CANopen Safety in mobile machinery

The demand of exchanging information in mobile machines increases constantly. More sensors provide a broader and more precise feedback. All this information must be made available at places of the machine and to the outer world.

For many years, communication in mobile machines was dominated by either CANopen or the CAN-based J1939. Two major trends have made it necessary to look over the fence and consider alternatives at least for a part of the communication tasks. One is the requirement of safe communication for safety functions set forth in the EN ISO 13849 and detailed in revised C- standards. The other one is the increasing volume of data, which can be logging data, data for different setup conditions or simply for much bigger PLC programs. Which role can CANopen Safety play to support these demands and what are its limitations?

Allocation of roles

With the increasing number of tasks and requirements it becomes necessary to allocate the right bus system at an early stage. Especially as nowadays more options than just CANopen and J1939 for communication are available. More and more mobile machines utilize Ethernet and USB besides CAN-based communication. Now, what does a typical allocation of communication tasks look like?

CANopen still plays the leading part in cyclic communication between sensors, actuators, nodes, and the PLC as long as no safety functions are involved. Furthermore the communication between PLCs (cross communication) and from PLC to displays is CANopen-based. The bandwidth for this kind of communication is sufficient, the availability of CANopen components meeting mobile machinery requirements is unsurpassed, it is widely spread and well known in the industry, and the protocol has proven its robustness.

CANopen Safety comes into the picture if safety functions are involved which cannot be addressed by CANopen. Although the data throughput is limited compared to CANopen due to the two data frames being sent instead of one, CANopen Safety has become the standard in safe communication in mobile machines. Meanwhile other alternatives of implementing safe communication via CAN have become available. Although they may have their advantages in some areas, one important point is missing. As these approaches are proprietary, the opportunity of selecting the best product from different vendors for a specific task got lost. In contrast, CANopen Safety has become a per se standard in safe communication of mobile machines, as no other safe fieldbus provides a broader range of mobile suitable sensors, joysticks, and PLCs.

Ethernet addresses the increasing need for non-cyclic data exchange in many fields. It is the bus-system which allows a fast data transmission to or from remote servers via router. But which kind of data is suitable for Ethernet communication? Firstly, Ethernet is a preferable way to load firmware, application programs, and graphical data to PLCs and displays. It is faster and more convenient than CAN and especially as the still used EIA 232. Secondly, mobile machinery ▷

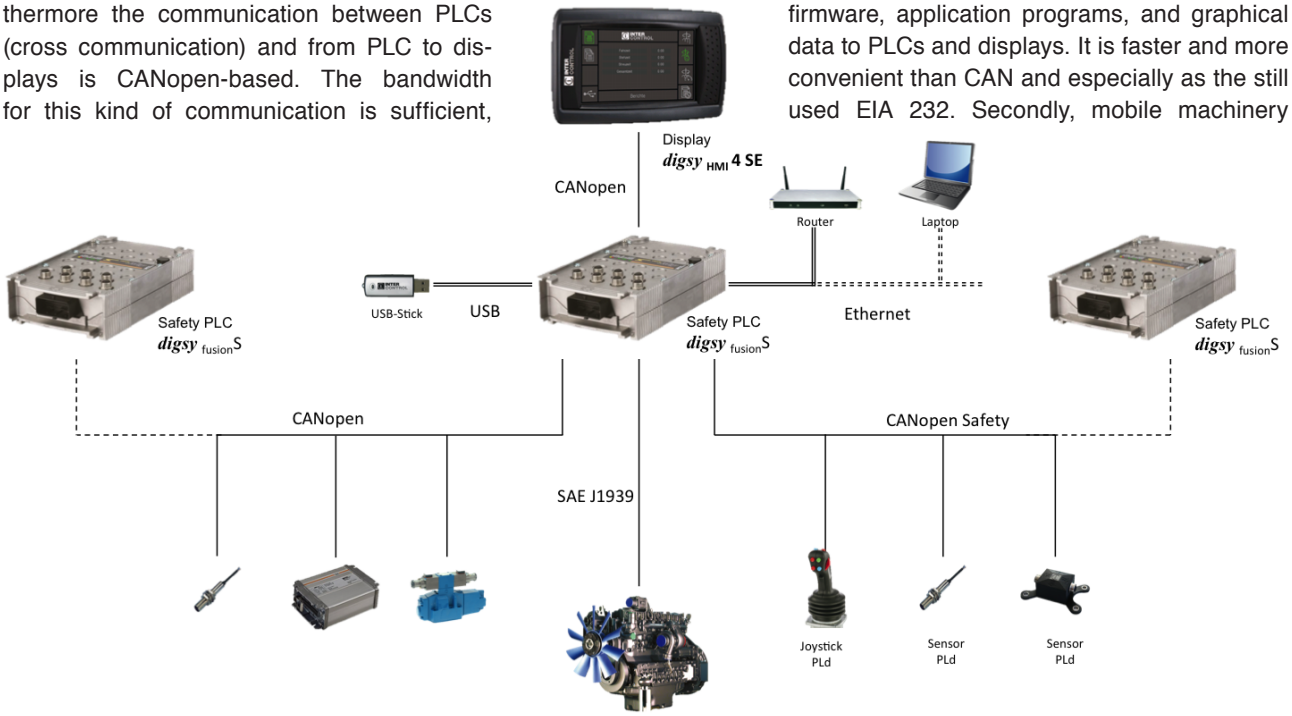

Figure 1: Exemplary communication architecture for mobile machines (Photo: Inter Control)

