Safety CAN: Why and how?

Why should a safety-related CAN protocol be used? Is it necessary? And if so, which protocol is the most feasible? We take a look at where the demand for safety protocols comes from and at existing technical solutions.

If you want to place a product like a machine or a vehicle on the market, you have to consider the legal requirements. Those are specified in national laws like the Product Liability Act or European directives like the Machinery Directive or the Regulation for Vehicle Type-Approval. All of them refer to state-of-the-art technology, which is described by the harmonized product or sector standards. For any kind of machine with safety-related parts of a control system, the most commonly used standard is ISO 13849. Concerning data communication, it refers to IEC 61508-2, providing a choice of two data communication architectures. With the White-Channel, the entire transmission path has to be developed compliant to the standard, whereby with the Black-Channel, only the endpoints are considered safety-relevant and the transmission is protected via a safety protocol. In both cases, for non-rail applications, IEC 61784-3 "Functional safety fieldbuses" is referred to, whose principals have been implemented for example in the CANopen Safety standard EN 50325-5.

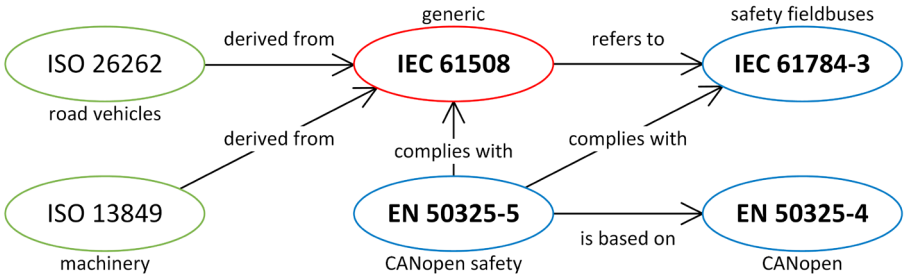

Figure 1: Relationship of the relevant standards (Photo: STW)

For road vehicles, ISO 26262 defines a number of techniques to reach the required diagnostic coverage for a communication network like CAN. Those are for example information redundancy, timeout monitoring, or frame counter, which are needed to detect faults like corruption of information, delay of information, or loss of information. Even if the standard does not explicitly claim a standardized protocol, especially the interconnection of parts or systems of different manufacturer makes the use of common protocols more efficient than investing in a proprietary solution. However, what are the use cases for those protocols? Let us have a look at a simple application: A sensor measures pressure and the data is processed by a control unit. At the end of the control path there is some kind of actuator on the machine or vehicle, like a pump switch, which is regulated by another control unit. The units are interconnected by a bus system. The hazard and risk analysis orders the pump to switch off if the pressure exceeds a threshold value. In consequence, you have to build a safety function by using a highly reliable or safety-related sensor and actuator as well as two safety-controllers. But how do you ensure that the switch-off signal is transmitted reliably? You could wire an additional safety-related signal line between the control units or you use the existing non-safe communication channel in combination with a safety protocol.

As CAN is still a widespread bus system in the industry, let us have a look at the technical solutions for this standard. With the rising need for safety-related CAN communication, several companies have come up with ideas on how it can be realized. As an example, Pilz developed Safety BUS p, which is an event-driven CAN protocol and primary used in fabric automation. By adding additional measures to the OSI layer 2 and 7, it is made suitable for safety applications up to SIL 3 according to IEC 61508. Transmission errors and device errors are detected by a combination of sequential numbers, timeout detection, echo check, IDs for transmitter and receiver, as well as data protection with CRC.

In 1993, the CANopen protocol was developed within a European research project under the chairmanship of Bosch. Because this OSI layer 7 protocol – also known as the CiA 301 specification – was very successful, it was enhanced to CANopen Safety (CiA 304) for safety-related automation applications up to SIL 3 according to IEC 61508. An additional message object makes it possible to transmit safe and non-safe data on the same communication line. The safety-related data object (SRDO) consists of twice the same data but once inverted. The two ▷

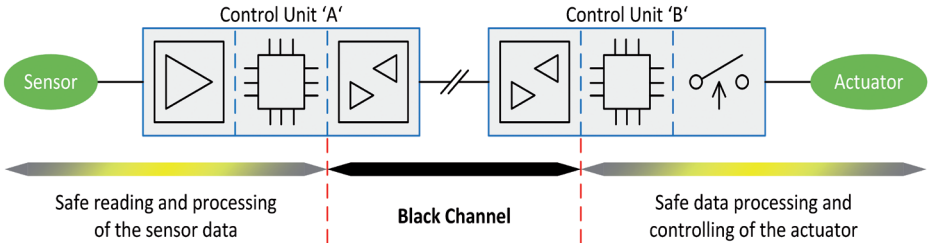

Figure 2: Example of a safety function (Photo: STW)

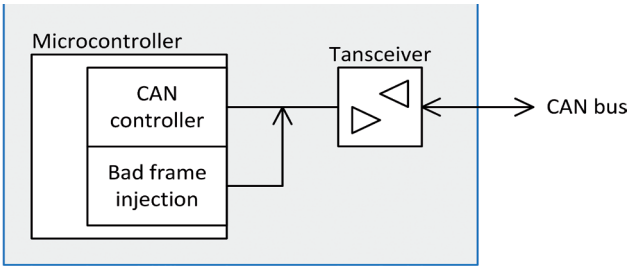

Figure 3: Bad frame injection to test the CAN controller (Photo: STW)

CAN messages of an SRDO have to be transmitted within the safety-related validation time (SRVT) and periodically within the safeguard cycle time (SCT).

One problem of this protocol is the CRC of the CAN messages being part of the safety mechanism and therefore its integrity has to be guaranteed. This is why the receiving part has to provide a redundant CAN controller, because it is supposed that the CRC calculation might be corrupted. This has been implemented for example on the CANopen Safety chip CSC01 and its successor CSC02 by Systec Electronic on the basis of a 16-bit micro-controller. Although the marketing of the chip has been stopped, the technical principal is still state-of-the-art. Sensor-Technik Wiedemann has found a solution to omit the second CAN controller through a test of the CRC mechanism. For this purpose, at start-up a corrupted CAN frame is injected into the receive line, to check if the CRC hardware finds the error. With this measure, SIL 2 according to IEC 61508 can be achieved.

Another problem of the CANopen Safety protocol is that the two CAN messages of the SRDO lead to a heavy busload if many participants are sending on the bus. Therefore, Sensor-Technik Wiedemann has developed an optimized CAN safety protocol named ESX CAN efficient Safety (ECeS). The concept of this protocol is that only six of the eight data bytes of a CAN message are used for information. The remaining two bytes contain a message counter and an 8-bit CRC with a suitable hamming distance. Together with a defined SCT and the bad frame injection test, this protocol can be used for safety applications up to SIL 2 according to IEC 61508. The data throughput of ECeS exceeds CANopen Safety.

At this point of our examination, we can already say that using a safety-related CAN protocol is not an option but mandatory for CAN applications with requirements on functional safety. The type of protocol mainly depends on the kind of application and especially on the question, which and how many other participants are involved in the safety function, and which protocol is implemented or can be implemented on them. ◀

Author

Philipp Luger
Sensor-Technik Wiedemann
info@sensor-technik.de
www.sensor-technik.de