When end of the 90ties the CANopen Safety protocol (CiA 304) was initially developed, most of the machine builders and their suppliers were not really interested in safety-related communication systems. Some companies specialized in safety such as Pilz, Jokab, and Schmersal had developed in parallel other CAN-based safety protocols. The best known is Safetybus-p by Pilz. Esalan by Schmersal was not commercially successful, and the CAN-based safety protocol from Jokab was a proprietary approach and therefore had limited success only.

In the early days of the CANopen Safety protocol, several CiA members were not only involved in the specification, but even started some product developments. Port implemented the protocol as an extension of its CANopen protocol stack and sold it to several customers, who still use CANopen Safety as an embedded network for their own products. A typical example is Elobau: The company offers a range of 25 units (also called “safety relays”). Together with coded magnets, available in various sizes, the company provides contact-less machine safeguarding solutions. The products are compliant to EN ISO 13849-1, which defines a safety integrity level (SIL) for the devices. But like most of the other early CANopen Safety developments, these products are not available for open communication systems. They are used in turn-key solutions.

Other CiA members formed a consortium, which initiated the development of the CANopen Safety Chip (CSC). Systec, a provider of CANopen software, was contracted to make the implementation. The company also developed and marketed the CSC01 starter kit. The CSC01 was based on the M16C micro-controller by Renesas, which provided an on-chip CRC hardware. This was necessary to meet the timing requirements for a single-chip implementation. The microcontroller used two on-chip CAN modules, sending alternatively the CAN frames in order to avoid a misbehavior caused by a single-failure. TÜV Rhineland certified the CSC01 in 2004.

“The Safety-related Data Object (SRDO) is made by two CAN data frames and requires two timers.”

The basic idea of CANopen Safety is the transmission of process data twice independently in two CAN messages. The first message contains the process data as in normal PDOs, while the second frame transmits the same data but bit-wise inverted. The two used CAN-IDs are different in minimum in two of the eleven bits. The consuming safety-related device crosschecks the received process data. Thus, an SRDO is made of two CAN messages. In addition, there are two timers observing the correct transmission of the two messages: The Safety-related object validation time (SRVT) is the maximum time allowed between the two messages and the safeguard cycle time (SCT) is the time between two SRDOs. If one of the timers expires, the actuating device shall go into safe state. This shall also happen, if any other single failure occurs.

If a sensor (input) device detects any single failure, it shall stop transmission of SRDOs, which will be detected by all SRDO consuming devices, which will then transit into safe state. The benefit of the simple SRDO protocol is that no additional CRC is required and that the standardized CANopen profiles can be used without any change. But the simplicity of the CANopen Safety protocol has some drawbacks on the other side: Safe configuration of application parameters is not standardized by the CiA 304 specification and needs to be solved in manufacturer-specific parameters, in particular, if the devices are not pre-configured by the manufacturer. The safe configuration of communication parameters is standardized by means of an object dictionary entry, which contains a CRC sum.
calculated after configuration. The CANopen Safety protocol stack checks periodically, if the CRC sum is still the very same. Any inconsistency would lead to stop device operation and to go into safe state. CiA has submitted the CANopen Safety protocol (CiA 304) for European standardization in the range of the EN 50325 series. However, the release of the standard has been delayed for different reasons, most of them quite formal. But such is standardization politics. Standardization is just one key to the success. Another one is to meet the relevant directives of authorities.

“The European machine directive 98/37/EC is valid until end of 2011.”

The Machinery Directive 98/37/EC suitable for non-programmable safety-related devices and machines, which was based on EN 954-1, was accepted and used by the machine building industry for many years. By definition, the Machinery Directive applied to machinery, moving machines, machine installations, and machines for lifting and transporting people, as well as safety devices. The specified essential health and safety requirements (EHSRs) cover the entire scope of mechanical engineering and are a vital aspect of the industrial community. Overall, the Machinery Directive harmonizes the requirements of the European Union (EU) and European Norms (EN). The goal of this directive is to ensure the safety of people, domestic animals, or property from threat of endangerment produced by machinery or safety components. The CE mark is affixed to a finished product, signifying that the machinery has been tested and conforms to all applicable EHSRs outlined in the directive.

The revised Machinery Directive 2006/42/EC, published on June 9th, 2006, did not introduce any radical changes, but aimed at consolidating the achievements of the Machinery Directive in terms of free circulation and safety of machinery while improving its application (see below). As under the old Machinery Directive, the conformity of most machinery will continue to be certified by the manufacturer himself. The exceptions include (see Machinery Directive Annex IV):

- Circular, band and portable chain saws (sawing machines)
- Hand-fed surface planing machines for woodworking
- Thicknessers for one-side dressing
- Combined wood working machines
- Hand-fed tenoning machines
- Hand-fed vertical spindle molding machines
- Presses including press breaks for cold working of metals
- Injection or compression machines for plastics or rubber molding
- Machinery for underground work (e.g., machinery on rails, hydraulic-powered roof supports, or internal combustion engines)
- Manually loaded trucks for collection of household refuse incorporating compression mechanisms
- Guards and detachable transmission shafts with universal joints
- Vehicle-servicing lifts
- Devices for lifting persons, who are at risk of falling more than three meters
- Machines for the manufacture of pyrotechnics

