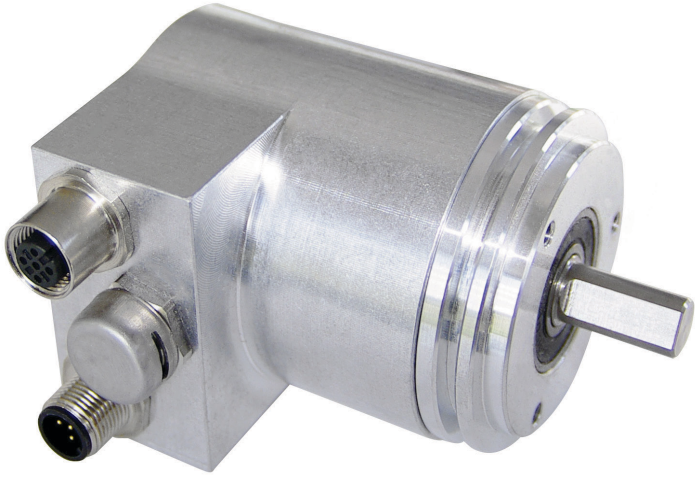
POSITAL

WHITE PAPER

Safety First - Selecting the Right Position Sensors for Safety-Related Motion Control



For safety-critical applications, motion control systems must be able to trust the position feedback that it receives from encoders and other sensors. If a sensor malfunctions, the controller must be able to quickly recognize the fault and take appropriate action. Component failure can be detected more readily if there are redundant feedback channels in the control system. If the control system receives similar signals from two different sensors set up to measure the same mechanical property, it can reasonably assume that both are functioning properly. Discrepancies between the readings would signal a fault. This paper discusses several strategies for implementing redundant feedback channels in motion control systems and weighs their relative strengths.

Join our Network!

www.posital.com

Enhanced Safety Through Redundant Feedback

For safety-related equipment, the motion control system should operate in a fail-safe manner. That is, the system should be able to detect faults in the encoders and other sensors that provide position feedback and take appropriate actions to bring the machinery to a safe condition.

A widely used strategy for ensuring that information from sensor is trustworthy is to build redundancy into the control feedback loops. For each safety-related action of the machine, (e.g. rotation of an elevator's cable drum, movement of a robot's arm, or extension of a crane's boom) two or more semi-independent measurement systems would be installed to monitor the same mechanical motion. This enables the control system to detect sensor errors and avoid dangerous loss-of-control situations. Duplicating each element of the feedback loop by adding extra encoders and communications cables will achieve this goal, but at the price of extra expense and increased mechanical complexity. The additional components will also take up valuable space in complex machinery.

Safety Certified Encoders

An alternative approach is to use special 'safety certified' encoders. This type of encoder has two measurement modules installed in a single housing, sharing the same input shaft. A signal processing chip compares outputs from the two modules and – for most devices of this type – shuts down measurements and issues an alarm signal if a discrepancy is detected. Redundancy, in this case, is built into the encoder. Encoders with these characteristics can be designed to comply with Safety Integrity Level (SIL) or Performance Level (PL) standards. (See sidebar for a summary of safety standards.)

An advantage of safety certified encoders is that they can simplify the development of safety-critical systems. The control system will receive either reliable position data, or a clear signal that the encoder has developed

a fault. However, this approach can be inflexible when handling failure situations: if the sensors simply switch off, the control system has little guidance as to how to transition the machinery to a safe state.

Certified devices can be significantly more expensive than 'ordinary' encoders largely because of the cost of certification by an independent testing laboratory. And, while these devices eliminate the need for doubling the number of encoders installed, they are only available in a limited number of mechanical configurations.Machine builders may be obliged to modify their designs to accommodate these sensors.

Diverse-Redundant Encoders

A new type of encoder introduced by POSITAL provides a middle ground between complex duplicate encoder installations and expensive safety certified devices. Diverse-redundant encoders have two measurement modules built into a single housing, sharing a common shaft. However, unlike their SIL or PL-certified counterparts, diverse-redundant encoders do not compare the output from the two measurement channels. Instead, both output signals are transmitted

About Safety Standards

There are several international standards that address functional safety in machinery or control systems, including:

- IEC 61508: Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems
- ISO 13849-1: Safety of machinery —a safety standard which applies to machinery control systems that provide safety functions.

These standards address different areas of concern and are not always consistent in detail. There are, however, important common themes:

- While absolute safety is impossible to achieve, including special design features (termed "safety functions") can reduce risks to acceptable levels.
- The need for special safety functions depends on both the probability of something going wrong and the potential consequences of an accident/failure.
- To be effective, safety functions must meet reliability standards (performance levels or safety integrity levels) that are appropriate to the level of risks and consequences.

