March 2022

CAN Newsletter

Hardware + Software + Tools + Engineering

From eight to more than 700 members

History and trends: CAN lower OSI layers

History and trends: CAN in elevators

History and trends: CAN in agriculture and farming

30 years CiA

www.can-newsletter.org

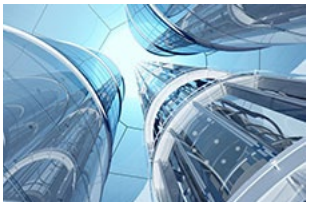

IFD Intensive Fieldbus Diagnostic –
Detect faults before they occur at all.
CANtouch®
IFD
INTENSIVE FIELDBUS DIAGNOSTIC
GEMAC
Safe in every situation.
GEMAC
gemac-chemnitz.com
GEMAC
GEMAC Motus XC
XC6MZ360-O
Order No.: PR-2/116-30
Serial No.: 27116-30/000001
7.5...36 VDC • IP6K7/IP6K9K
Interface: CANopen
GEMAC Chemnitz GmbH
Made in Germany
POWER IMU
GEMAC Motus® –
The FIRST POWER-IMU for Mobile POWER-Machines.

Table of contents

30 years CiA

History and trends

Automotive



CANopen

Brief news

30 years of CAN in Automation

CiA 1992-2022

On March 5, it has been 30 years since six companies and two individuals have established the CAN in Automation (CiA) international users' and manufacturers' group. Today, more than 700 companies and other legal entities have joined the nonprofit CiA association. In the beginning, this industry consortia focused on the development of non-automotive CAN applications. Nowadays, CiA members develop and specify also the CAN lower layers and support all industries using CAN-based technologies. In total, CiA specifications comprise more than 25 000 pages.

On June 1 and June 2, CiA celebrates its 30th anniversary with an in-person event in Nuremberg (Germany). The two-day event comprises four sessions with presentations and includes the regular annual general assembly with election of the board of directors and members of the CiA Technical Committee and the CiA Business Committee. At the second day, some CiA technical groups have the opportunity to meet. In parallel to these meetings, the newly-elected CiA Business Committee pre-discusses the requirements for 2023. For registration please contact CiA office at events@can-cia.org.

Today, there are three generations of CAN data link layers (DLL): Classical CAN, CAN FD, and CAN XL. With these improved DLL protocols and the SIC (signal improvement capability) transceiver technologies, CAN is well prepared for the future and can continue its success story.

Imprint

Publishing house
CAN in Automation GmbH
Kontumazgarten 3
DE-90429 Nuremberg
publications@can-cia.org
www.can-cia.org
Tel.: +49-911-928819-0
Fax: +49-911-928819-79

Reiner Zitzmann (CEO)
VAT-ID: DE812852184
HRB: AG Nürnberg 24338

Publisher
CAN in Automation e. V.
Kontumazgarten 3
DE-90429 Nuremberg
VAT-ID: DE169332292
VR: AG Nürnberg 200497

Editors
Olga Fischer (of)
Cindy Weissmueller (cw)
Holger Zeltwanger (hz)
(responsible according to the press law)
pr@can-cia.org

Layout
Nickel Plankermann

Media consultants
Tobias Kammerer
Birgit Ruedel (responsible according to the press law)
Rozanna Rybin
publications@can-cia.org

Downloads December issue
(retrieved February 22, 2022)
8737 full magazine

From eight to more than 700 members

(Source: Adobe Stock)

This year, the CAN in Automation (CiA) nonprofit association celebrates its 30th anniversary. In short recap, the CiA initiator, Holger Zeltwanger, reflects some of the important milestones.

Everything started already in 1991 in Munich (Germany) on the System tradeshow. In those days, I was the editor of the German VMEbus magazine. I discussed with some companies promoting first CAN board level products compatibility issues regarding the physical layer and interoperability in respect to higher OSI layers. The result was simple, I invited eight companies to a very first meeting to discuss how to overcome compatibility and interoperability problems to Nuremberg in January 1992, where I was living. Surprisingly, 23 companies showed up. At the end of the meeting, I got the task to prepare a next meeting to inaugurate a nonprofit association according to German laws (we German love clubs).

On March 5, 1992, six companies and two individuals founded the CAN in Automation (CiA) international users' and manufacturers' group. CiA was registered by German authorities as a nonprofit entity. In the same year, 15 CiA members participated in the Interkama tradeshow demonstrating for the first time a CAN network connecting products from different vendors. The products utilized already 9-pin DIN connectors with a standardized pinning that is still used today.

The next two years, CiA was busy developing the first specifications. The CAN Application Layer (CAL) specified in the CiA 200 series was an academic approach. Nevertheless, several applications made use of it. Bosch and some partners adapted it and specified a CAL-based communication profile within the Esprit research project sponsored by the European Community. In 1994, the results of this project were handed over to CiA for further developments and maintenance. Nowadays, this approach is known as CANopen comprising application layer and profile specifications.

Also 1994, I organized the first international CAN Conference (iCC) in Mainz (Germany). In those days, the CiA headquarters was still a one-man show. After the successful iCC with more than 200 participants, CiA hired the first secretary. Membership was growing, and I was not longer able to work as fulltime editor and administrating the CiA association in parallel. I quit my job as editor and began to work fulltime for CiA. To be honest, I was still working for my own publication, the CAN Newsletter, which I started already in June 1992.

Figure 1: Already in 1992, CiA members demonstrated at the Interkama fair the interoperability of very first CAN-connectable devices and tools (Source: CiA)

The next steps, were the release of CANopen specifications. This included the CiA 301 application layer and communication profile, the CiA 401 profile for modular I/O devices, and the CiA 402 device profile for drive and motion ▷

Figure 2: Holger Zeltwanger, the initiator of CAN in Automation

controllers. CiA also organized joint stands for its members at Hanover Fair and other tradeshows. One remarkable milestone was the international standardization of CANopen in EN 50325-4. In those days before the year of 2000, CiA also developed a CANopen conformance test tool with the support from National Instruments. The series of annual iCC continued. They took place in France, Netherlands, Italy, U.S.A., and other countries.

Beginning of the new millennium, CANopen penetrated many new markets including rail vehicles, construction machines, refusing collecting vehicles, elevators, and maritime electronics; just to name a few. The number of CANopen profile specifications increased dramatically, and CiA hired more engineers to support the editing of documents. The business of seminars was growing as well as the demand on free-of-charge support for CAN device manufacturers and system designers. In these years, I traveled increasingly to North America and to Asia to bring CAN technology to other continents.

In the 2nd decade of this century, the CAN FD data link layer was developed by Bosch and some other CAN interested parties. In the beginning, CiA was only indirectly involved. But during the CAN FD development, CiA organized so-called plugfests to prove the interoperability of first CAN FD implementations and to test the physical limits of the CAN FD communication. CiA also developed CAN FD device and network recommendations and published them in the CiA 601 series. This included the SIC (signal improvement capability) transceiver as specified in CiA 601-4, which becomes now the dominating transceiver technology in CAN FD networks.

In 2018, CiA started on demand of Volkswagen the development of CAN XL, the 3rd generation of CAN technology. End of 2021, CiA has released the CAN XL data link layer and physical coding sublayer specification (CiA 610-1) and the CAN SIC XL physical medium attachment sublayer specification (CiA 610-3). The first CAN XL plugfest organized by CiA took place in June 2021. Of course, in all the 30 years, CiA has improved its technical documents and is continuing to do so. CiA has now more than 700 members and 14 employees are working in the CiA office managed by Reiner Zitzmann. ◀

hz

(Source: Adobe Stock)

History and trends:

CAN in elevators

In 2002, CiA members started to develop the CiA 417 profile for lift control systems. CANopen used in lifts became CANopen Lift. The goal was to agree to a common specification, which enables suppliers to design interoperable CAN-connectable devices for elevators.

The history of elevators begun with human or animal powered hoists. Some early ones were even driven by water power. Modern elevators started in the 19th century: In 1852, Elisha Graves Otis introduced safety contrivance for elevators. The first electric-driven elevator was manufactured by Werner von Siemens in 1880.

Nowadays, there are millions of elevators in operation. Most of them use electrical drives, the other ones are driven by hydraulics. Just in 2020, over one million units were installed and many others were retrofitted. Vertical transportation of human beings is very safe (some people state that elevators are the most reliable transportation technology) and very resource efficient in comparison with horizontal transportation.

Electric control systems for elevators are used for a long time. Beginning of the 90ties, Kone was one of the first companies using CAN networks to control elevators. Today most of the control systems for elevators make use of CAN networks. In the beginning, the CAN networks implemented proprietary higher-layer protocols. In 2002, some CAN in Automation (CiA) members started to develop a CAN-based application profile for lift control systems. The initiator was Joerg Hellmich working with Boehnke & Partner (now he is the Managing Director at Elfin). The profile is now known as CANopen Lift and it is specified in the CiA 417 document series.

CANopen Lift: Specifying virtual devices

The CiA 417 document series specifies an application profile based on the classic CANopen application layer (CiA 301). Application profiles describe the functional communication interfaces for the whole network. CiA 417 specifies the interfaces of functional entities called virtual devices. This includes call, car drive, and car door controllers as well as input panel, output panel, car drive, car position, load measuring, car door, light barrier, remote data transmission, and power-measuring units. A CANopen Lift device can implement one or multiple virtual devices. This allows very flexible network system designs. Usually, a CANopen Lift network system comprises two network segments connected via a transparent PDO bridge. This means, from a logical point of view it looks like a single seamless network.

All necessary PDOs for a single-shaft lift control system are specified; some of them are distributed in broadcast other peer-to-peer. For multi-shaft lift control systems, the communication between the controllers is manufacturer-specific. Nevertheless, each device can implement up to eight instances of the application profile, so it can be ▷

Figure 1: CiA's official CANopen Lift logo (Source: CiA)

used in up to eight lift control systems.

As already mentioned above, the virtual device concept allows the design of PDO-transparent bridges. The virtual device definitions for the car drive unit (motion controller) and car position unit (encoder) follow the generic CANopen device profiles for motion controllers and encoders. However, in lift control applications different object dictionary entries are used. The CiA 417 specification comprises several parts: Part 1 describes general definitions (including additional error codes), Part 2 specifies virtual devices, Part 3 specifies PDOs, and Part 4 specifies application objects (process data and configuration parameters). All parts are available on CiA's website.

As far as possible, the virtual device definitions are implementation-independent. The CANopen Lift specification enables system designers to select CiA 417 compliant devices from different suppliers and to integrate them into networks without huge efforts. For example, the car position unit can be implemented in traditional rotary encoders as well as sensors using other technologies to measure the position, such as ultrasound or magnetic tape. Usage of standardized interfaces allows the lift operator an open maintenance of the lift system. Software tools for implementation and diagnosis are available by different providers.

CANopen Lift is suitable for very small applications as well as for complex systems. Over the last ten years, the CiA 417 specification has been extended. It covers modern system requirements including pre-emptive maintenance and the link to cloud services. Since CiA 417 version 2.1.0, the boot-up and program download procedure is introduced. The CiA 814-1 application note provides the implementation hints for the CiA 417 compliant bootloader.

In the first days of CANopen Lift, there were available just a very few car drive units compliant with CiA 417. But ▷

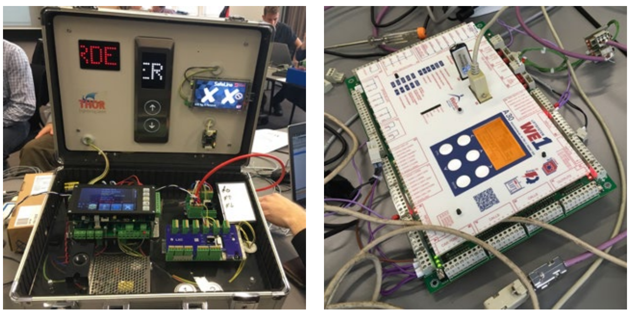


Figure 2: 2019, live in one of CiA's CANopen Lift plugfests: On the left, CANopen Lift controller and units in one box connected to car drive units from other companies; On the right, CANopen Lift host controller tested on interoperability with drives and panels (Source: CiA)

Figure 3 In the Globen Shopping mall 29 lifts use CANopen Lift controllers (Source: Hisselektronik)

those days are gone, nowadays, there are several manufacturers offering CANopen Lift electric inverters. Some companies providing CANopen Lift inverters are, in alphabetic order, for example Control Techniques, Fuji, Gefran, Liftequip, Yaskawa, and Ziehl-Abegg. Most of them have already participated in CANopen Lift plugfests organized by CAN in Automation. In these plugfests, the interoperability to CANopen Lift host controllers featuring car drive controller functionality is approved. One of the market-leading CANopen Lift controller suppliers is Boehnke & Partner. In the last years, the company alone has delivered already about 25 000 CANopen Lift based host controllers. The potential of CANopen Lift has been recognized and so further devices are currently being developed.

