

## Safety or true safety

Functional safety is usually required in mobile machinery. TWK (Germany) has a long history in developing functional safe sensors, measuring rotations, length, speed, or inclinations, etc. The following statement by product manager, Achim Albertini, explains the difference between “safety” and “true safety”.

“You might wonder whether there is any difference at all. There is! In the functional safety sensor technology industry, sensors are often labeled “Safety.” These are sensors that convert mechanical measurements into electrical data. However, this does not necessarily reflect our understanding of safety. Our safety sensors meet very high requirements and standards, so we can rightly speak of ‘true safety’.

Therefore, it is advisable to take a close look at the safety sensors to ensure that we are using the right ones. First, let us consider the important standards that are the primary focus of this statement. The first is the IEC 61508 standard, which covers the functional safety of electronic systems with SIL (safety integrity level) classification. The second is the ISO 13849 standard, which covers the safety of machinery and safety-related parts of control systems with PL (performance level) classification. The higher the classification, the greater the reliability and the lower the probability of a fault not being detected by the component that could cause a hazard. Many of our sensors feature a SIL 2 and a PL d classification. Some even have SIL 3 or PL e. It is important that this safety level is confirmed by an official body. That is why we have our safety sensors thoroughly tested and certified by TÜV according to one or both of these standards, as required. Sometimes other standards are added, such as ISO 26262 with ASIL (automotive safety integrity level) D, in case of automotive applications.



(Source: Adobe Stock)

In order to achieve these safety levels, many design requirements must be implemented. It is also important not only to just meet the classification level (e.g., SIL 2), but to have a good buffer, as the sensor is usually a device in a transmission chain, and the entire chain must meet a certain level.

### What measures do we take to achieve this goal?

Firstly, the mechanical movement must be detected reliably and without slipping. This requires a form-fitting connection between the sensor and the moving application. Our rotary encoders offer a wide variety of shaft types to facilitate this, including solid shafts with a fitting or disc spring and hollow shafts with a groove. This prevents any twisting going unnoticed. However, for this reason, each sensor must also be firmly connected to the application by the customer.

Let's take a look inside: Our sensor technology is always designed to be redundant. The signals from the dual sensors are then compared in the control unit, which contains all the necessary firmware and software for signal processing and output (plausibility check). Only if the deviation is below a threshold value, is the signal - e.g., the shaft position of sensor 1 of a rotary encoder - output as a reliable value via the interface, for example a CANopen interface. The firmware in the control unit is designed so that all internal processes – reading data, calculating, transmitting and storing intermediate



values, etc. – are secured with CRC checksums. Additional testing and control processes, known as double checks, enable functionally safe operation. For instance, the limit value relays in the SIL-2 cam switches and vibration sensors are continuously checked to ensure they are in the correct switching state. SIL 3 goes even further: the signal-processing controllers are designed with redundancy.

### More questions

Are all supply voltages within the target range? Are the RAM and ROM memory areas working correctly? Are the output drivers online?

The next step is to transfer the resulting data, i.e., angle and speed data or acceleration and inclination data. This transfer is performed twice in CANopen Safety: via normal and inverted bit patterns immediately one after the other. Parameterization data for the sensor is always secured with a checksum. This type of transmission ensures that the safe measured value determined by the sensor also arrives safely in the host controller. 'Safe' means that the probability of an undetected error is very low, as approved according to the SIL/PL classification. This means that the risk posed by the system or machine is very small, but cannot be eliminated entirely.

However, it is not only the finished sensor that is subject to strict rules in order to meet safety criteria, but the entire development process as well. Before and during

the development of a new safety product, all requirements that must be met are determined. To ensure functionality, all associated test procedures - the test cases - are also formulated. This can involve several thousand individual processes in order to capture all characteristics. Only this meticulous approach leads to a safe result.

The aim of all measures is therefore always to prevent malfunctions and, if a malfunction does occur, to detect it as quickly as possible. If incorrect behavior is detected, the sensor immediately switches to a fail-safe state. This means that an error is sent to the control system (status bit) and the sensor stops transmitting data. All safety relays (if present) open. The safety controller responds by transferring the system or parts of it to a safe state in order to prevent damage.

Our safety sensors meet very high requirements and standards, so we can rightly speak of 'true safety'.

*Achim Albertini (Product Manager at TWK)*

As an established family business, we began designing safe sensors a long time ago, and our experience and know-how in this area has rightly earned us a strong market position. That is why we continue to do what we do best: developing and producing functionally safe sensors – true safety.”

# BY ENGINEERS, FOR ENGINEERS

We take pride in offering solutions for CAN that work 'out of the box'.



**CanKing 7**  
Kvaser's free next-generation bus analysis software



**Loggers & Edge Devices**  
CAN-based logging and edge computing



**PC Interfaces**  
Easily connect CAN to your computer



**Gateways & Bridges**  
Reliable wireless alternatives to CAN cabling



**Embedded Interfaces**  
Industry-leading embedded CAN interfaces



Explore our world  
[kvaser.com](http://kvaser.com)

**KVASER**  
Advancing connectivity