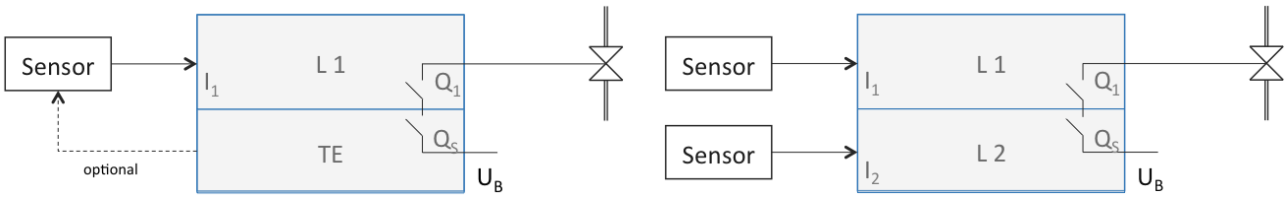

Figure 2: Category 2 and Category 3 according to EN ISO 13849 (Photo: Inter Control)

has an increasing need for set values addressing different machine modes and different set up conditions. These set values are provided as recipes, load moment tables, coordinates or others and can add up easily to more than 1 MiB.

Thirdly, mobile machines gather more and more data. Either to log their own conditions over time in PLC-based error or data log books to support technical analysis, or to collect data about the working process and to document the result of their job and to provide data for commercial statements. All this data has to be forwarded continuously or at a certain event to a database for further handling. Giving the increasing size of the collected data, CAN will be too limited for this job in more and more cases.

Although USB is not a common communication network on mobile machines, it can be a suitable interface for providing data to or gathering data from the machine. While Ethernet always requires some settings to establish the communication, a USB stick can easily be connected to a PLC or display without special preparation on the machine. The data sent or received from the machine typically has the same characteristics as the data communicated via Ethernet. With the opportunity to define the desired data exchange between PLC and USB-stick by script, mal-operation can be reduced significantly.

This allocation of tasks within the communication of mobile machines can lead to the exemplarily architecture that is shown in Figure 1. To enable such a communication structure, safety PLCs like the digsy fusion S provide four CAN networks with CANopen Safety, CANopen, J1939 or CAN protocol. Each protocol can be configured at each CAN network. Furthermore Ethernet, USB, and EIA 232 are available.

Separation of safe and non-safe programs

As CANopen Safety is based on CANopen, CANopen users can adopt it relatively quickly. Nevertheless, implementing safe communication and safe functions in a machine control system goes hand in hand with restrictions and extra effort in programming, testing, and documentation as defined in the V-model of the IEC 61508.

To reduce this extra effort to the necessary minimum, Inter Control's safety PLC digsy fusion S provides the opportunity to run two application programs – one safe and one non-safe. As a key functionality, the digsy fusion S separates the non-safe program from the safe program in a way that stops the non-safe program from interfering with the safe program. Now it is possible to limit the effort of safe programming, testing, and documenting to the safe functions by concentrating them in the safe application program. All non-safe functions on the other hand should be realized in the non-safe application program – with reduced effort.

In the digsy fusion S, all CANopen Safety messages are sent to the safe program. Although CANopen Safety should be used for communication related to safety functions, this information might also be needed by the non-safe program. Via an implemented interprocess communication, this data can easily be made available for the non-safe program.

Cross communication

Beside the classic communication between PLC and sensor or PLC and node, it might be necessary to establish a safe communication between PLCs. The digsy fusion S supports this so-called cross communication. To set up a cross communication, one PLC has to be configured as a CAN master while the other PLC has to be configured as a CAN slave. Regarding the communication, this PLC configured as a CAN slave behaves like a CAN node, but from the control perspective it maintains its entire functionality as a PLC. This master slave architecture can be extended with more PLCs configured as slaves.

Depending on the requirements of machine specific C-level standards or due to the result of a safety analysis, it could be necessary to realize a safety function as a Category 3 architecture according to EN ISO 13849 (Figure 2). CANopen Safety sends one data object with two data frames, where the second data frame is bitwise inverted and has a different CAN-ID than the first data frame. Due to this and further measures, the protocol itself supports Category 3 requirements. Besides the protocol, the hardware must be designed to meet Category 3 requirements as well. This could be realized e.g. by two CAN receivers where each receiver handles one of the two data frames. The digsy fusion S provides such means and is therefore able to process CANopen Safety messages according to Category 3 or Category 2 requirements. ◀

Author

Alexander Holler
Inter Control
Holler.Alexander@intercontrol.de
www.intercontrol.de