Other lift controller providers include, for example in alphabetic order, Bucher Hydraulics (on page 39 you will find an article from them), Elfin, Elgo, Intec, Kollmorgen, RST, Safeline, Sprinte, Thor Engineering, Weber, and of course, a range of others. The list of companies providing CANopen Lift capable products is a very long one.

A little throwback

In 2019, the CAN Newsletter reported about one of the biggest projects with a CANopen Lift control system almost done in Sweden. In the Globen Shopping mall 29 lifts use CANopen Lift controllers. In a special issue of the CAN Newsletter in 2013, the project Mora Hospital was described. The lifts were undergoing modernization as one of the elements in the streamlining of care at Mora Hospital. The CANopen Lift control system collects external calls and priority lift calls are freely programmable. The position of the car is indicated on the FD4-CAN floor displays connected to the CANopen Lift network. In the same CAN Newsletter issue, there are reports about CANopen Lift applications for public means of transport. Kölner Verkehrs-Betriebe (KVB) in Cologne (Germany) and the Metro in Brussels (Belgium) decided to equip their new lifts with controls, operating and display panels, and further assembly groups with CANopen technique. These examples proof, CANopen Lift can be found everywhere.

CANopen Lift plugfests

As already mentioned above, many providers of CANopen Lift products test their devices on interoperability during plugfests organized by CiA. On request, the nonprofit association organizes plugfests for its members. This is done to detect system integration problems before the products are shipped to customers. CiA members implementing the CiA 417 profile in their CANopen Lift devices proof jointly that their products provide plug-and-play capability. CANopen Lift controller suppliers can provide a list of interoperable devices and CANopen Lift unit vendors can provide a list of interoperable controllers. This helps to simplify system integration. System designers get a better understanding of the problems occurring during component respectively device integration. The participants learn from each other, together they solve interoperability issues. They share their experiences regarding functionality of CAN components, CANopen devices, and CAN-based network systems. Last but not least, the results of plugfests are a valuable input for improving of the related CiA specifications. The CiA association is a neutral platform to maintain the CiA 417 application profile specification and to organize plugfests. It also provides supplier- and product-independent training and education services.

CANopen Lift today

The CiA special interest group (SIG) lift control (CANopen Lift) maintains the CiA 417 specification series. The SIG ▷

Since many years, the following basic building blocks are standardized in CiA 417:

- Call controller: It manages the call requests from the input panel units and acknowledges them to the output panel units. It requests the car drive controller to move the car and requests the car door controller to open or close the doors.
- Input panel unit: It is installed as in-car call panel or as floor call panel. There are also general input devices (e.g. for key-switch or fire alarm).
- Output panel unit: It is installed as in-car display panel or as floor display panel. It could be also a generic output panel providing acoustic announcements.
- Car drive controller: It commands the car drive unit to move the car.
- Car drive unit: It moves the car upwards and downwards.
- Car position unit: It measures the position of the car. Optionally, it provides speed, acceleration, and jerk values. There may be four units in the lift control system.
- Car door controller: It commands to open and to close up to four car lift doors. It receives optionally data from the light-barrier unit.
- Car door unit: It opens or closes the car lift doors.
- Light barrier unit: It detects subjects and objects entering the protected area of the car doors.
- Load-measuring unit: It provides the current load of the car and indicates overload situations to the car drive controller.

In the last few years, the following functional entities have been added to the CiA 417 set of specifications:

- Power-measuring unit: It provides the measured power consumption. It can measure the overall or the device-individual power consumption.
- Remote data transmission unit: It features gateway functionality for remote control or remote diagnostics purposes.
- Access remote unit: It reads different media to allow access, e.g. chip and smart cars, RFID tags, bar codes, or finger prints.
- Monitoring unit: It serves as condition monitoring as recommended in VDMA 24582.
- Position supervisor unit: It comprises the car position unit 1 and monitors speed, deceleration, door contacts, safety limit switches, and unintended car moves.

(Source: Adobe Stock)

constantly improves functional description of the application and communication interface for specified CiA lift components and the lift host controller. Furthermore, SIG also introduces new application functions and new lift component specifications. The purpose is to provide highly-readable specifications for implementing interoperable CiA 417 devices for lift manufacturers and system designers. SIG lift control approves release of CiA 417 specification versions with key functionalities and even retains previous specification versions to become publicly available to widespread and improve acceptance of CANopen in the elevator markets. In April 2022, CiA provides a free-of-charge webinar regarding lift control.

There is a range of CANopen Lift related products and it would be impossible to mention all of them. Langer & Laumann provider of door solutions for lifts, for example, offers the TSG V4 lift door operator with CANopen ▷

CiA 417 on Youtube

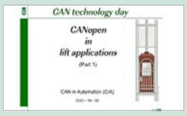
On its Youtube channel, CiA also provides content regarding CANopen Lift. Watch here:

CANopen Lift profile

Webinar from 2021-02-02

CANopen Lift CiA 417

Webinar from 2021-10-14 in Cinese language



CANopen Lift

Technology day 2020

CANopen Lift at Interlift

At the biannual Interlift trade show in Augsburg (Germany), CiA members presented several times the CANopen Lift demonstrator, the first one in 2009. The marketing group (MG) CANopen Lift initiated the development of this demonstrator. It demonstrated the interoperability of CiA 417 compliant devices. The modular system consisted of different independent lift control systems implemented in building blocks comprising a host controller, a car drive unit, a positioning unit, I/O panels, and a car door unit). Usually, four building blocks make one lift application. Each building block hosts one or two devices. In 2019, CiA didn't show the demonstrator but continued the activity with several members presenting their CANopen Lift products and generic CAN tools and gateways by means of product panels on the CiA stand. Unfortunately, CiA is not present at the Interlift 2022 due to the Covid-19 pandemic.

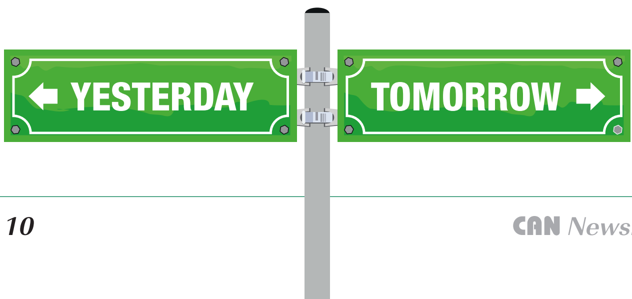
Then…

..and now

Lift profile. The TSG is available in different variants. The company Elfin Technology, is specialized in the development and design of electronic components and software as a service in the lift industry. With more than ten years of experience in the development of CANopen (Lift), they are one of the pioneers of the industry. They support users to implement this technology in their products and also offer a range of CiA 417 based TFT displays suitable for lifts in hotels, office buildings, hospitals, shopping malls, airports, or railway stations. The Flexpage displays can be used in elevators of all brands, for new installations and modernization. Via the integrated CANopen interface, the displays can be used in elevators from various providers and by means of input/output modules parallel wiring is also possible for elevators without a bus connection. CANopen Lift allows them to be flexibly adapted to design requirements and application areas.

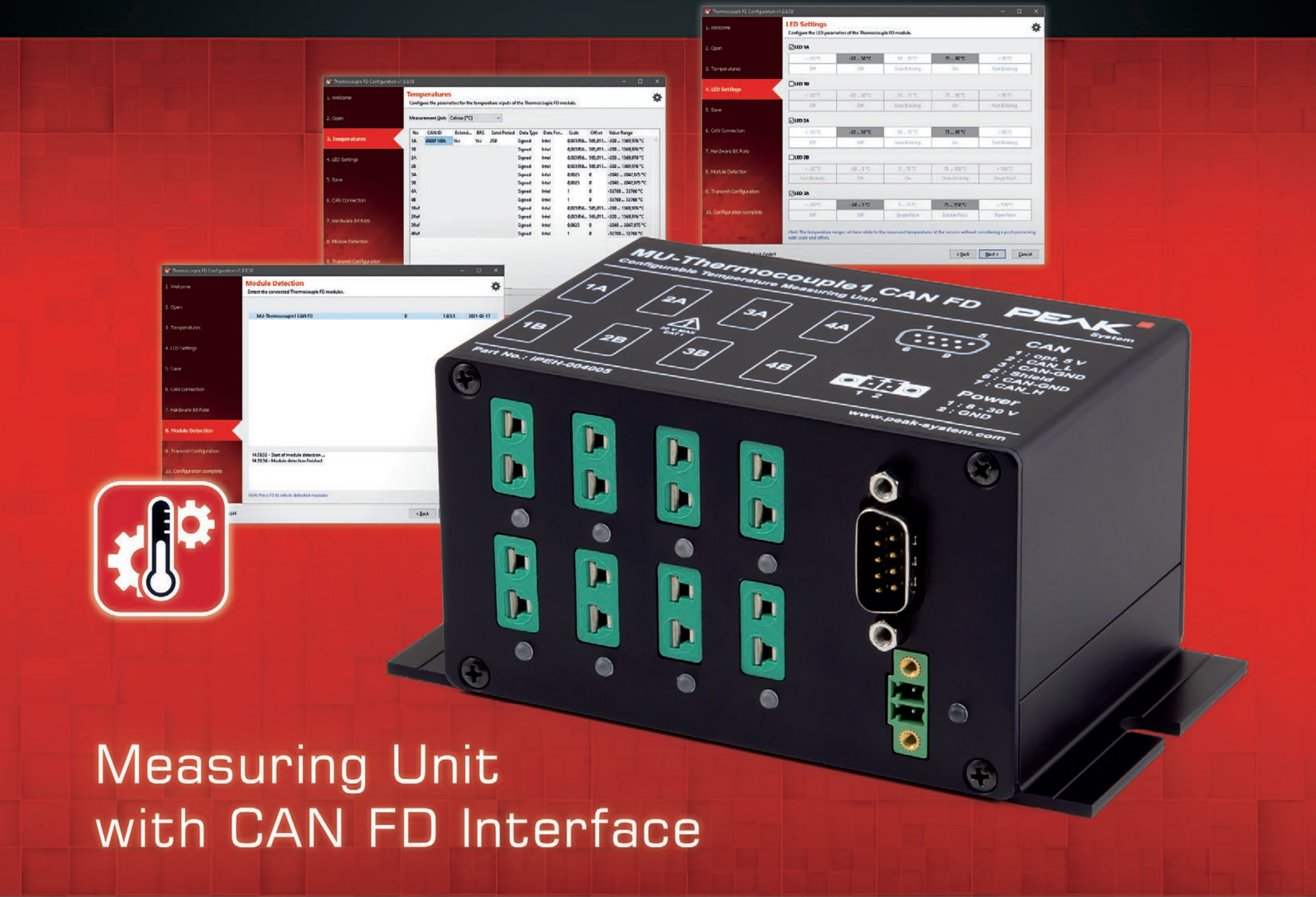
With the Limax series, Elgo Electronic provides an absolute measuring shaft information system, which is used for positioning the elevator cab. It supports CiA 417 and can be connected to the controller via CAN interface. The lift controller MLC-8000 from Intec also uses CAN technology. It can be used for small lifts as well as in the high-end range (up to 64 floors, up to 8 lifts per group). The controller was developed based on the CiA 417. The units in the CANopen Lift supported Zadyn range of frequency inverters from Ziehl-Abegg, were developed exclusively for lift technology. The varied housing designs and construction make them suitable for either control cabinet installation or wall mounting in the machine room or elevator shaft.

Today, many controllers and devices from different manufacturers are already available with CANopen Lift. This profile is the open network approach for elevators. It enables to buy and use devices from different manufacturers depending on own application requirements. ◀



Author

Cindy Weissmueller
CAN Newsletter
pr@can-cia.org
www.can-newsletter.org



Measuring Unit with CAN FD Interface

■ MU-Thermocouple1 CAN FD

The MU-Thermocouple1 CAN FD from PEAK-System allows the measurement of 8 temperatures via thermocouples of the types K, J, or T depending on the product version. The measurement data is transmitted via a CAN interface that supports the modern standard CAN FD in addition to CAN 2.0.

Data processing, message transmission, and LED indication are set up with a free Windows software. The configuration created on the computer is transferred via CAN to the device which then runs as an independent CAN node. Multiple devices can be configured independently on a CAN bus.

