Safety and security requirements in mobile machines

Holger Zeltwanger (CAN in Automation)

Mobile machines are equipped with electronic control units (ECU) comprising sensor, actuating, and processing functionality. They are often networked with other devices, in particular with human machine interfaces and operator displays. Such electronic control systems needs to fulfill safety requirements and associated directives. In addition, there are security requirements protecting the mobile machines against unintended manipulation, sabotage, and unauthorized usage. Such requirements are not limited to the ECUs, but cover also the used communication technologies. The requirements of governmental authorities, operators, and machine builders are sometimes different.

In most modern mobile machines, there are network-based control systems. Many of these networks are based on CAN (Controller Area Network), an internationally standardized bus-system (ISO 11898 series) originally developed for in-vehicle networking of passenger cars. Many of them use proprietary higher-layer protocols (HLP). Increasingly standardized HLPs such as SAE J1939, CANopen (EN 50325-4), or Isobus (ISO 11783 series) are preferred.

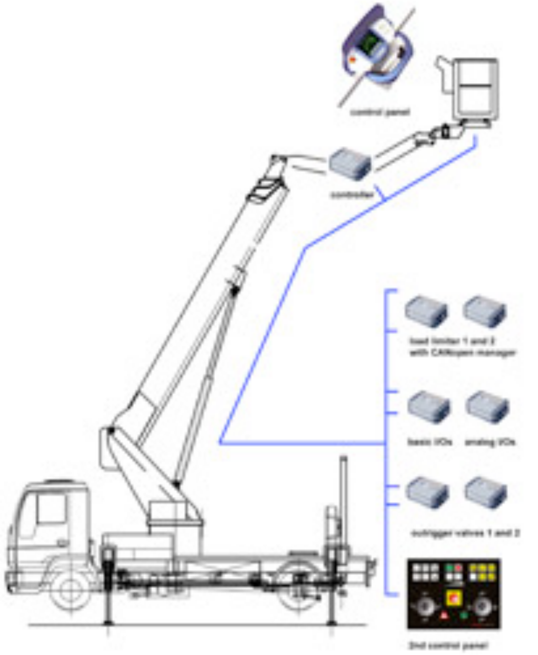


Figure 1: According to the new Machine Directive aerial working platforms requires functional safety

Mobile machines are subject of safety and security requirements. These requirements are made by customers and suppliers in order to protect the operator and the machine against harm and destruction. There are also requirements by governmental and non-governmental authorities. This includes insurances and other parties interested in the health of the operator and machine. To make it clear and address this frankly: It is money what matters. Insurances don't want to pay in case of injured people or machines. Of course, there are also general rules and laws, which take care that nobody is harmed.

European machine directive

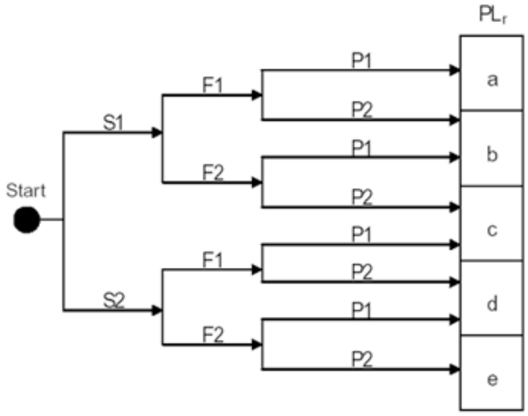
Functional safety requirements are not new. Since many years, the machine builders have to meet national safety regulations. One of the simplest safety functions is the emergency button. In critical situations, the operator or someone else should be able to safely switch-off the machine. Such an emergency switch with redundant switch elements was hardwired and was able to shut down the moving parts of the machine. In more complex machines a simple shutdown is not always the best solution. A controlled switching off is often the better approach. But this requires a safe controller, safe sensors, and safe actuators communicating via safe communication systems. In the past, safety has been regulated in the EN 954 standard, which didn't cover programmable electronic control systems.

