Decision support for functional safety encoders

If to use certified or non-certified functional safety products for safety-related applications is a hard question. In this article several technologies used in encoders are explained.

Figure 1: Application areas for the encoders are for example an aerial ladder (Source: Fraba)

Today, engineers have the choice of using certified or non-certified functional safety products for safety-related applications. This choice is not easy, and the task is likely to be influenced by considerations such as the availability of products, their cost, and the required integration effort. As well, the ability to react quickly to end-customer demands for machine adaptation can be critical to the final decision.

Fraba has extensive experience in the development of safety products. In 2009, the company introduced their first SIL3 / PLe-rated encoders with a CANopen Safety interface. This encoder was based a redundant design, with duplicate optical measurement systems. By comparing the output from these two systems, the device's primary micro-controller (MCU) could detect errors or component failure with a sufficient level of certainty to meet SIL3 requirements. This system was implemented with a pre-certified micro-controller running the CANopen Safety stack. A second small MCU provided a monitoring function. With two redundant measurement modules, these devices were slightly longer than the company's standard optical encoders and more expensive. However, these devices offered important advantages over the use of two standard encoders to achieve redundancy, eliminating the need for duplicated couplings, mounting brackets, and cables. SIL3-rated encoders were available in single or multi-turn versions.

More recently, Fraba developed a second generation of safety encoders as successor, designed to meet SIL2 / PLd requirements. These are based on magnetic measurement technology, which is less expensive than optical systems and better suited to harsh environmental conditions. They feature two redundant Hall sensors. These sensors measure the rotary position of a single magnet mounted on the encoder's shaft and mechanical gearing. There are several MCUs that carry out signal conditioning for the two position sensor channels and verify the position values read by the two channels. Both single-turn and multi-turn models are available with CANopen Safety interface and Profisafe interfaces. CANopen is widely used for mobile and construction machines while Profisafe is important for manufacturing automation.

A main advantage of the two encoders series described above is that they are easy to integrate into safety-critical systems. The engineer can "trust" these safety-certified devices and the position values that they produce, leaving users to focus on the remainder of the application task. On the other hand, this ease of use has the drawback of reduced flexibility when handling failure situations. These sensors simply transmit an error code and switch off when a measurement discrepancy is detected. Safety requirements are fulfilled, but availability is gone. Customer specific requests for adaption build into the hardware and software, requiring extra effort for implementation, testing and documentation, is leading to less flexibility.

Ten years of experience in this market has taught us that machine builders often face enormous price pressure, especially for high volume projects. There are also time-to-market pressures that require high flexibility. In response to these needs, Fraba has developed a product series of less expensive non-certified encoders that are also suitable of use in safety-related applications. The key concept here is to build devices that combine two different measurement technologies – optical and magnetic – in a single encoder package. These "redundant-diverse" encoders implicitly qualify for a safety level of PL d according to ISO13849. Unlike the SIL-certified devices described above, comparison and verification of the measurements from these two channels is here the responsibility of the PLC logic. Is this type of encoder suitable for safety applications requiring PLd levels of ▷

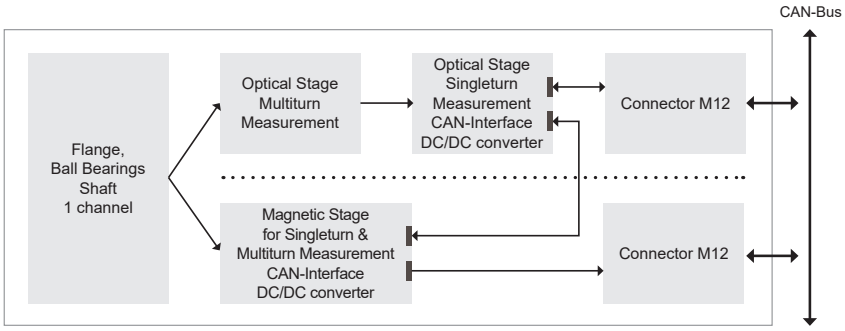

Figure 2: Block diagram of a redundant diverse encoder (Sourc: Fraba)

performance? The answer is yes, because these devices meet key performance/reliability requirements: MTTFd is high; CCF exceeds 65 points; and the overall architecture of the device meets Category 3 requirements. That means that on the PLC side a DC (diagnostic coverage) of "low" is adequate, reducing the implementation effort (e.g. to simple comparison of the two channels).

By defining of a suitable allowed deviation range between the two both position values, the engineer can optimize control system behavior to meet application requirements. In case of an obvious failure in one encoder channel, the PLC can change the machine operating mode from 'automatic' to 'with assistance' and continue to use the output of the functioning encoder channel, taking into account the fact that it is operating at a reduced level of trustworthiness. In the end, this means a higher availability than with a safety device that just turns off in the case of failure. For mobile machines like concrete pumps or aerial platforms, a level of high availability is an important requirement.

In summary, safety certified encoders are a good choice for customers using lower quantities, short development times, lower safety knowledge, and acceptance of higher product cost. However, for cases where high flexibility, series volumes, and price pressure are of prime importance, a non-certified redundant diverse encoder technology offers a lot of benefits. It's up to the customer to decide on the right technology for his application.

The Bauma 2019 exhibition takes place from 8 to 14 April in Munich, Germany. Fraba shows there its products in hall A2, stand 434.

Author

Klaus Matzker
Fraba
info@posital.de
www.posital.de