Specifications

- 8 Mini sockets for thermocouple types J, K, or T
- 4 galvanically isolated measuring modules, each with 2 thermocouple sockets of the same type
- Measuring ranges:
  - J: -210 to +1121 °C (-346 to 2050 °F)
  - K: -200 to +1370 °C (-328 to 2498 °F)
  - T: -200 to +400 °C (-328 to 752 °F)
- Measurement accuracy: 0.2 % or 1 K
- Accuracy of the reference temperature sensors at +25 °C ambient temperature: typically ±0.5 K, maximum ±1.0 K
- Maximum resolution of temperature data: 1/16 °C
- High-speed CAN connection (ISO 11898-2) for data transfer and configuring
  - Complies with CAN specifications 2.0 A/B and FD
  - CAN FD bit rates for the data field (64 bytes max.) from 25 kbit/s up to 10 Mbit/s
  - CAN bit rates from 25 kbit/s up to 1 Mbit/s
  - NXP TJA1044GT CAN transceiver
  - Galvanic isolation up to 500 V
- LEDs for measurement channels and power supply
- Configuration with a Windows software via CAN (requires a PEAK CAN interface)
- Voltage supply from 8 to 30 V
- Extended operating temperature range from -40 to 85 °C (-40 to 185 °F)

Scope of Supply

- MU-Thermocouple1 CAN FD in aluminum casing
- Mating connector for voltage supply
- Configuration software for Windows
- Manual in PDF format

www.peak-system.com

Take a look at our website for the international partners. Scan the QR code on the left to open that page.

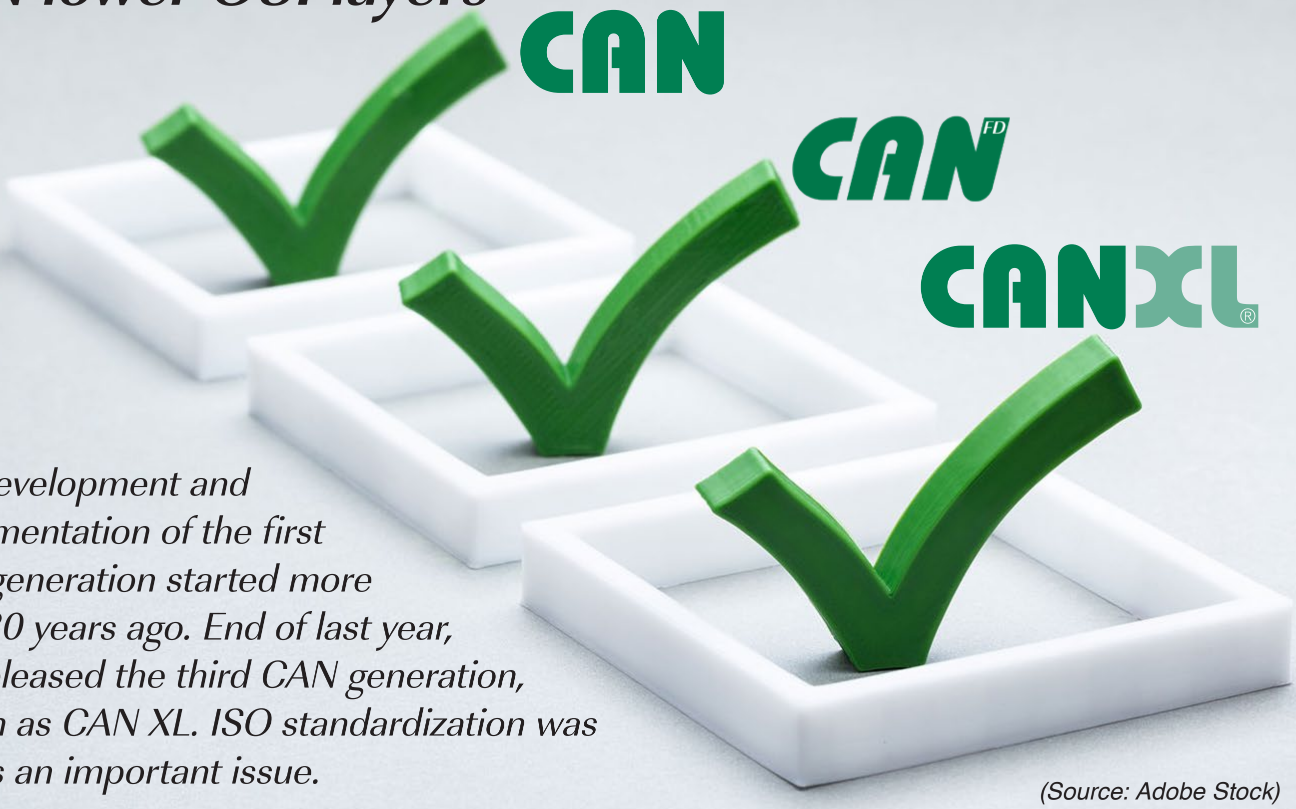
PEAK-System Technik GmbH

Otto-Roehm-Str. 69, 64293 Darmstadt, Germany
Phone: +49 6151 8173-20 - Fax: +49 6151 8173-29
E-mail: info@peak-system.com

PEAK System

History and trends:

CAN lower OSI layers



The development and implementation of the first CAN generation started more than 30 years ago. End of last year, CiA released the third CAN generation, known as CAN XL. ISO standardization was always an important issue.

(Source: Adobe Stock)

The seven-layer Open Systems Interconnection (OSI) model was developed in the late 1970s. It describes the flow of data to be transmitted to receivers through seven abstract layer entities. Nowadays, the OSI model is used to describe communication in a unique manner. CAN communication technology covers just the two lower layers, the data link layer and the physical layer. The fathers of CAN at Bosch did not care so much on the OSI layer modeling. This is, why the Bosch CAN 2.0 document did not specify services and service access points (SAP) between the data link sub-layers and the physical sub-layers. In the beginning, the CAN protocol featured an 11-bit identifier (ID) field; the 29-bit ID field was introduced in a second step, also known as CAN 2.0B. CAN 2.0A controller chips not supporting the 29-bit frame format were available only for some years.

End of the 80s, Intel and Philips Semiconductors (today: NXP) implemented the CAN data link layer and the PMA sub-layer in silicon. Intel's i82526 and Philips' 82C200 stand-alone CAN controllers are legend. In these early days, no standardized transceiver was available. The first CAN node designers used proprietary modified EIA 485 circuitries.

The first CAN generation

In 1993, the CAN data link layer (DLL) was internationally standardized in ISO 11898 (1st edition). This standard covered both CAN protocol versions, CAN 2.0A and CAN 2.0B. It split the DLL in two sub-layers, the logical link control (LLC) and the medium access control (MAC) sub-layers. This modeling was adapted from Ethernet. The ISO 11898 standard also introduced service specifications for these sub-layers describing implicitly SAPs. As the CAN 2.0A/B specification, this ISO standard also comprised the physical coding sub-layer (PCS), which is part of the OSI physical layer. The original ISO 11898 standard also included the physical medium attachment (PMA) sub-layer, which is implemented in CAN transceiver chips. First CAN high-speed transceiver engineering examples arrived in 1992. The first demonstration of ISO 11898 transceivers was done by CiA members on the joint booth of the Interkama tradeshow in October 1992. They used the transceivers from Philips Semiconductors (now: NXP).

Mid of the 90s, an increasing number of chipmakers launched CAN stand-alone controllers as well as CAN controllers integrated into micro-controllers. Just to name a few: Besides the early birds, Intel and Philips Semiconductors, Motorola (now: NXP), National Semiconductor, and Siemens (now: Infineon) entered the CAN controller business. The CAN (high-speed) transceiver market was dominated from the beginning by Philips Semiconductors (now: NXP). Of course, other chipmakers offered pin-compatible components, for example, Siliconix and Texas Instruments.

End of the 90s, General Motors developed the Single-wire CAN (SWC) transceiver standardized in SAE 2411. The speed is limited to a nominal bit rate of 33,3 kbit/s respectively to 83,3 kbit/s in the so-called high-speed mode for diagnostics purposes. Up to 32 CAN nodes per network are possible. The SWC transceiver provide sleep ▷

functionality. Due to the single-wire approach, there is no differential voltage on the network-line. This leads to a lower robustness compared with the ISO standard. Therefore, SWC is not more recommended for new designs.

Beginning of the millennium, the ISO 11992-1 standard was published. It specified a dedicated PMA sub-layer for the CAN truck/trailer connection, which is able to drive two nodes. Unfortunately, the standard has had some weaknesses and was not implemented, but referenced by European regulation. Wabco (now: ZF) implemented a technical improved CAN transceiver, which was not available on the public market. The 3rd edition of ISO 11992-1 released in 2019 has fixed the technical issues and is harmonized with the ZF transceiver features. The ZF transceiver is also used by the competitor Knorr-Bremse.

In 2003, ISO 11898 was split into two documents: ISO 11898-1 (2nd edition) and ISO 11898-2. The updated standards specified the Classical CAN data link layer including the PCS sub-layer respectively the high-speed PMA sub-layer for bit rates up to 1-Mbit/s.

The carmakers requested a low-power CAN transceiver, which was standardized in 2006 as ISO 11898-3. The drawback of this fault-tolerant transceivers was the to 125 kbit/s limited speed. This was the trigger to develop the low-power option for high-speed transceivers standardized in ISO 11898-5 released in 2007. In 2013, high-speed transceivers compliant with ISO 11898-2 with selective wake-up functionality (ISO 11898-6) saw the light of day. The idea was to bring not needed electronic control units (ECU) into sleep mode and to awake them individually, when necessary. But the success was not that overwhelming, which may change in the next years.

The second CAN generation

CAN with flexible data-rate (CAN FD) was pre-developed by Bosch on demand of General Motors and non-automotive CAN users represented by CiA desiring more bandwidth and larger frame payload. Especially, the carmakers were interested to reduce software download times at end-of-line. To flash the ECUs (electronic control unit) via CAN within the cars took in worst case several hours. Even to cut this time only by half is already a huge success.

During the CAN FD standardization, there were detected some problems in the detection of single-bit failures. The introduced stuff-bit counter and the following parity bit solved this issue as well as the properly selected initial value for the cyclic redundancy check (CRC) sequences. At the end, CAN FD features a lower probability of undetected failures than Classical CAN. The 3rd edition of ISO 11898-1 released in 2015 standardized both the Classical CAN and the CAN FD protocols. One year later, ISO updated the high-speed PMA sub-layer introducing more challenging parameters to allow bit rates higher than 1 Mbit/s. This included symmetry requirements for rising and falling signal edges. There were two parameter sets standardized. CiA recommends using transceivers ▷

The CAN FD Light approach provides a commander/responder communication solution for price-sensitive networks used for example in smart headlights (Source: Adobe Stock)

featuring the more symmetric edges. This allows to use not optimized network topologies and still to achieve bit rates of 2 Mbit/s and more. ISO 15765-5 standardizes the bit-timing for CAN FD point-to-point networks used to connect a diagnostics tool to the in-vehicle network gateway. CiA provides general guidelines for the CAN FD bit-timing settings.

In order to reduce ringing caused by not optimized network topologies, CiA members developed the signal improvement capability (SIC) transceiver specification (CiA 601-4). In the meantime, several semiconductor manufacturers provide such SIC transceiver.

There was another demand from the automotive industry to use CAN FD in a commander/responder communication without arbitration. As a consequence, this leads to responder nodes, which do not need costly add-on circuitry such as oscillators. The tradeoff is that only the commander can initiate a communication. The responders just answer the communication request. CiA members developed the CAN FD Light specification (CiA 604-1) suitable for responder nodes. First implementers are STMicroelectronics and Texas Instruments. Applications include smart headlights controlling a bunch of LEDs. Another application field is the internal networking of battery cells. CAN FD Light is a candidate for an annex of ISO 11898-1; so-to-say a dedicated implementation of CAN FD. The CAN FD Light approach has some technical similarities with the Classical CAN serial link I/O (SLIO) concept, which was commercially not successful. Philips Semiconductors (now: NXP) launched the first SLIO component in the very early 90s; but the time was not yet ripe. A few years later, LIN was developed and introduced. CAN FD Light is a candidate to substitute LIN, because of higher bit rates (1 Mbit/s and more) and larger payloads (up to 64 byte). CAN FD Light is a candidate to be used instead of LIN, when higher bit rates and more payload is needed.

The third CAN generation

Surprisingly, just four years after the introduction of the second CAN generation, the third CAN generation was initiated. Volkswagen (VW) requested extra-long (XL) frames able to transport TCP/IP segments/packets with 10 Mbit/s. In 2019, CiA started the development of related CAN XL specifications. End of 2021, the CAN XL data link layer (CiA 610-1) and the CAN XL physical medium attachment sub-layer (CiA 610-3) were released. In the next step, these documents will be integrated into the ISO 11898-1 respectively ISO 11898-2 standards.

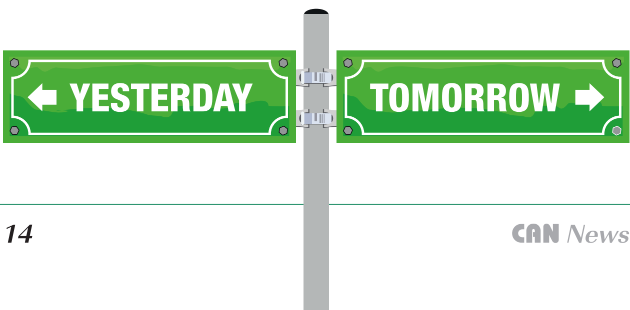
CAN SIC XL transceivers can support bit rates up to 20 Mbit/s. The maximal achievable bit rate depends on the network topology and the selected physical layer components such as cables and connectors. Additional circuitry to improve electromagnetic compatibility (EMC) or galvanic isolation has an impact on the bit rate, too.