The so-called new Machinery Directive 2006/42/EC regulates the technical requirements also for electronically controlled machines – in particular for those control systems, which are programmable. After some political delay it came into power by end of 2009. The directive references to several international standards including the IEC 61508 standard providing a general framework for developing safety-related control systems. The ISO 13849 and IEC 62061 standards specify the methodology for the assessment of risks, the conceptual plan and validation of functional safety for open-loop control systems including all relevant safety components.

SIL or PL rating

Historically, SIL (Safety Integrity Level) is often used to rate functional safety. SIL refers to the functional safety rating standardized in IEC 61508 and its numerous derivate standards such as IEC 62061 and IEC 61800-5-2.

But with the adoption of the European Union's new Machinery Directive, and its switch from EN 954 to ISO 13849, there is increasing interest among manufacturers in establishing Performance Levels (PL) for their products and systems. In both PL and SIL (if applied to machinery control systems), the probability of failures is given in PFH (probability of failure per hour). Both ratings have requirements concerning the structure, the degree of fault self-detection (built into a device), and the confidence that design faults have been avoided (called "systematic capability" in IEC 61508). The essential difference between PL and SIL are the parameters that express the degree of fault detection, the degree of redundancy, and the degree of reliability. The PL not only has a PFH, but also a reliability value for each channel inside the safety-related system. This is called the MTTFd (mean time to dangerous failure) of a channel. Because the new Machine Directive references the ISO 13849 standard, the PL rating is more or less mandatory. Of course, you can convert a SIL rating into a PL rating and vice versa. There are also activities to merge the ISO 13849 and IEC 62061 standards, which implies a comparison of PL and SIL ratings. The merging result will be the ISO 17305 standard. This will overcome the difficulties resulting from the overlapping of ISO 13849 and IEC 62061. An ISO/IEC joint group is doing the merging. The group has started its work already in March 2012.



LEGEND: S1 (slight reversible injury), S2 (serious irreversible injury or death); F1 (less often/short exposure time), F2 (frequent to continuous/long exposure time); P1 (possible under specific conditions), P2 (scarcely possible)

Figure 2: Performance Level ratings

The required Performance Level is highly political; meaning it depends on common understanding, power of involved authorities, users and operators, etc. Just a few examples, to prevent uncontrolled acceleration of a mobile machine or the transition of electrohydraulic components to safe-state are normally PL-c rated. Preventing uncontrolled movements a truck-mounted crane is typically PL-d rated.

Safe CAN communication

In general, there are many options to achieve a safe communication in CAN-based networks. One option is to use redundant control systems cross-checking each other. In case of result mismatch, the machine transits into safe-state. However, redundant networks are expensive. It even may happen that the availability is lower compared with a non-redundant bus-system. Another option is to use sufficient methods to detect any single failure (e.g. running numbers, cross-checking of redundant information, proofing timings, etc.). Several proprietary protocols have been developed. One of the first was Safetybus-p by Pilz. Most of the others invented in the 90ies were not commercially successful.

The CANopen Safety protocol was the first standardized safety solutions for CAN-based networks. It was introduced already before the millennium. Its idea is simple: Transmit the PDO (process data object) content in another PDO (using an CAN-ID different in at least two bits) with bit-wise inverted data-field and call these two data frames SRDO (safety-related data object). This SRDO made of two CAN data frames is transmitted periodically with the Safeguard Cycle Time (SCT). This time is checked by the SRDO receiving devices. They go into safe state, when this time is elapsed and no new SRDO is received. In addition, the CANopen Safety protocol stack observes the time (called Safety-related object validation time, SRVT) between the two data frames making an SRDO. If the SRVT elapses and the second part of the SRDO is not received, the devices transits immediately into safe state. The CANopen Safety protocol has been approved for SIL-3 applications by TÜV Rhineland. Note: The CANopen Safety protocol stack also needs to fulfill the required safety level. In particular, the device internal checking of the memory has to be sufficient (test coverage).