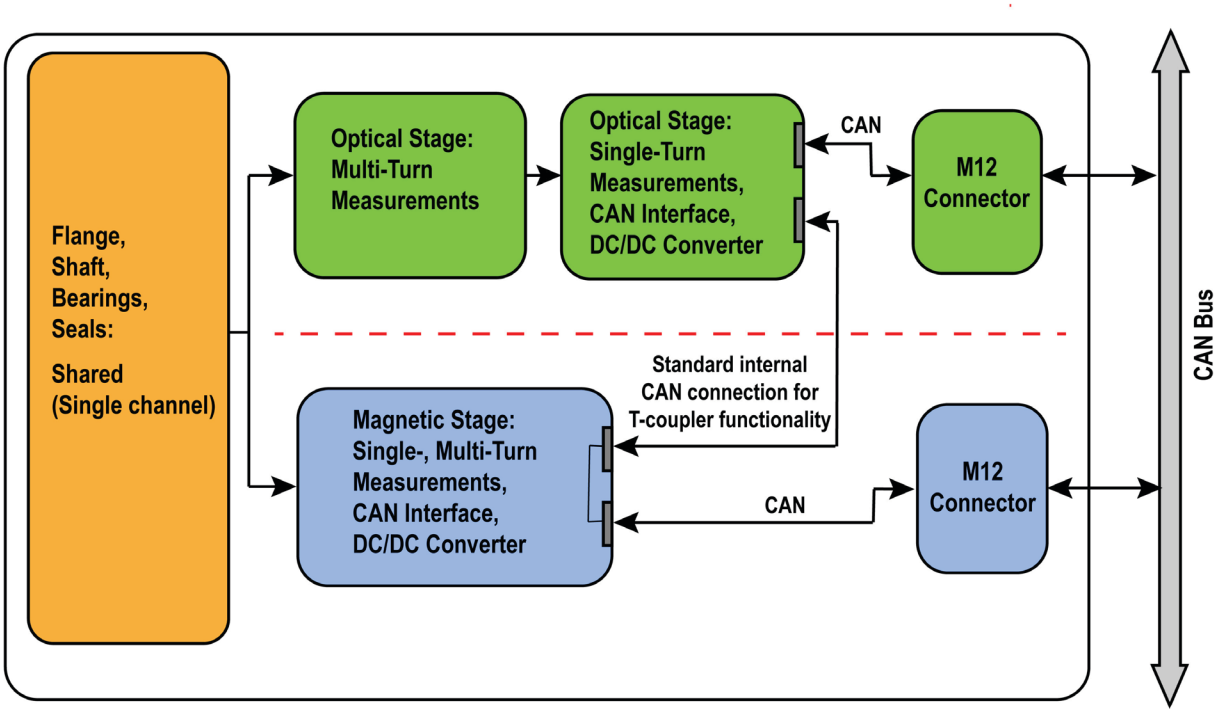
In ISO 13849-1, the level of reliability required for a safety function is defined in terms of a performance level, ranging from PL a to PL e. If, for example, accidental malfunction could cause a serious injury to a person who frequently works close to a piece of machinery, the standard requires that the machine and its safety systems have a performance level of at least "PL d". To achieve this performance level, MTTF (Mean time to dangerous failure), DC (diagnostic coverage) and Cat. (system architecture category) must all reach defined thresholds.

In IEC 61508, performance requirements are defined in terms of Safety Integrity Levels (SIL), ranging from SIL 1 (for situations with low risk and moderate consequence) to SIL 4 (high risk, serious consequences). SIL 2 is approximately equivalent to PL d and requires a similar level of reliability in safety functions.

directly to the controller (PLC, or control computer) to be evaluated there. This arrangement simplifies machine layout, since there is only one device to install for each control loop. And, since these devices are not formally certified, they are less expensive than their SIL-rated counterparts. They are also available in a greater variety of mechanical configurations.

An important feature of diverse-redundant encoders is that two different measurement technologies – optical and magnetic – are used for the two measurement modules. This improves diagnostic coverage and reduces the possibility of common cause failures. Both measurement systems are based on well-established encoder technologies designed to operate reliably over a wide range of temperatures. As well, both measurement channels feature battery-free multi-turn rotation counters for zero-maintenance operations. Diverse-redundant encoders are available with a wide range of mechanical options that include aluminum or zinc-coated steel housings, environmental protection up to IP66/IP67, multiple connector types and a variety of shaft and flange designs.

Diverse-redundant encoders support CANopen communication protocols, with J1939 connectivity under development. The CAN controller would "see" two separate devices, measuring the same rotary motion. The controller is responsible for comparing the measurements and deciding whether they are reliable.



Block diagram of a diverse-redundant encoder

POSITAL

WHITE PAPER

Does the lack of device certification put an extra burden on machine builders to prove the safety of their products? The answer depends on the complexity of the design. Even if certified components are used in the design, certification of the complete machine requires an end-to-end assessment of the design, including the way in which the control system handles component failure. Shifting responsibility for fault detection from the device to the controller may require only a minor increase in programming effort.

ISO13849 allows the use of non-certified redundant devices in safety applications, provided there is an end-to-end assessment of the design. By making the controller responsible for the verification of the two measuring channels, instead of the sensor, the designer has more flexibility in responding to the requirements of the application. If it is possible to determine which channel is faulty through a plausibility check, then the machine could be transitioned to a restricted operational mode, relying on information from the surviving encoder. If an impact analysis permits, the system can be kept running – possibly with manual override – until the faulty components are replaced.

Which Approach is Best for My Application?

For simple systems with few motion control feedback loops, the use of duplicate, redundant sensors can be a cost-effective choice.

For one-off or low volume products developed under tight time constraints, the convenience of working with SIL or PL-certified encoders (reduced development times, less safety knowledge required) might outweigh the extra cost and limited availability of these devices.

For many projects, diverse-redundant encoders

can provide a best of both worlds solution. There is only one device to mount on the machine, reducing complexity and space requirements. Meanwhile, the two independent measurement channels provide a sound basis for building machines that can be certified to Performance Level PL d, Cat. 3, according to ISO 13849.

With duplicate feedback loops or diverse-redundant encoders, the control system might be able to use other system knowledge to make a reasonable assessment as to which of the redundant measurement system is malfunctioning and whether the surviving system can be relied on to provide useful position data. In this case, the designer might be able to implement a restricted operating mode to extend the availability of the machine for a limited time. In any case, replacement of the defective device would be an urgent priority.