The cascaded CRC fields, the fixed stuff-bits, and the other CAN XL protocol features makes the third CAN generation to the most reliable one. The robustness of the CAN XL communication is in minimum as high as in Classical CAN and CAN FD. One of the important features is the scalability of the PMA sub-layer. CAN XL controller can work with all kinds of CAN high-speed technologies.

It seems that the CAN XL technology is already mature. The first CAN XL plugfest was a success and there more such interoperability tests in the pipeline. First CAN XL supporting micro-controllers are under development. CAN SIC XL transceiver prototype implementations have been tested in the mentioned plugfest and others will follow.

The future for all three CAN generations seems to be bright. Depending on the application requirements, the user can choose a CAN protocol (Classical CAN, CAN FD, or CAN XL). Selecting CAN FD or CAN XL gives the user another level of scalability regarding the transceiver technology as explained above. This makes CAN technology very suitable for sub-backbone and front-end networking, where reliability and robustness matters. The traditional reasonable prices for the hardware are important for high-volume applications. ◀

hz



History and trends:

CAN in agriculture and farming

(Source: Adobe Stock)

The world human population is growing. CAN was helping, is helping, and will be helping to provide people with food and beverage.

Agriculture is the practice of cultivating plants and livestock. The history of agriculture began thousands of years ago, when humans started to settle down: Nomadic gatherers and hunters turned into arable farmers, cattle breeders, and sedentary fishermen. In the antic high cultures, agriculture technology was developed to enable the building of cities and monuments. Not everyone was involved in the production of food. There were a lot of workers and administration staff.

Nowadays, the farmers need to feed about eight billion of people. This can only be achieved when using sophisticated technology including electronic-controlled and automated machines. Smart farming is the buzzword: It has a real potential to deliver a more productive and sustainable agricultural production, based on a more precise and resource-efficient approach. It comprises agricultural automation and robotics, precision agriculture, and management information systems.

Isobus and its predecessors

Already before CAN was invented, German engineers discussed and developed the LBS (landwirtschaftliches Bussystem; engl. agriculture bus-system) network approach for connecting electronic equipment within agriculture machinery. When CAN was introduced in 1986, the LBS specification adapted this serial network technology and standardized it in DIN 9684/2-5. But it was not flying due to some technical issues regarding the physical layer specification. Additionally, the North American farming industry was in favor of the J1939 CAN-based network technology, originally developed for commercial road vehicles. The result of the worldwide harmonized and joint development on both sides of the Atlantic Ocean is well-known: Isobus, internationally standardized in the ISO 11783 series, is worldwide used to connect tractors and implements. Implements is the name for any kind of attached machinery: sprayers, fertilizers, harvesters, etc.

One of the most important benefits is the development of the virtual terminal (VT) approach. It allows using the truck-mounted display for all connected implements. The VT communicates via the CAN-based Isobus network with the implements. The farmer controls the implements via the VT and the implements provide status information to the VT.

The development of the Isobus technology started mid of the 90ties. In 2001, first machinery using it arrived on European farms. Today, there are many implements with an Isobus interface. The CAN Newsletter Online reports regularly about new product developments and the progress of the 14-parts ISO 11783 standards series.

Table 1: Isobus standards overview

Part-no.	Title	First issue	Current issue
1	General standard for mobile data communication	2007	2017
2	Physical layer	2002	2019
3	Data link layer	1998	2018
4	Network layer	2001	2017[a]
5	Network management	2001	2011[a]
6	Virtual terminal	2004	2018
7	Implement messages application layer	2002	2018
8	Power train messages	2006	2015
9	Tractor ECU	2002	2012[a]
10	Task controller and management information system data interchange	2009	2015
11	Mobile data element dictionary	2007	2016
12	Diagnostics services	2009	2019
13	File server	2007	2016
14	Sequence control	2013	2018

[a] under systematic review

Associations promoting Isobus

There are several associations, which help to promote the development and to increase interoperability of Isobus-based applications. SAE (Society of Automotive Engineers) develops and publishes J1939-based standard series referenced by Isobus specifications. AEF (Agri- ▷

cultural Industry Electronics Foundation) is the nonprofit association promoting and pre-developing the Isobus protocols. The AEF members jointly work on interoperability solutions. The foundation also proves and certifies devices in so-called Isobus plugfests. The CC-Isobus is a joint development activity of several implement manufacturers, which develop and provide a broad portfolio of VT products. Established in 2009, this competence center has designed the CC-I 1200 terminal, for example, which has been installed more than 50 000 times. DLG (German Agriculture Society) organizes the worldwide biggest Agritechnica tradeshow in Hanover (Germany). The awards, conferred by a committee of experts appointed by the DLG, recognize leading technologies and new developments in the agricultural equipment and machinery sector.

Embedded machine control

Agriculture and forestry machines are equipped highly with electronics. These include the Isobus backbone networks connecting electronic control units (ECU) and additional sub-layered embedded CAN-based networks. Some of them use proprietary application layers, while others are based on J1939 or CANopen.

As some recent examples, Actia offers the SPU40-26 safety power unit with an ISO 11783 compliant interface, which has been certified and proved by AEF. B-Plus has a range of CAN- and Isobus-capable development tools, measurement technology, as well as several controllers in its product portfolio. Bernecker + Reiner, Epec, ifm electronic, Intercontrol, and STW provide host controllers with Isobus-connectivity. They are linked via the CAN interface with the operator displays. Some of them support the virtual terminal function (VT).

Syslogic offers AI (artificial intelligence) PCs with a J1939 (FD) interface and Crosscontrol offers terminals with a CAN FD interface. These provide a higher throughput than the current Isobus or proprietary Classical CAN interfaces. But some farmers prefer traditional tablet computers as user interface. Such solutions are offered e.g. by Reichardt. Ruggedized J1939-connectable in-vehicle telematics tablets are offered by Waysion Technology, Zhangzhou Lilliput Electronic Technology, and Ruggon.

TTControl's HY-TTC 500 controller family with three CAN interfaces meets safety standards up to EN ISO 25119 Ag PLd, IEC 61508 SIL 2, and ISO 13849 PLd. A typical Isobus-compliant job controller platform is the APC mobile 3100 by Bernecker + Reiner. The company's X90 controller features a CANopen Safety interface. This safety-related network can be used for implement-internal control purposes.

Smart work-light system

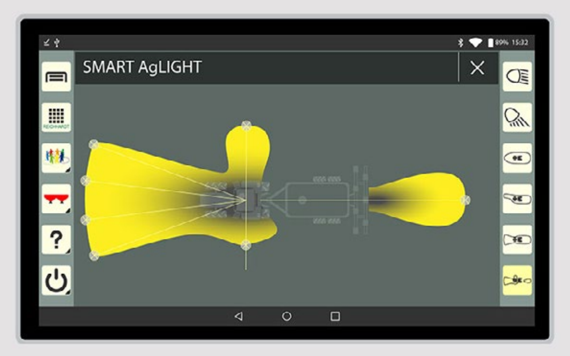


Figure: Direct and indirect glare can be avoided and work areas can be optimally illuminated, even in a vehicle combination. Here, the area to the left of the vehicle is dimmed accordingly for a vehicle driving alongside. (Source: Reichhardt)

The Smart Aglight by Reichhardt is able to distribute light continuously for long-distance and close-range lighting by individually controlling and networking the diffusing lenses of the work-lights. Precise, storable light profiles are adapted to equipment combinations and operating conditions. The lights are operated via an ISO-VT (Isobus virtual terminal) or wireless via mobile terminals, which allows to use smartphone apps and further functionalities. Existing machines can be retrofitted. The recognition of the implement via Isobus adapts the light field to the machine combination. Using a wireless link, the light profiles of several vehicles can be interlinked. Thus, direct and indirect glare is avoided and the working areas are optimally illuminated.

Camera systems for process monitoring and safety in semi-autonomous machines or in field robotics are also supported. In combination with mobile communications, Bluetooth, or Wifi, features such as coming-home or wake-up functions via cell phone or tablet are possible as well.

Controller for agricultural machinery

TTControl lately developed the Isobus-compatible TTC 2300 ECU (electronic control unit) series for off-highway machinery, such as agricultural implements, harvesters, farm tractors, and hybrid electric vehicles. The series is scalable according to advanced and automated off-highway applications. It is designed to be the heart of a centralized electronic architecture and can serve as a vehicle control unit (VCU), a safety monitor, or a head-unit controller for agricultural implements.

The controllers are TÜV safety certified and meet safety standards from the agricultural, construction, and automotive industries, said the company. They are designed for communication with IoT (Internet of Things) networks. The ECUs provide processing of information from analog, digital as well as smart sensors and are able to control electric motors and further actuators.

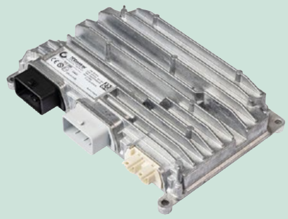


Figure: The controller is built for use in rugged operating environments (Source: TTControl)

Optimized tractor control: TIM

The TIM (tractor implement management) function allows the implement to send commands to the tractor. In this way trailed machines can control functions such as PTO (power take off) shaft, lifting gear, driving speed, steering angle, or hydraulic valves. Thus, the combined machinery automatically adjusts to the current situation reducing the operator's burden, increasing machine performance, and productivity. Several tractor manufacturers already integrate TIM in their vehicles and implements. Fendt, Krone, John Deere, Kubota (Kverneland), Lemken, and Claas are just some examples.

TIM was originally invented by John Deere and is further developed by AEF. First TIM solutions were introduced at Agritechnica 2009. At that time only the machines of the same manufacturer could exchange data. With the release of the TIM specification version 2, the implement sends information to the tractor via a standardized and secure communication. Nowadays, it is a cross-product and cross-manufacturer solution i.e. a tractor-implement combination from different manufacturers is possible. Using Isobus-tested devices with the TIM function (certified by AEF), farmers expect that the coupling of the tractor and the implement works in a plug-and-play manner.

Awarded Isobus solutions

On the Agritechnica tradeshow in 2019, DLG has awarded several Isobus solutions. For instance, the automated tractor and implement guidance system for wineyards, which was jointly developed by Fendt and Braun. The ground contour, vines, poles, etc. are recorded using laser technology and the information is passed on to the tractor via the Isobus interface. Additionally, the 3D position is determined with a gyroscope and the tractor assumes the track and implement guidance based on this information.

The Isomax solution by CNH Industrial global agricultural brand New Holland is a hardware and software interface compliant with ISO 11783 series. All hardware components are AEF certified, all software is open source, and the system is compatible with all brands. System features include automatic implement recognition to facilitate operation.

Figure 1: The awarded automated vehicle by Fendt and Braun (Source: Fendt/Braun)

Additionally, the IQblue retrofit TIM solution by Lemken was awarded. Deploying a GPS receiver, it allows users to automate agriculture machines for ploughing, cultivating, tilling, etc. Another winner was the Nevonex open Isobus platform powered by Bosch. Like an operating system, it forms the basis of software applications to program new and legacy machines. An integrated interface management enables optional access to the platform via the Isobus.

John Deere reveals a fully autonomous tractor

Figure: The 8R tractor uses cameras and artificial intelligence to navigate (Source: John Deere)

Already in 1837, Deere & Co. helped mechanize agriculture with the first commercially successful steel plow. At the CES 2022, John Deere revealed a fully autonomous 8R tractor combined with a chisel plow, GPS guidance system, and artificial intelligence technologies.

The autonomous tractor has six pairs of stereo cameras, which enables a 360-degree obstacle detection and the calculation of distance. Images captured by the cameras are passed through a deep neural network that classifies each pixel in approximately 100 milliseconds and determines if the machine continues to move or stops, depending on if an obstacle is detected. The tractor is also continuously checking its position relative to a geofence, ensuring it is operating where it is supposed to, and is within less than an inch of accuracy.

To use the autonomous tractor, farmers need to transport the machine to a field and configure it for autonomous operation. Using a smartphone app, they can start the machine. While the machine is working the farmer can leave the field to focus on other tasks, while monitoring the machine's status from their mobile device. John Deere Operations Center Mobile application provides access to live video, images, data and metrics, and allows a farmer to adjust speed, depth and more. In the event of any job quality anomalies or machine health issues, farmers will be notified remotely and can make adjustments to optimize the machine performance.

"It's a monumental shift," said Jahmy Hindman, Deere's chief technology officer, of the new machine. "I think it's every bit as big as the transition from horse to tractor."