For SAE J1939-/1 there is no standardized safety communication specified. In May, there was submitted a proposal for a safe J1939 communications adaptable also for ISO 11783 and CANopen. Similar to the CANopen Safety approach, a second CAN frame is transmitted. The first CAN message is normal J1939 (or Isobus) message (called SDM = Safety data Message) containing safety signals, followed by the SHM (Safety Header Message). Both messages make the Safety Data Group (SDG). The SHM provides in the 8-byte data field a 3-bit sequence number, a 16-bit CRC (protecting the data in the SDM), and the CAN-ID of the related SDM. This approach could be also used for CANopen: The PDO containing safety process data is protected by the SHM. Of course, the SDG is transmitted periodically (SCT) and the time between SDM and SHM (SRVT) is also observed by the protocol software. TÜV South has approved this concept for SIL 2 and PL-d.

Machine builder requirements

The machine builder likes to buy safe devices from different manufacturers, in order to avoid dependencies from a single source. This means, standardized safe communication systems are needed. For the mobile machine industry, there are two higher-layer protocols established: CANopen and J1939-based solutions (SAE J1939-71 for diesel-powered vehicles and ISO 11783, also known as Isobus, for agriculture and forestry vehicles. CANopen networks are mainly used for superstructures and body electronics.

In the last years, just a few CANopen Safety controllers were available. Since this year, the number of available safety controllers featuring CANopen Safety has increased.

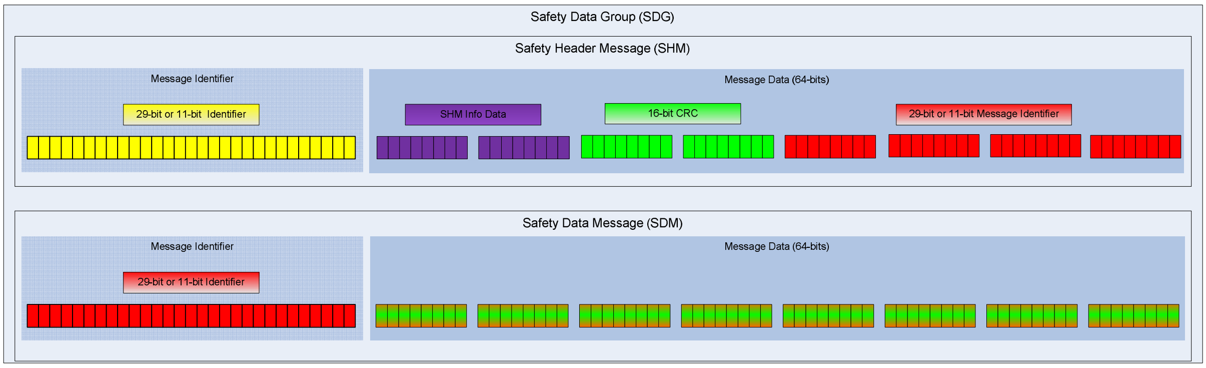

Safety Data Group (SDG)
Safety Header Message (SHM)
Message Identifier
29-bit or 11-bit Identifier
Message Data (64-bits)
SHM Info Data
16-bit CRC
29-bit or 11-bit Message Identifier
Safety Data Message (SDM)
Message Identifier
29-bit or 11-bit Identifier
Message Data (64-bits)

Figure 3: The safety protocol submitted for SAE J1939 uses two CAN messages

Also the availability of sensors and hydraulic devices supporting CANopen Safety is still limited.

The situation for the controller may become better soon, because there has been introduced a TÜV-certified PLC runtime software with an embedded CANopen Safety protocol stack, which complies to SIL 2. Also most of the already launched safety controllers are compliant to SIL 2, which is sufficient for most of the mobile machine applications.

There is no CANopen Safety conformance test plan standardized. Conformance testing is like spellchecking and doesn't guarantee any device interoperability. It just increases the possibility of interoperability. Interoperability test are much more important. The CANopen Safety starter-kit provided by one of the protocol stack providers could be regarded as the "golden" CANopen Safety slave. It uses the CANopen Safety Chip (CSC) by CiA. This is a single micro-controller implementing the CANopen Safety protocol using two on-chip CAN modules. TÜV Rhineland has certified it (SIL-3). If other CANopen Safety devices can communicate with the I/O modules provided with the starter-kit, they could be regarded as interoperable. However, an interoperability test needs to be specified. CiA will do this using the experiences from the first CANopen safety plugfest to be organized in the next month.