On the device-level a certification by notified bodies is necessary for the following safety components:
Dossier

- Electro-sensitive devices (nonmaterial barriers, sensor mats, electromagnetic detectors, light curtains, etc.)
- Two-handed controls
- Automatic movable screens
- Roll-over protection structures (ROPS)
- Falling-object protective structures (FOPS)

In order to give the industries a transition time, the presumption of conformity to EN 954-1 was valid to the end of last year (December 29th). But some European industries were too lazy, not willing or unable to adopt the new directive in time. So it happened that normally happens, if industries are not prepared or in delay: The EC Machinery Working Group met on December 8th, 2009 and voted to prolong the cessation of EN 954-1 (1996) beyond end of 2009. Two third of the participants were in favor of the prolongation. On Monday, December 28th, the Official Journal of the European Union, 2009/C 321/09, announced the prolongation of EN 954-1 until December 31st, 2011. They also published a correction from EN ISO 13849-1:2006 to EN ISO 13849-1:2008. The first significant to those announcements is that for the first time in two years either EN 954-1:1996, EN ISO 13849-1:2006, or EN ISO 13849-1:2008 may be used as a basis for presumption of conformity. This is a significant advantage for non-European companies still struggling to understand the additional requirements. In summary, these companies can continue to follow the requirements of EN 954-1 for two more years.

The prolongation solves the problem of the insufficient availability of products, which are designed according the new directive and related standards. But it does not answer a lot of legal questions. For example: Is it allowed to mix devices designed and certified by the old and the new directive? And there are even more open questions. Not all players in the safety game are happy about the prolongation, especially those companies that have made their homework and developed products according to the new Machinery Directive.

To make it clear, the scope of the new Machinery Directive is extended, since construction-site hoists and cartridge-operated fixing and other impact machinery will no longer be excluded. In addition, the borderline between the Machinery and the Low Voltage Directives is clarified. The distinction will no longer be made on the basis of the “main risk”. Instead, the new Machinery Directive lists six categories of electrical machinery that are subject to the Low Voltage Directive – for other electrical machinery, the safety objectives of the Low Voltage Directive apply for the electrical risks, but the obligations concerning conformity assessment and the placing on the market are governed by the Machinery Directive.

The borderline with the Lifts Directive has also been clarified. The new text modifies the scope of the Lifts Directive so that lifts with a travel speed no greater than 0.15 m/s will be excluded from the Lifts Directive and will thus be subject to the Machinery Directive. The range of safety devices subject to the Machinery Directive has been clarified. An indicative list of safety components is given in a new Annex.

“There is an urgent need for more CANopen Safety products.”

Nowadays, there are just a few CANopen products available, which provide CANopen Safety functionality. There is just one configuration tool on the market, which supports CANopen Safety. Of course, this may change in the future, but there is an urgent need for more CANopen Safety products. Even if the industry got some more time to adapt the Machine Directive 2006/42/EC, the device manufacturers need to hurry up. Otherwise, we will have the same problem in two years.
PLCs with CANopen Safety support. It would be helpful, if the PLCopen Safety compliant runtime software, as offered by different companies, provided also CANopen Safety protocol support. KW Software has implemented PLCopen Safety and offers related tools for parameterization, configuration, and programming, which are compliant to IEC 61508 (SIL 3). Since 2007, the software house provides CANopen connectivity (CiA 301 and CiA 302), theoretically a CANopen Safety extension can easily be added. However, nobody has done it yet. The CANopen extensions of the Proconos IEC 61131-3 compliant runtime environment and the Multiprog CANopen configuration tool were developed in cooperation with Ixxat.

For rail vehicle applications, Luetze has developed a very interesting controller that supports the CANopen Safety protocol (up to SIL 3) plus bus-line redundancy as specified in CiA 302. With this approach it is even possible to reach SIL 4. CANopen Safety may become important for rail vehicle applications, when safety-related subsystems will be based on CANopen technology.

“Safety-related CANopen sensors are used mainly in outdoor applications.”

CANopen networks are quite well accepted in mobile machines, heavy-duty vehicles including trains as well as other applications in harsh environments. In some of these applications safety-related communication is required. Safety-related sensors measure angles and speeds as well as distances and limits. The measurements are transmitted safely via CANopen to the controller, which safely commands the actuators mainly by means of safe discrete interfaces. Up to now, there are only a very few safe actuators available, which feature CANopen Safety. Most of them are not available on the open market.

TWK was one of the first encoder manufacturers, who implemented the CANopen Safety protocol in its sensors. The company offers electro-magnetic rotary encoders as well as inclinometers with CANopen safety. Both kinds of sensor are compliant to IEC 61508 (SIL 2). The encoders of the T-series and the R-series contain an ASIC with integrated Hall elements to detect the rotary motion of an external permanent magnet, which is located in a shaft or in a hub. In the second version the hub can be mounted directly on the shaft, which has to be detected and thus this version needs less space than a solution with a shaft encoder. One of the first applications is a military one.