From automated to autonomous

Autonomy has been creeping into tractors and other farm equipment for decades, with recent advances building upon progress in robotics and self-driving cars. Advances in sensing, communication, and control technologies coupled with global navigation satellite systems (GNSS) and geographical information systems (GIS) enable tractors to become automated or even autonomous. Self-driving tractors could help save farmers money and automate work that is threatened by an ongoing agricultural labor shortage. The gathered data about the soil and precision farming applications help to enhance productivity and optimize resource efficiency.

The increasing autonomy requires additional sensors connected to the CAN-based in-vehicle networks. Typical examples include cameras, 3D sensors, and GNSS systems. GNSS-supported steering systems are already used in daily farming work. Due to real-time kinematics (RTK), intervention is no longer required when the farmer has to line up their tractor or other self-propelled machines such as sprayers, choppers, and harvesters with the next track with an accuracy of two to three centimeters. Of course, the steering wheel needs to be moved by an electric motor. For instance, Reichardt provides the PSR Advanced automatic steering system using GNSS, low-wear synthetic tactile sensors, and ultrasonic sensors. It includes an Isobus terminal as well as several panel-apps and can be used for retrofit applications.

Self-steering tractors have existed for some time now. Hereby, the tractor does most of the work, with the farmer stepping in for emergencies. The technology is advancing towards driverless machinery guided by GPS. Recently, John Deere already introduced the fully autonomous 8R tractor. Further tractor manufacturers are expected to follow.

CAN in animal farms

CAN-based networks are embedded, and thus invisible for "outsiders", in many applications for livestock cultivation e.g. in cowsheds, pig farms, and poultry barns. Already mid of the 90ties, CAN networks were used in cowshed carousels. They connected feeding equipment and devices measuring the water amount the animals were taking. Today, service robots feed and serve animals with increasing autonomy.

For example, the Netherlands-based company Lely manufactures robot milking systems. The CANopen-interconnected Lely Astronaut A4 milking robot including a mechanical arm and teat-cleaning equipment, can handle about 180 milkings a day. The system is trained to prepare the cow for milking, to (re)attach the teat cups, to detach after milking, and to carry out post-treatment. The walk-through functionality allows the cow to walk straight in and out of the milking box without making turns. The animals go into the milking box on their own because they know there is food in the form of a measured amount of grain. The milk quality can be measured, monitored, and diagnosed using the CANopen-based MQC (milk quality control) tool. This provides the user with vital information on mastitis, fat and protein, and lactose for managing milk quality and cow's health. Alarming deviations are noticed and reported. Lely partnered with Strypes (Netherlands) to develop this remote monitoring and diagnostics software solution.

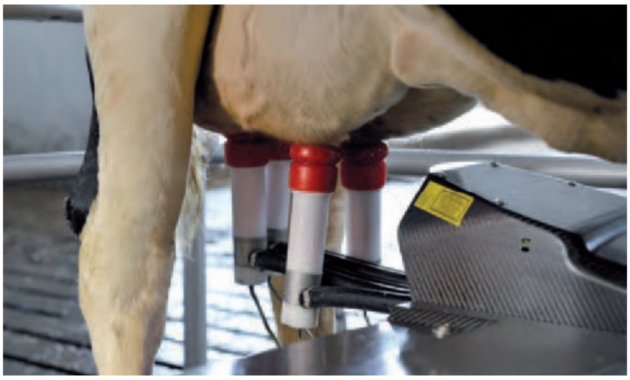


Figure 2: After going in the box the robotic arm moves under the cow, scans it with lasers to find the teats, and attaches four teat cups (Source: Lely)

Another solution to create an easier workplace for milkers is the MDS Saccomatic IDC by the Danish company SAC. This milking control unit communicates via CANopen and registers milking and milk flow, gathers milking data, and displays the required data. It can be extended and connected to a cow identifier and a milking management system to process data from the milking parlor. To ensure that the operator has a complete overview of the milking parlor, the IDC can be connected to touchscreens. In case of a problem, a "cow-related" alarm flashes on the screen. The milker with a few moving parts can also measure the electrolytic conductivity of the milk. This makes it possible to diagnose mastitis in an early stage so that the dairy farmer can begin treatment to prevent the inflammation from spreading.

In a further example, the German company GEA is providing an automated rotary milking parlor Dairyproq, which also uses embedded CAN communication. For milking, the cow steps straight onto the rotary milking parlor where the Milkrack system automatically attaches the teat cups thanks to a 3D camera. The solution allows an undisturbed milking process, said the manufacturer. Also here, the conductivity sensors monitor every udder quarter, which allows to gather information about the milk quality and to manage cow's health preventively. Using the monitoring software GEA Farmview, the automated milking system can be checked via online diagnosis.

The German company Weda provides CAN-connectible stable climate control solutions for pig farms. The Veco.Mate product range includes control systems, alarm units, and power supplies. The controller with a touchscreen provides connection options for reading probes, sensors, measuring fans as well as for setting and controlling of hatches, fans, heaters, valves, etc. It records the climate condition values (temperatures, humidity etc.) for up to 12 months. Via the integrated LAN (local area network) interface, the computer can be operated via a PC or a smartphone using the integrated web server. The alarm computer manages up to 16 separate alarms triggered by ▷

detecting of abnormal conditions. The power supply units developed for agriculture use integrate two rechargeable batteries or a 230-VAC unit, which maintain the output voltage in a power-failure event. If the unit is connected to the alarm computer, the user is automatically informed about a power failure.

Hotraco Agri (Netherlands) is a supplier of computer-based control and monitoring systems for pig and poultry farms. These include HVAC (heating, ventilation, and air conditioning) systems, feed and water control, animal weighing, and egg counting. The control systems use internally CAN networks. Via an up to 500-m CAN backbone network, it is possible to connect several controllers in different houses. CAN switches with four ports are used to bridge the backbone to the local in-house CAN or CANopen networks. For poultry barn ventilation and air conditioning, pad cooling and nozzle systems are used. The Mira-P poultry computer manages and controls all common barn situations and processes, such as ventilation, heating, cooling, the registration of feed and water, as well as weighing of birds. Cascaded via CAN, the Mira-P controllers can be connected to the Smartlink gateway. The latter allows access to the controllers via a PC or a smartphone.

Figure 3: The control systems for poultry farms include HVAC (heating, ventilation, and air conditioning) systems, feed and water control, animal weighing, and egg counting (Source: Adobe Stock)

Farming robots are coming

In recent years, agricultural robots have moved into smart platforms providing physical interaction with the environment. Unmanned agricultural ground vehicles (UAGVs) have a huge potential to optimize crop yields and increase sustainability. For example, some already available automated guided vehicles use electrical motion controllers with CANopen interfaces by Maxon or Dunkermotoren.

Robotic and artificial intelligence are used to improve precision of the crop irrigation. Agricultural robots enable weed monitoring and control in spite of variability in the field conditions. The involved perception systems can detect and classify weed plants from crop plants, and weed control mechanisms cover both chemical and mechanical weed control. In orchard operations, robotic technologies are used for major tree fruit production tasks, including robotic pruning, thinning, spraying, harvesting, and fruit transportation. Mechanical harvesting machines such as canopy and trunk shakers are widely used for collection of some crops. These machines incorporate artificial vision systems to perform a pre-grading of the product in the field. For example, harvest-assist platforms in citrus orchards are capable of both inspecting collected fruits and separating them into categories.

Figure 4: In-built perception systems allow robots to inspect and collect ripe fruits (Source: Adobe Stock)

Collaborative robots (Cobots) and robot swarms are mainly in prototype and research status. Small automated and self-propelled units instead of a big machine are the trend. For example, the grubber is no longer a single unit with a 9-m working width. Instead, several smaller units are interconnected wirelessly. Thus, depending on the field size, it is not necessary to provide the maximum capacity in every case.

The growing number of robotic milking installations on farms has been driven by the need for better labor management and improved quality of life for dairy producers. The robotic milking systems (RMS) on farms consider barn design, feeding management, and udder health in automated systems. The trend towards robotic milking is set to continue into the future. Automation in meat processing operations is challenging, as the robotic systems have to deal with deformable biological products that lack uniformity. Some advances in robotic automation are achieved for the processing of fish, beef, pork and lamb, as well as poultry.

Future trend: Precision agriculture

Precision agriculture is a farming management concept, which considers the different potential soil productivity inside of a field. It is based on observing, measuring, and responding to given field conditions. The goal is to enhance productivity and optimize resource efficiency. Involved technologies include GPS (global positioning system), GIS (geographical information system), and GNSS systems. The ability to locate the precise position in a field allows for the creation of spatial maps for such measured variables as crop yield, topography, moisture levels, nitrogen levels, pH, and others.

This data can be collected by CAN-connected, real-time sensor arrays mounted e.g. on GPS-equipped combine harvesters. In conjunction with satellite imagery, the data is used by variable rate technology (VRT) ▷

including seeders, sprayers, etc. to optimally distribute resources. Recent technological advances have also enabled the use of real-time sensors directly in soil, which can wirelessly transmit data.

Precision agriculture is also enabled by unmanned aerial vehicles (drones), which can include CAN-based networks. These agricultural drones can be equipped with

Figure 5: Equipped with cameras, the agricultural drones capture multispectral field images to build precise topography maps used to correlate crop health with topography (Source: Adobe Stock)

cameras to capture multispectral field images used to process and analyze vegetative information. Providing of additional geographical references such as elevation allows to build precise topography maps used to correlate crop health with topography. The correlation results help to optimize crop inputs such as water, fertilizer, herbicides, and growth regulators through variable rate (VRT) applications.

The IoT (Internet of Things) technology comes into play with the interconnection of sensors and the farm-management software. Via web-based applications the farmers can gather precise information about the field conditions and react on them correspondingly. Smartphones and tablets are increasingly used in precision agriculture as they come with helpful applications (e.g. camera, GPS, accelerometer) and are portable, affordable, and have a high computing power. Dedicated agriculture applications such as field mapping, tracking animals, obtaining weather, and crop information can also be installed. A variety of agricultural machine manufacturers provide smartphone applications to control and monitor of some tractor and implement functions.

These innovations can also be used for the welfare of animals. Cattle can be outfitted with internal sensors to keep track of stomach acidity and digestive problems. External sensors track movement patterns to determine the cow's health and fitness, sense physical injuries, and identify the optimal times for breeding. All this data from sensors can be aggregated and analyzed to detect trends and patterns.

The machine learning technology (artificial intelligence) uses the data input from different sources to process the information and to control the actuating machines in the optimized way. It may also provide predictions to farmers at the point of need, such as the contents of plant-available nitrogen in soil, to guide fertilization planning. As agriculture becomes ever more digital, machine learning will underpin efficient and precise farming with less manual labor.

IoT gateway for agriculture vehicles

Figure: Claas and Liebherr co-operate regarding IoT applications (Source: Liebherr)

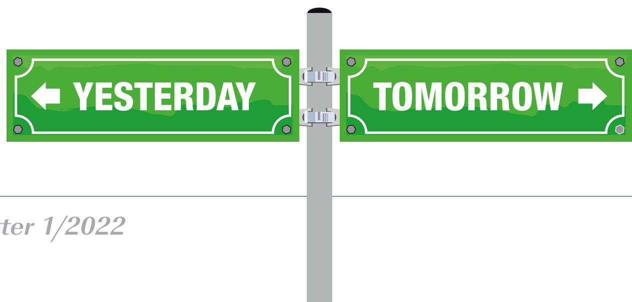
Claas, the manufacturer of agriculture machinery, uses the programmable IoT gateways by Liebherr in its combine harvesters, forage harvesters, and tractors.

The IoT gateway links Claas' digital services with the CAN-based in-vehicle networks using Isobus protocols. The web-based digital services include data management and precision farming. While tilling the fields, the machine continuously collects data and saves it in the cloud, so that the farmer can access it for future optimization. This data collection enables the targeted management of agricultural land by means of adapted fertilization and regulation of the sowing rates. The real-time remote diagnosis capability in case of a fault, maximizes the machine's availability. Every day, tens of thousands of Liebherr IoT gateways ensure the efficient connection of machines worldwide.

Outlook

Machine vision, navigation, actuation, communication, and control technologies help to save labor, improve precision and enhance efficiency in agricultural operations. CAN plays an important role for interconnection of the sensing, actuating, and controlling equipment. In sophisticated agriculture machines, there are up to ten CAN networks. In the future, also this industry will backbone such networks by means of an Ethernet network. AEF is working on an Ethernet-based high-speed Isobus. CAN FD and CAN XL may also be considered for embedded implement communication.

More and more farms around the world are automated. Current agricultural robotics systems are still limited and fully robotized farms are not yet available. Should more autonomous robotic systems become feasible, the role of humans in agriculture will not be eliminated. Humans will still be needed for supervision and collaboration. ▷



The agriculture industry, powered by the work of machines, increases the need for IoT-based smart solutions. Precision agriculture is an application of digital farming technologies such as satellite navigation and imaging, robotics, IoT, and machine learning. Observing, measuring, and responding to given field conditions, precision agriculture enhances productivity and optimizes resource efficiency. This is increasingly required in the future to satisfy the growing demand for food and beverage. ◄

Author

Olga Fischer
CAN Newsletter
pr@can-cia.org
www.can-newsletter.org

Standards and specifications

(Source: Adobe Stock)

This section provides news from standardization bodies and nonprofit associations regarding CAN-related documents. Included are also recommended practices, application notes, implementation guidelines, and technical reports.