One important requirement from the machine builders point-of-view is the acceptance of safety-certified devices by different authorities. It should not happen that different authorities measure differently. The authorities should rate equally the devices. This should include the ratings for communication protocols and their implementations.

Device design requirements

The device providers like to have a clear situation regarding the requirements of the certifying authorities. If the authorities have different opinions on how to evaluate functional safety, it is risky to be an early bird in the safety business.

For small device suppliers or those with low-volumes it is required that there are some pre-certified safety components. This includes hardware and software. Precertified safety software would help those device manufacturers selling only low volumes. Safety PLC software and safety protocol stacks could help a lot. The same is with pre-programmed micro-controllers featuring functional safety. Unfortunately, most of the safety micro-controllers confirm with the automotive standards (ASIL as specified in ISO 26262).

From a commercial point-of-view it should be avoided that any small change in safety specifications, safety standards, and so on will require a re-certification of the product. In order to avoid misunderstanding, I don't want, that any risky behavior be implemented into components or devices or systems. On the other hand, we should be allowed to use safety-certified components or devices on the next integration level. Otherwise we delay the system design of safety machines and we increase the development time.

An example: If the ISO 13849 and IEC 62021 standards have been merged into ISO 17305 in the near future, this should not require that all already certified safety components and devices need to be recertified.

Upcoming security requirements

In order to avoid unauthorized usage of mobile machines including sabotage and stealing, the control systems of mobile machines need to implement security mechanism. This is especially necessary for equipment using embedded and open networks, which are physically accessible from outside. If open interfaces are provided (e.g. for diagnostic purposes) firewalls and authentication are required.

The Construction Equipment Association (CEA) has organized in May this year a workshop addressing the topic of security in construction equipment including mobile machines. Security strategies may be needed for agriculture and forestry mobile machines, too.

Trucks already implemented anti-theft devices as well as remote access to disable functions, when the truck has been stolen and is in standstill and has been locked.

For those security functions authentication is needed. Related methods have been already developed by IT and other industries, which can be adopted. The ISO is going to standardize the Vehicle Station Gateway (VSG). This will be a joint activity of different ISO technical committees (e.g. TC 22 and TC 207). It is a very political task, due to the commercial interest of many different parties including vehicle makers and governmental authorities as well as the IT industry.

In mobile machines, secure communication is also required for weight measuring such as in refuse-collecting vehicles, etc. In some applications, the unloading of garbage should be recorded securely by means of GPS data, in order to avoid that the waste is delivered to an unauthorized dump.

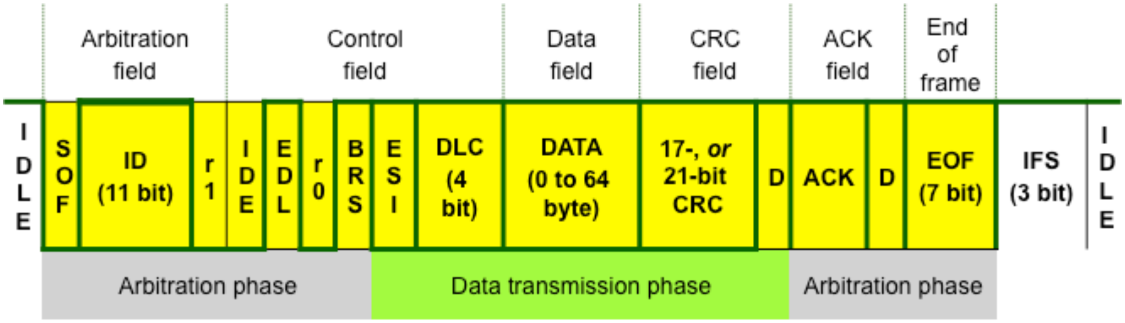
CANopen provides some mechanism to detect "strangers" in the network. The Identity parameter can be used for that purpose. However, it is just suitable for detecting unintended integration of devices, but it is not sufficient for authentication. Protection against "criminal" attacks requires some encryption of data. Up to now, no general solution has been adapted for CANopen networks.