Furthermore the hub version has no moving parts in the electronics case, which makes the encoder wear-free and allows a potting for a higher protection grade. The separation of magnet and electronics in two mechanical parts yields to a movement, which requires no torque. The T-series of rotary encoder were designed with the main focus on robustness, the R-series rotary encoder on compactness, respectively.

The T-series of rotary encoder are dedicated for harsh environments. In the shaft version they have a two-chamber construction to separate rotating components from the electronic circuits. Thus also a potting of the electronic chamber is possible to obtain protection grades up to IP69K, which allows applications in liquids, e.g. under water. The housing is made of seawater resistant aluminum or stainless steel with a wall.
thickness of 5 mm in versions with 50-mm housing diameter. Smaller versions with housing diameters of 36 mm or 42 mm are available, too. Single-turn (resolution 12 bit) and multi-turn versions (4,096 revolutions) are available. The detection of the revolutions is realized with a counter (with and without battery) or with an absolute multi-turn gearbox. This gearbox allows the registration of an overrun after power outages under all circumstances. In addition to the position a velocity signal is provided. The R-series rotary encoders (with 9-bit or 12-bit resolution) have a compact setup. In the shaft version three models with different ball bearings for different protection grades (IP53, IP64 or IP68) are offered. The code sequence and a preset value are programmable by the user.

TWK has also introduced an inclinometer with CANopen Safety connectivity. It is used for example in telescope booms from Cavotec Alto. They are based on an MEMS (micro-electro-mechanical systems) circuitry measuring acceleration or gravity. The NKN and NBN series of inclinometers contain two sensor channels to detect angular movements within one or two axis to be chosen out of three degrees of freedom (x, y, z). The two-channel version represents a redundant system with the nodes 1 and 2. In the first instance node 1 sends its data. By implementing the CANopen Safety protocol to CiA 304, V1.01 the device will conform to SIL 2 IEC 61508. Two mechanical configurations of the inclinometer are available. Model NKN is a square-shaped PCB measuring 55 mm by 55 mm. Model NBN is a transducer unit with a robust aluminum or stainless-steel case and one or two connectors for serial connection with other CANopen devices. The measurement span of both items is ±90° maximum. It can be configured to unsymmetrical deflections, i.e. to +30°/-90°. Many of the other manufacturers of rotating encoders and inclinometers also develop safety-related devices. About one year ago, Posital introduced its first encoder with CANopen Safety connectivity. Certification however is timeconsuming: End of last year, the TÜV Rhineland gave approval and certified the encoder. Starting with the first quarter of 2010, the serial production of safety-related optocode encoders will start. They are suitable for SIL 3 applications. The according to IEC 61508, EN 62061 (SIL CL 3) and EN ISO 13849 (performance level e). Operated with protective extra low voltage (PELV), they are suitable for use in motion control and lift applications as well as construction machinery and machine tools. A special feature is the redundant encoder design: thanks to dual optical arrays and two gearboxes, the units ensure optimal reliability while measuring only 16 mm more than normal models. Node-ID and bitrate (up to 1 Mbit/s) are configured via a rotary switch at the connection cap. Like all optocode encoders, the safety models use a proven optoelectronic scanning method to record position values. The single-turn sensor provides a resolution of 13 bit per revolution. Additionally, a maximum of 16,384 revolutions (14 bit) can be registered in multiturn mode, thereby covering a 27-bit measuring range. The encoders are available as solid shaft or synchronous shaft models. The units provide IP65 protection on the housing side and IP64 on the shaft side (an optional sealing ensures IP66).

FSG located in Berlin (Germany) has developed a broad range of CANopen Safety sensors including in tilt angle, rope length and live ring transmitters. Additionally, the company offers safety-related limit switches (cam-operated) as well as manually and pedal actuated control transmitters. Like the other sensors, the wind velocity indicators are mainly used in cranes and excavators. The food pedal is compliant to IEC 61508 (SIL 2) and ISO 13849 (PL d).

The CSC01 is no longer available for new designs, due to the withdrawal of the used micro-controller version. Of course, there is a successor, pin- and software-compatible. To be honest, there are a very few minor software incompatibilities, as usual.

“The CANopen Safety Chip is already pre-certified and simplifies the implementation of CANopen Safety.”

CiA ported the CANopen Safety software to the new micro-controller version and submitted the CSC02 to TÜV Rheineland for re-certification. In November of last year the CSC02 received the certificate. Volume production can start right now. The CSC02 is available in different housings. The first customer is Posital, who uses the chip in its safety encoders (see above).

The CANopen Safety protocol, also approved by TÜV Rheineland, seemed to be not that often used as it could be. The main reason is the penetration of safety networking in those industries, in which CANopen is dominant. Industries such as construction machines, off-road and off-highway vehicles are just starting to implement safety controllers and networked safety devices. One of the reasons is the lack of available safety products. So what we have now is a typical hen-egg problem. The prolongation of the presumption of conformity to the old Machinery Directive until end of 2011, gives the industries an additional chance to implement safety networks such as CANopen Safety.

www.can-cia.org