ISO 11898-1 and ISO 11898-2 are under revision

In January, the ISO Working Group (WG) 3 of Subcommittee (SC) 31 of Technical Committee (TC) 22 started to review the ISO 11898-1 standard (CAN data link layer and physical coding sub-layer). CAN in Automation (CiA) has submitted the CAN XL data link layer specification (CiA 610-1) and the CAN FD Light specification (CiA 604-1) for integration into ISO 11898-1. Editors of the standard, officially called project leaders, are Florian Hartwich and Dr. Arthur Mutter (both are working with Bosch). The new edition will comprise all CAN data link layer protocols (Classical CAN, CAN FD, CAN FD Light, and CAN XL). This includes the specification of the Classical Base Frame Format (CBFF), the Classical Extended Frame Format (CEFF), the FD Base Frame Format (FBFF), the FD Extended Frame Format (FEFF), and the XL Frame Format (XLFF).

The above-mentioned WG 3 convened by Holger Zeltwanger (CiA Managing Director)has also started to revise ISO 11898-2 (CAN physical media attachment (PMA) sublayer). The new edition will include the documents submitted by CiA: the CAN SIC (signal Improvement capability) PMA specification (CiA 604-1) and the CAN SIC XL PMA specification (CiA 610-3). The CAN SIC XL transceiver supports the optional PWM (pulse-width modulation) coding in the dataphase at the attachment unit interface (AUI). All other CAN transceivers specified in ISO 11898-2 feature an NRZ (non-return-to-zero) coding. Editors of the new document are Yao Yao and Holger Zeltwanger from CiA. ■

CiA specifications to be released

The CiA 610-1 and CiA 610-3 documents specifying the CAN XL data link layer and CAN SIC XL physical layer will be published soon as Draft Specifications (DS). This means, they are part of the 1-year CiA 600 document series subscription. This subscription includes also the CAN FD Light specification (CiA 604-1), also released soon as DS. Subscribers receive for one year all documents of this series released as DS.

The CiA 400 document series subscription comprises all CiA profile specifications in DS state. The CiA profiles for lift control systems (CiA 417 series), for refuse collecting vehicles (CiA 422 series), for medical contrast media injectors (CiA 425-2), and for photovoltaic systems (CiA 437 series) will be released within 2022 as Draft Specifications (DS). Additionally, the CiA profiles for low-voltage switch gear devices (CiA 442), for container-handling systems (CiA 444 series), for RFID devices (CiA 445), and for pump devices (CiA 450) are prepared for publication as Draft Specifications. Further candidates, to be released in DS status are CiA 457 (CANopen profile for wireless communication), CiA 458 (CANopen profile for energy measurements), and the CiA 459 series (CANopen profile for in-board weighing devices). ■

CiA workshops scheduled

CiA organizes several online workshops to initiate further specifications and technical reports. The CiA workshop on aerial working platforms (AWP) and other fire-fighting vehicle body sub-systems is scheduled on March 22. The objective is to identify new profile specification work items. Additionally, the workshop evaluates the requirements for embedded networks in stabilization leg sub-systems. Interested CiA members can register for this free-of-charge workshop.

CiA plans further workshops on cybersecurity, truck body gateways, drilling machines, laboratory automation, and battery management. Furthermore, a workshop on configurable physical layer infrastructure devices (such as bridges and switches) is in the pipeline. It covers also devices connecting Classical CAN, CAN FD, and CAN XL network segments. All these workshops will be scheduled soon. Interested parties may contact CiA office for more details. ■

SAE J1939 related documents

The new edition of the quarterly updated digital annex (DA) of J1939 has been published in January this year. This spreadsheet comprises Suspect Parameter (SP) and Parameter Group (PG) specifications and other application profile related items. It includes also references to other documents specifying J1939 PGs, for example, those standardized in DIN 4630 for commercial vehicle body applications. Typical DIN 4630 devices control tail lifts, truck-mounted cranes, refrigerators, and tippers. The German standard written in English language also comprises the gateway unit to the in-vehicle networks. This is the base for the DIN 14704 standard, which specifies the gateway for fire-fighting trucks. It is currently under development and will also be published in English language. The CiA SIG (special interest group) fire-fighting is observing this standard.

The J1939/21 (J1939 application layer and mapping to Classical CAN) has been released with improved session information. This allows to indicate, if a segmented message has been aborted by the initiator or the responder node. This was an issue in Isobus applications, when two nodes transmit the same parameter group longer than 8 byte. Recently, there was another finding regarding the pause timing parameters of the transport protocols. In Figure C1 the value needs to be corrected to 10 ms to 200 ms. This will be done in the next release coming shortly.

End of last year, the version 3.00 of the Digital Tachograph Specification for remote company card authentication and remote data downloading has been released by the Heavy Truck Electronic Interfaces Working Group (DTCO). Unfortunately, the references to ISO 16844 series documents are unclear or they point to withdrawn documents (e.g. ISO 15765-3). This will be fixed in the next version to be released as soon as possible. ■

DroneCAN and UAVCAN

Drones use increasingly embedded CAN networks, the DroneCAN higher-layer protocol will support the mapping to CAN FD in the next version (Source: Adobe Stock)

DroneCAN is the open source higher-layer protocol used by the Ardupilot and PX4 projects for communication with CAN-connectable drone peripherals. It was developed to continue the development of the UAVCAN v0 protocol. The proposed introduction of the UAVCAN v1 protocol involved changes to the original approach that increased complexity and did not offer a smooth migration path for existing deployments. After extended discussions within the UAVCAN consortium, which is a member of CiA, it was decided that the best solution was to continue development of DroneCAN v0 under the name DroneCAN. Starting with DroneCAN v1, the protocol will evolve to add new features to assist in the widespread adoption of CAN throughout the UAV (unmanned arial vehicle) industry. The DroneCAN project is committed ensuring this evolution is done in a manner, which retains compatibility with existing DroneCAN devices. Key feature for the next version is the support of CAN FD. ■

Status of CiA documents

CiA develops and maintains technical specifications and technical reports. They run through different stages. In the beginning, there are Work Drafts (WD). The first specification release status is called Draft Specification Proposal (DSP). These are only accessible for CiA members. The next stage is Draft Specification (DS). Such documents can be purchased by non-members, too. There are different CiA document series, which can be subscribed for one year. This means, all DS documents released in a calendar year are provided to the subscriber.

The last status is Public Available Specification (PAS). These documents can be downloaded free of charge from CiA's website ((DEEP LINK)). Such specifications are rather mature and have been implemented by many parties.

CiA Technical Reports (TR) comprise recommendations, application notes, and implementation guidelines. Normally, they can be downloaded free of charge from CiA's website. Exceptionally, they can be limited to CiA members and document series subscribers. ■

Improving automotive CAN diagnostics

(Source: Adobe Stock)

As automotive CAN FD networks are proliferating throughout today's road vehicles, it is important to diagnose, if there is a fault on the CAN lines. As new features find their ways into the vehicle, the number of CAN nodes increase as well as the overall complexity of the communication network has created the need for transceivers with network diagnostic capabilities.

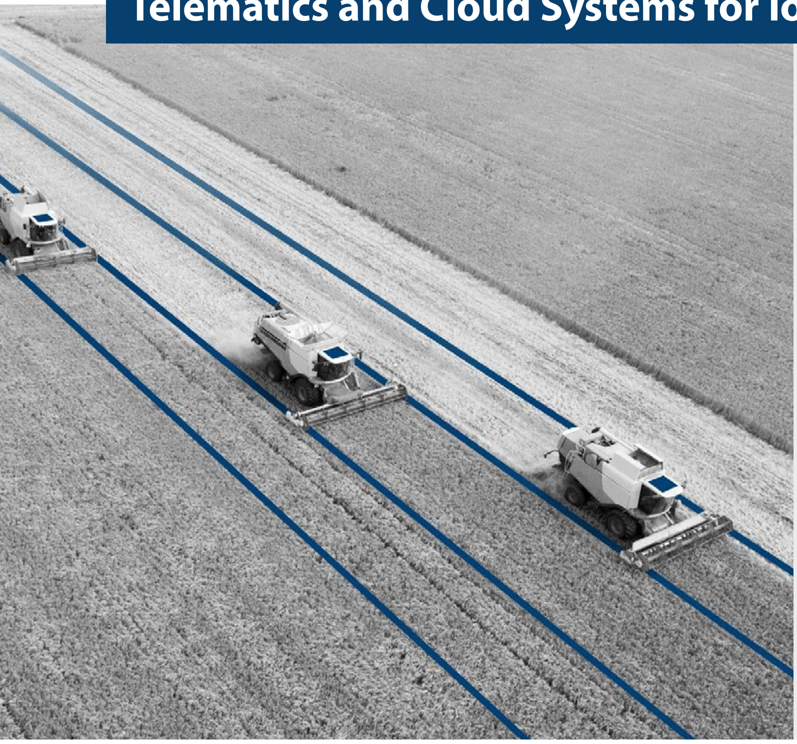
Legacy CAN high-speed transceivers compliant with ISO 11898-2 served their purpose in delivering robust CAN communication throughout the vehicle, but lack the ability to communicate network fault conditions when they occur. Transceivers have, over time, migrated from an 8-pin component to more complex components by adding pins. These more complex components come in 14-pin packages, but are still basically the 8-pin components with an added nFault pin that marginally addresses a network fault condition. System-basis chips (SBCs) are also rapidly being adopted across numerous applications throughout the vehicle. As such, CAN FD transceivers and CAN FD SBCs must become smarter and need more capable interface with the MCU (microcontroller unit) than a general purpose pin control. This interface could be Serial Peripheral Interface (SPI), which offers high bandwidth for communicating the latest features of a smarter transceiver or SBC. Some of these components include fail-safe modes, which can intervene if a CAN node is otherwise stuck in a higher power state. This prevents the transceiver from needlessly draining the battery or allowing invalid data frames on the CAN network during certain fault cases. This article considers methods to avoid invalid data and how TI's CAN transceivers and SBCs can help a node's local processor determine if an issue exists on the CAN network.

By understanding the amount and complexity of electronics is increasing each year, transceiver architecture improvements are needed. These new complexities need more useful information and control in order to enable the most robust CAN node architectures. Improved network diagnostics is one area that has been lacking. Electronic control units (ECUs) tend to follow a general architecture. It will consist of a local MCU, communication ports (CAN FD, LIN, Ethernet), and power. There will often be other specialized interfaces such as motor drivers, LED drivers, and cameras. The ECU's primary function could be for advanced driver assistance system (ADAS), body electronics and lighting, infotainment and cluster, or even electric vehicle/hybrid electric vehicle (EV/HEV) applications. For such systems, CAN FD is an appropriate interface, because of its higher data throughput and robustness, when compared to other automotive communication options.

Sontheim

High-end Connectivity and Data Management

Telematics and Cloud Systems for IoT and Service 4.0



Continuous digitization for smart vehicles

Modular on-board units – from cost-saving entry telematics up to high-end modules. Including updates-over-the-air, embedded diagnostic functionality and up to 4× CAN channels (CAN FD ready).

Sontheim IoT Device Manager and IoT Analytics Manager – for a highly secure, comfortable and individual visualization as well as management of your data and fleet.

COMhawk® xt – Telematic ECU Series

- Up to 4× CAN acc. to ISO 11898
- LTE, WLAN, Bluetooth, LAN
- Multi-protocol support (J1939, J2534, UDS, KWP, …)
- Positioning (GNSS)
- Embedded diagnostic functionality
- Integrated update-over-the-air functionality

In applications like ADAS or radar, knowing if the CAN network has some common faults would be beneficial to the system designer or vehicle repair technicians. Understanding if there is a network fault and not just a faulty ECU and possibly general location could reduce help reduce down time. Knowing this difference allows services to avoid un-needed warranty component replacements. If the network has a fault that prevents communication between one or more of the nodes on the CAN network, diagnostics can be difficult. In comparison, in a scenario where only one ECU has an issue, communications may not be blocked, but some other action is required for resolution.

In many CAN FD networks, the CAN high (CAN_H) and CAN low (CAN_L) lines are used in a line topology with 120-Ω termination resistors at each end. Another CAN network configuration is a star topology with a central 60-Ω termination resistor. For our examples, we will consider a mostly linear, non-star topology.

Figure 1 depicts a simplified three-node CAN network. The CAN FD transceiver must be able to handle certain network fault voltages that can swing between -42 V and +42 V for 12-V battery systems and between -58 V and +58 V for 24-V battery systems.

