safety for industrial equipment (to SIL3) for its incremental encoders, including those with analog Sin Cos outputs and digital TTL and HTL outputs. With TTL and HTL output encoders, designers have a product technology that is compatible with most of the existing sensors on the market, giving designers greater choice and flexibility, especially when it comes to refurbishing/upgrading existing systems. Engineers can

Figure 2 - MODULAR SAFETY SOLUTION EXAMPLE



Products such as encoders and safety modules that are certified for functional safety can easily be used to retrofit existing equipment to allow for a modular safety solution that raises the system's safety level up to SIL3/PLe.

simply swap out older components for new, and in doing so immediately improve a system's overall Functional Safety level. These newer components are often more sophisticated and a single device can sometimes be used to perform tasks that previously may have required multiple devices to achieve the same level of safety.

In the example of a metal forming press, a number of control technologies may be required including cameras, switches, proximity detectors etc. By using encoders with a Probability of Failure per Hour (PFH) at the higher end of SIL 2, additional components of a lower SIL, but on the cusp of SIL 2, can be added without compromising the system's overall SIL rating. The overall PFH 'value' of every component gives the machine its Functional Safety rating.

Sensata's incremental encoders ensure this 'value' is kept within the boundaries desired, delivering HTL/TTL digital outputs that accurately define the resolution of the device. Besides position tracking, incremental encoders can also be used to determine velocity – an essential measurement in a potentially hazardous metal-stamping environment.

Sensata's extensive range of safety encoders include products that can be used in some of the most demanding and hazardous outdoor environments, including offshore and marine. They are washdown and IP certified accordingly.

THE FUNCTIONAL SAFETY ADVANTAGE

At a commercial level, bringing system design into line with global norms will enable manufacturers to better market their machines and compete worldwide.

The advantages of adopting Functional Safety are not simply about protecting people, the equipment, and the environment in which they operate; they are also about how Functional Safety design improves productivity, enabling systems to continue to operate while minor maintenance or repairs are undertaken.

Of course, any change to an existing engineering and design process adds cost, but with the new generation of sensors, encoders and controllers now available, engineers have the building blocks to create a safer system with comparative ease and only minimal cost. Existing systems can also be easily upgraded to achieve a higher level of safety without having to design from scratch.

Best practice in Functional Safety will not simply be driven by the need to conform to industry standards and to protect against accidents. Functional Safety also drives a more effective and productive operation, reducing downtime and costly repairs to often expensive equipment. Manufacturers that adopt Functional Safety into their processes and equipment will have the advantage of an internationally-recognized safety rating that enables their solutions to be sold on a global stage.