Higher bandwidth and more payload

The increasing requirements on safety and security functions lead to more complex communication with higher throughput and longer commands and status information. This requires more network performance. CAN-based solutions are already at their limits. In order to avoid more network segments, higher bandwidth and larger payloads are needed.

The CAN FD protocol provides this. With a data-field of up to 64 byte (instead of 8 byte) and an 8-times higher data-rate, the improved CAN protocol seems to satisfy the safety and security requirements.

The benefit: The robustness and the reliability of the communication are not affected. For example, the cabling could be the very same. However, the CAN nodes not supporting the improved CAN protocol will transmit error flags, when they receive CAN FD frames. This means, migration strategies need to be developed. One option is partial networking: The none-CAN FD supporting nodes should be in deep-sleep mode and may be awaked before the classic CAN communication. Another one is the strict separation of classic CAN and CAN FD communication.



SOF = Start of frame (bit is always of dominant state)
ID = Identifier (frame priority *and* content indication)
RTR = Remote transmission request (dominant, if data frame)
IDE = ID extension (dominant for base frame format)
EDL = Extended data length (recessive, if data field is longer than 8 byte)
r0/1 = reserved bit
BRS = Bit rate switch (recessive, if switched to alternate bit-rate)
ESI = Error state indicator (recessive, if transmitting node is in error passive state)
DLC = Data length code (indicates the length of the following data field)
CRC = Cyclic redundancy check (17-bit, or 21-bit)
D = Delimiter of CRC/ACK field (bit is always of recessive state)
ACK = Acknowledgment slot (correctly receiving node sends a dominant bit)
EOF = End of frame (all bits are always of recessive state)
IFS = Inter-frame space (the first two bits are always of recessive state)

Figure 4: CAN FD base data frame using an 11-bit identifier

CiA recommends to use a maximum ratio of 1:8 for arbitration to data-phase bit-rates. For typical mobile machine networks running today at 250 kbit/s this results in a 2-Mbit/s data-phase bit-rate. Of course, CiA also recommends using the very same bit-timing register setting in all connected nodes. Otherwise, sample-point tolerances in the arbitration phases may lead to timing failures, which can't be compensated by the CAN FD controller chip. In addition, it is recommended to use 2-Mbit/s qualified CAN high-speed transceiver chips. This means, they are proofed to support data-rates of 2 Mbit/s over the entire temperature range. This is because of the effect that in lower temperatures the dominant bits become longer and the recessive bits are shortened.

Summary

The increasing demand on safety and security in control systems for mobile machines requires higher performing networks providing more bandwidth and longer payload options. CAN FD, the improved CAN data link layer, is suitable for such applications. It uses the proven CAN physical layer and provides a reliable communication with a Hamming Distance of 6 meaning that five randomly distributed bit-failures are detected. With the automatic retransmission of faulty messages, the high availability of control systems can be achieved. It is not just that a machine transits into safe-state, there is also a requirement that the machine is available. For security demands, existing methods from the IT industry may be adopted.

Safe control systems for mobile machines are available. In order to increase the number of devices, it is necessary that the certification process should be optimized. Pre-certified hardware components and software libraries should be developed in order to simplify and accelerate the design of safe devices. The safety standards need to be more stable than in the past, in order to safe investments of device and machine manufacturers. Directives should not reference standards, which are changing frequently.

Holger Zeltwanger
CAN in Automation e. V.
Kontumazgarten 3
Phone +49-911-928819-0
Fax +49-911-928819-79
E-mail: headquarters@can-cia.org
Websites: www.can-cia.org
www.can-newsletter.org
www.cia-productguides.org