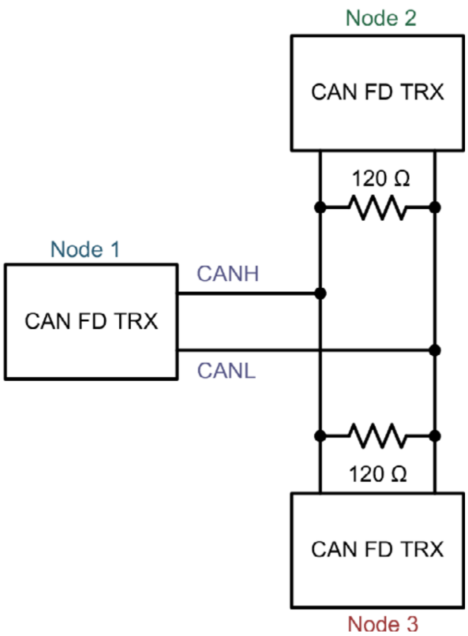


Figure 1: Three-node CAN FD network example (Source: Texas Instruments)

Legacy CAN transceivers from 8-pin to more capable 14-pin components have limited capability to communicate back to the MCU. 8-pin transceivers need all pins just for control, while 14-pin transceivers have added extra pins that can communicate limited information back to the MCU. Some 14-pin components have added the capability to detect certain network fault conditions such as CAN_H or CAN_L shorted to battery (Vbat), shorted to ground or being open (no termination between CAN_H and CAN_L). Communicating this fault information back to the MCU is challenging due to the single GPIO pin only communicating a high (logical 1) or low (logical 0) status. An example could be a nFault pin; a low indicates that a fault has occurred, but no real information is shared on what the fault was. Many SBC's include Serial Peripheral Interface (SPI) communication, yet the network condition communication between the transceiver and MCU has progressed very little.

Though it is possible to determine the presence and type of network fault, the location of the fault on the CAN network can influence how it appears to a connected transceiver. Let's start our analysis by considering the three-node configuration in Figure 1 and applying different network faults. Network faults typically manifest as opens and shorts. Figure 2 and Figure 3 show different scenarios of CAN_H and CAN_L being open. The location of the open lines can determine whether the fault is detectable.

In Figure 2, the opening occurs at Node 2 or Node 3. The whole network could detect this fault condition because one or both terminations are missing. When the fault happens at Node 1, only Node 1 will detect the fault. Node 2 and Node 3 will detect a "good" network, because the end-point termination is intact and therefore cannot report that an opening has occurred at Node 1. Figure 3 provides further examples, where either CAN_H or CAN_L is open, but these may not hamper network communication.

Network faults that are the result of a short have their own set of challenges. The short can be either CAN_H or CAN_L shorted to Vbat, Vcc, or ground, as well as CAN_H and CAN_L being shorted together. When shorted together, CAN_H and CAN_L could also be shorted to Vbat, Vcc, or ground. Figure 4 and Figure 5 show different cases for the short condition.

The faults shown in Figure 4 show cases where only one CAN line is shorted. In these cases, CAN data may be degraded, but communication might still be possible. With network fault detection, the issue can be identified confidently as a network short condition rather than seemingly random occasional communication failures. The issue arises when considering faults 10 and 11 shown in Figure 5. To understand the issue requires considering both Figure 4 and Figure 5 with the fault conditions shown. Faults 7 and 8 are distinct faults that a system would be able to identify as different. The issue is the ability to distinguish between fault 7 and fault 10 or between fault 8 and fault 11. A system may have both faults indicated when it is one or the other.

The faults shown in Figure 5 show cases, where both CAN_H and CAN_L are experiencing a short. During such conditions, it is unlikely that CAN data frames can be transmitted on the network. With clever design of a network fault detection circuit, each of these cases can be identified as unique fault conditions and ease suspicions of other hardware problems. Knowing which of these disruptive faults is occurring can help pinpoint which section of the CAN network needs service or repair to get the CAN network back online.

When a transceiver can determine a network fault has taken place, the system designer can decide the best method for communicating a fault condition. This communication could be a service light on the dashboard or stop communication with the nodes. Table 1 lists the fault conditions and whether the location of the fault can be determined. The information provided on a fault condition along with the CAN network architecture understanding ▷

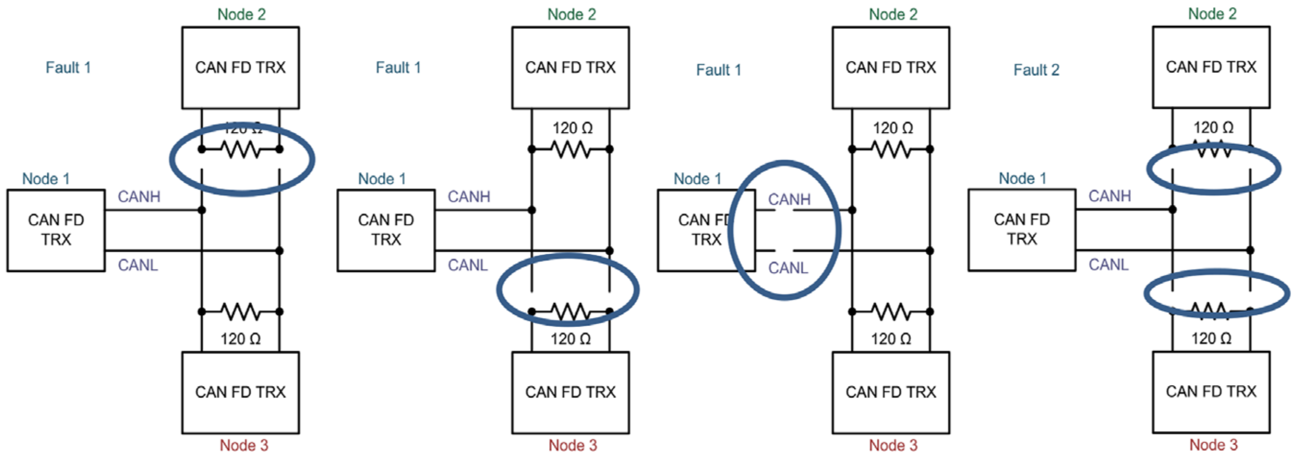


Figure 2: CAN_H and CAN_L both are open at same time (Source: Texas Instruments)

could be used by a service department to help narrow down possible locations of a fault.

As CAN FD communication and functional safety continue to grow in importance, network-fault diagnostics should be a consideration during the CAN network development process. Considering only the network fault tolerances of a CAN transceiver is becoming insufficient for today's robust networks. When autonomous vehicles become more ubiquitous, network fault tolerances will no longer be enough and smarter transceivers with advanced network diagnostic capability will be required.

Original equipment manufacturers (OEMs) are requesting more detailed information on network faults in transceiver solutions. In the future, CAN networks will need to be designed in a manner that will utilize smarter transceivers to help determine network faults and their locations. The ability to communicate with the MCU by providing diagnostic information will enable the future CAN network to be more robust. Such transceivers will provide reliable information to the system diagnostic methodologies that can help resolve network failures. To accomplish this, the transceiver functionality needs to go beyond network faults and a close collaboration between the CAN network designer and CAN transceiver manufacturer is required. Future smart transceivers can provide network diagnostic information back to the MCU, which can enhance the ▷

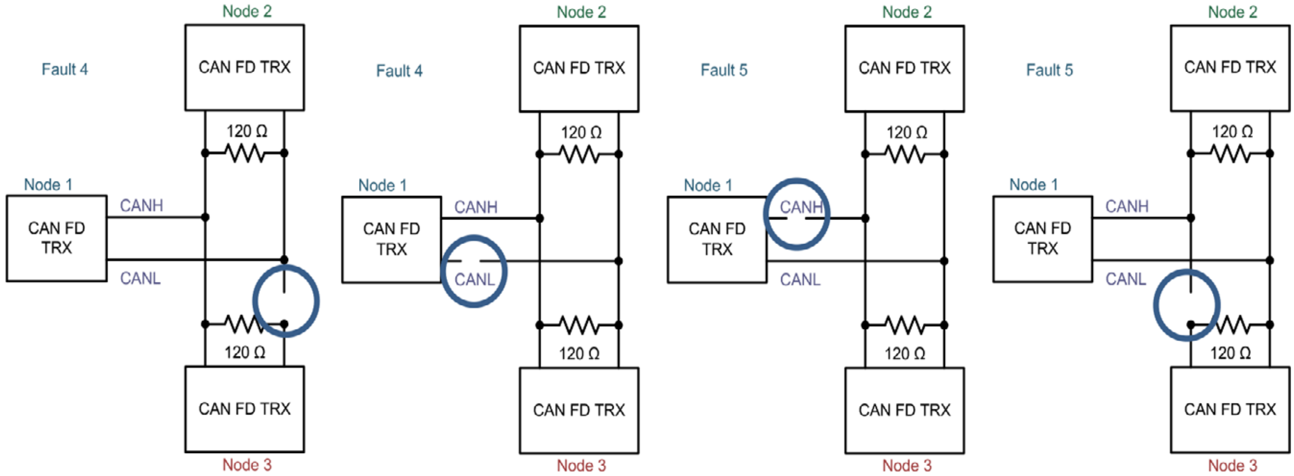


Figure 3: CAN_H or CAN_L are opened individually (Source: Texas Instruments)

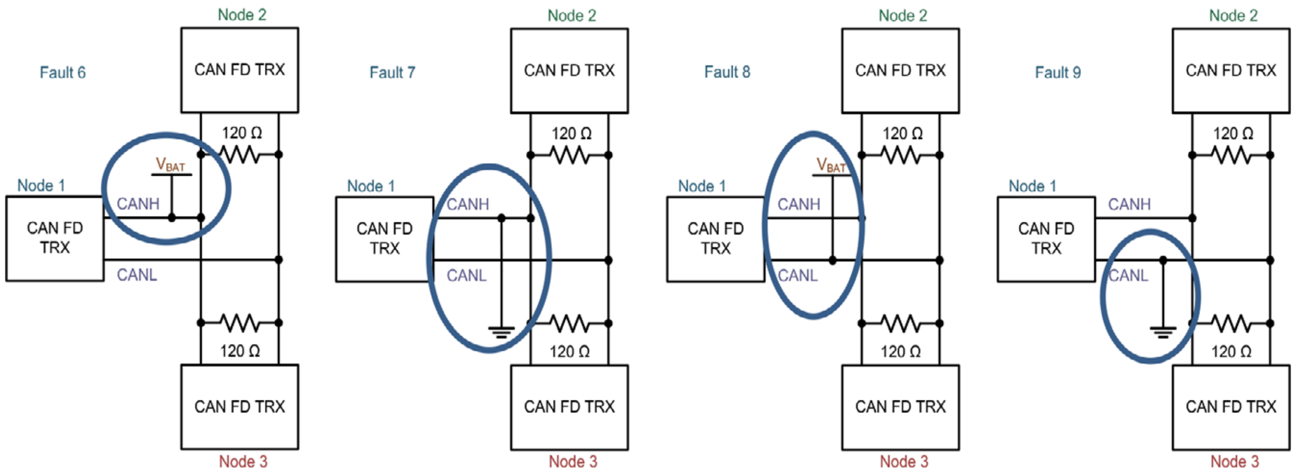


Figure 4: CAN_H or CAN_L shorted to Vbat or ground (Source: Texas Instruments)

robustness of a CAN network. Network fault diagnostics needs to be a system level design effort that includes a smart transceiver such as TCANxxxxx. If a critical fault is occurring at the electronic control unit, then the general communication of the network can be compromised. For complete coverage of a node, a system-level diagnostic solution is needed for each node and the ability to communicate this information back to a central controller.

Future CAN transceivers

What if an open fault condition takes place at Node 1 before a sleep command? The node may stay in a high- ▷

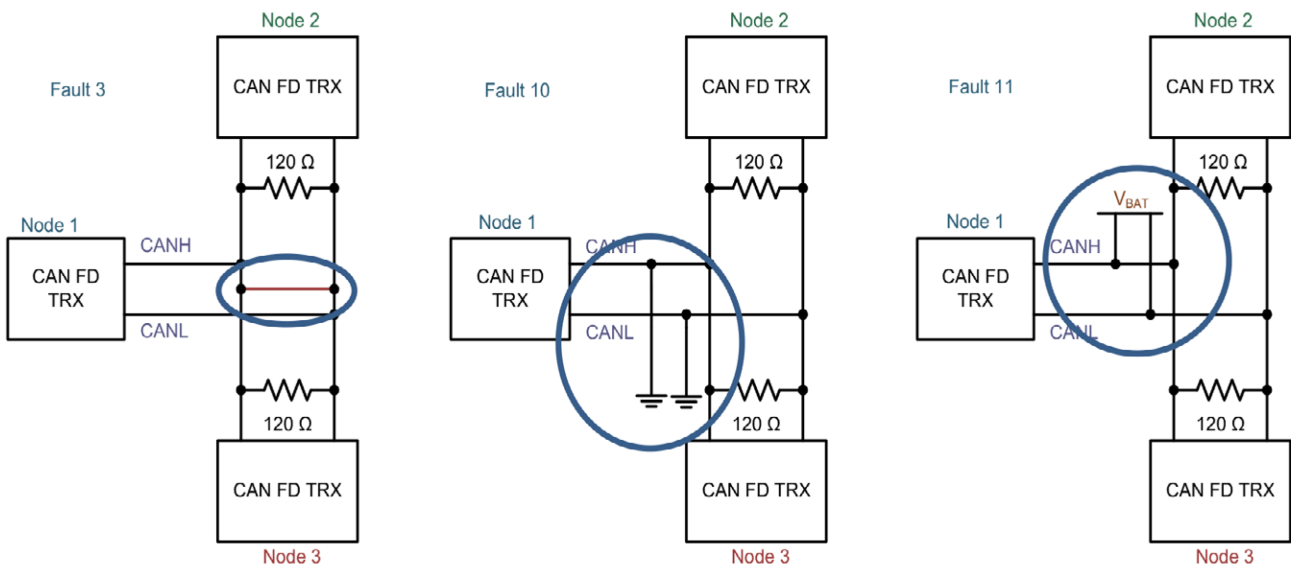


Figure 5: CAN_H shorted to CAN_L examples (Source: Texas Instruments)

Table 1: Network fault conditions and fault-location capabilities (Source: Texas Instruments)

Fault No.	CAN_H	CAN_L	Fault detected
1	Open	Open	All smart transceivers see this fault as missing termination, whether seeing no termination or seeing 120 Ω instead of the expected 60-Ω termination
2	Open	Open	Depending upon the open location, the smart transceiver can diagnose this fault as no termination
3	Shorted to CAN_L	Shorted to CAN_H	Yes, but not the location
4	Normal	Open	• Transceiver 1 can detect this fault but cannot tell the difference between it and fault 2 or 5 • Transceiver 2 and Transceiver 3 do not see this as a fault
5	Open	Normal	• Yes, but cannot tell the difference between this fault and fault 2 and fault 4 • Transceiver 2 and Transceiver 3 do not see this fault
6	Shorted to Vbat	Normal	Yes, but not location
7	Shorted to GND	Normal	Yes, but cannot tell the difference between this and fault 10
8	Normal	Shorted to Vbat	Yes, but cannot tell the difference between this and fault 11
9	Normal	Shorted to GND	Yes, but not the location
10	Shorted to GND	Shorted to GND	Yes, but cannot tell the difference between this and fault 7
11	Shorted to Vbat	Shorted to Vbat	Yes, but cannot tell the difference between this and fault 8

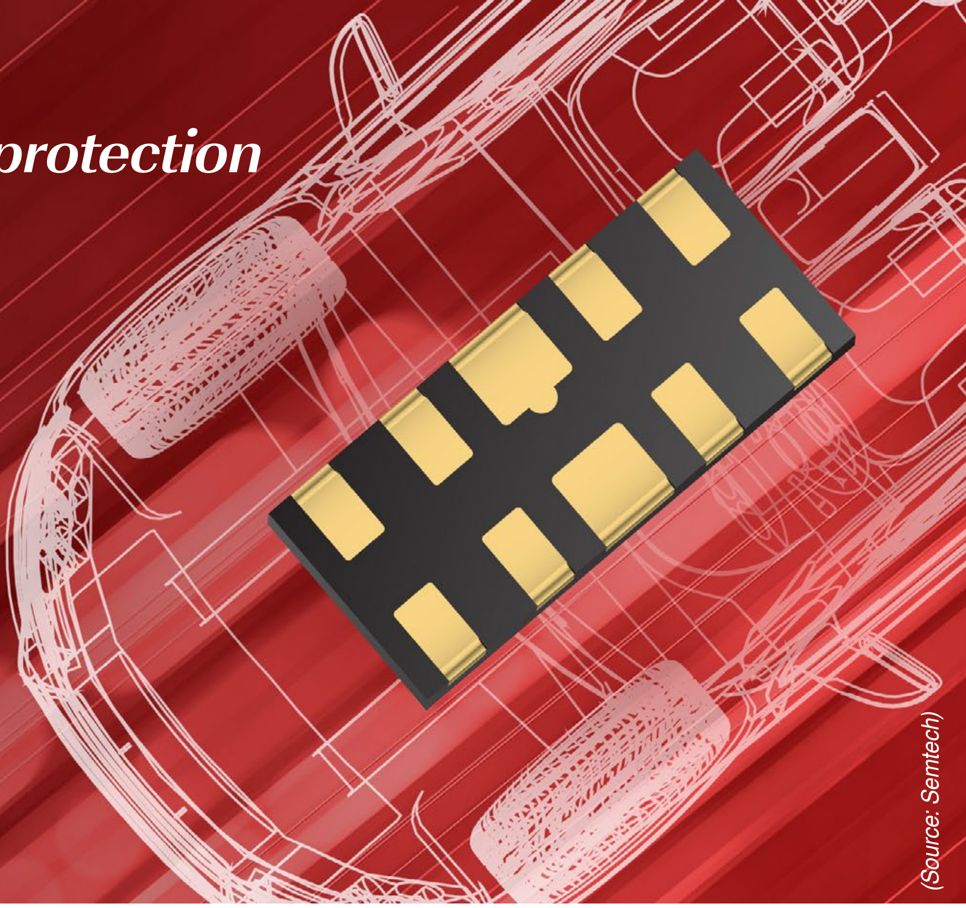
power state which could drain the battery. An example of this could be a car parked at the airport for a couple weeks. Smart transceivers that have advanced network diagnostics and a network designed to utilize the transceiver could mitigate the situation where the owner of the car returns home to a dead battery at the airport and thus avoiding a bad day. Texas Instruments has two transceivers today that support this advanced bus fault diagnostic capability, TCAN1144-Q1 and TCAN1146-Q1. ◀

Author

Richard Hubbard
Texas Instruments
info@ti.com
www.ti.com

Automotive CAN protection

In the harsh automotive environment, careful design and proper TVS (transient voltage suppression) diodes are crucial for safeguarding the communication networks and interfaces. Semtech's portfolio of TVS products protects CAN.



(Source: Semtech)

Motor vehicles have gone through much progress since their inception. Modern cars include autonomous and semi-autonomous driving, anti-lock braking systems, electric power steering, forward and rear collision warning, lane assistant, autonomous parking assistant, and automatic emergency braking. Advanced features such as GPS navigation, interior mood lighting, surround-view camera, advanced infotainment system, active antenna are standard in most modern vehicles.

Each vehicle feature is usually monitored and controlled by an individual electronic control unit (ECU). In a modern vehicle, there are about 50 ECUs to 100 ECUs, with each ECU responsible for one or more functions. The ECU works with multiple sensors such as the engine temperature sensor, air pressure sensor, door sensor, etc. It receives information from the sensors and adjusts the vehicle parameters under control accordingly. Sometimes one ECU may need to communicate with other ECUs to perform a designated function. For example, if you forget your car key in the ignition, the corresponding engine control ECU communicates with the door ECU to keep the door open and the speaker ECU to sound the alarm.

ECU communication via CAN

There are several in-vehicle network (IVN) protocols for data transmission between ECUs inside a vehicle. The most popular communication mechanism in modern vehicles is CAN. The bi-directional serial communication network allows ECUs to communicate without using any complex wiring. A twisted pair cable with a characteristic impedance of 120 Ω is used to transmit the data. One of the wires is called the CAN_Low (CAN_L) and the other, CAN_High (CAN_H), with a data transfer rate of 1 Mbit/s. The ECU is connected to the CAN network via a CAN controller, similar to a micro-controller that handles all the necessary data processing activities. There is a CAN transceiver that interfaces between the CAN controller and the CAN network. It converts the transistor-transistor logic (TTL) signal into the actual differential voltage signal for the CAN network to read and interpret. The CAN architecture is shown in Figure 1.

Transient protection of CAN

When designing a CAN interface system in a harsh automotive environment with 50 ECUs to 100 ECUs, ensuring sufficient protection from electrical overstress events (EOS) is imperative. One of the primary causes of EOS is electrostatic discharge (ESD). Moreover, with the miniaturization of the electronic components, it is even more essential to protect the components from ESD threats and meet modern-day vehicles' safety and reliability requirements.

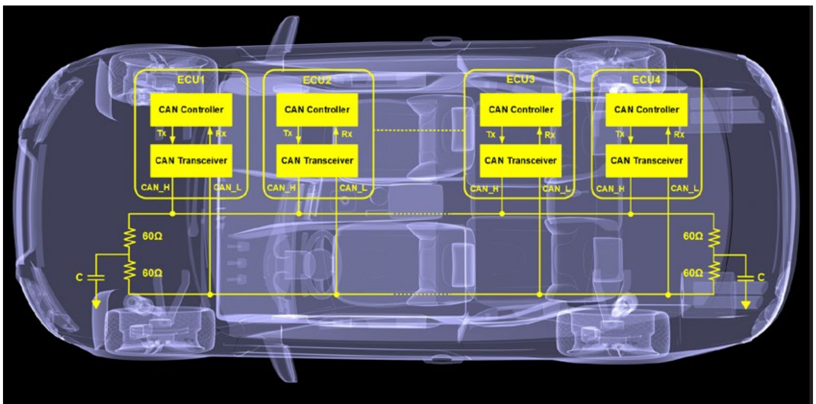


Figure 1: Automotive CAN network architecture (Source: Semtech)

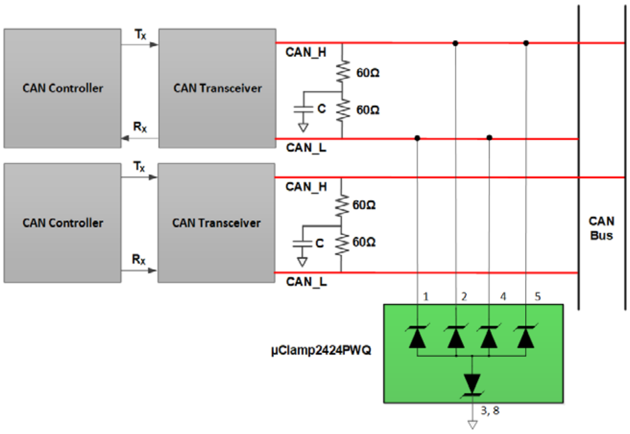


Figure 2: Possible ESD protection options of a CAN system (Source: Semtech)

Transient protection can be achieved by placing a transient voltage suppression diode on a CAN network data line to protect against transient events during the fast rise time in less than a nanosecond. Under normal operating conditions, the TVS diode presents a high impedance path to the protected circuit, so the device appears as an open circuit. It does not interfere with the rest of the circuit. During a transient event, the voltage on the terminals of the protected CAN transceiver can exceed safe operational limits. The TVS diode offers protection by providing a low impedance path so that the transient current is diverted away from the transceiver circuit. At the supposition of the ESD event, the TVS diode reverts to a high impedance state.

As mentioned before, the CAN network consists of two wires named CAN_H and CAN_L. CAN_H reaches 3,75 V when transmitting any data. At the same time, the CAN_L drops down to 1,25 V. When the CAN network is not transmitting any data, both CAN_H and CAN_L remain at 2,5 V. But we have to remember that a car generally uses a 12-V battery. Also, if a jump-start is required, it is done through a 24-V battery. So, the first criteria to select a TVS diode is the reverse working maximum voltage or VRWM, which should be sufficient to protect the CAN transceivers if the car's 12-V battery requires a jump-start from a 24-V battery in an emergency.

Another parameter that needs to be considered for selecting a TVS diode is the minimum breakdown voltage or VBR. It is the voltage when a TVS diode starts to conduct the current mentioned as a leakage current in the product's datasheet in any transient scenario. Semtech's µClamp2424PWQ (shown in Figure 2) is a four-channel device that can protect two sets of CAN_H and CAN_L in the CAN network architecture. µClamp2424PWQ has an operating voltage of 24 V with a minimum breakdown voltage of 26,5 V. These voltages are sufficient to protect the CAN transceivers even if the vehicle needs to be jump-started.

Now let us talk about another vital parameter called clamping voltage or Vclamp. The Vclamp is the voltage of a TVS diode that appears across the device at the maximum peak pulse current rating. Vclamp determines the voltage that the device endures during a transient event. A lower clamping voltage is suitable for the protection of a CAN system or any other system. The typical clamping voltage of µClamp2424PWQ is 44 V at a maximum peak current of 5 A. Each device line is rated for a maximum EOS current of 5 A (tp = 8/20 µs).

The CAN_H and CAN_L lines carry a differential signal with a maximum data-rate of 1 Mbit/s. Since they are high-speed differential data lines, TVS diodes should protect the circuit during transient events while ensuring signal integrity by maintaining a very low line-to-line capacitance. µClamp2424PWQ offers an extremely low capacitance of 15 pF (typ) and 18 pF (max) between the line and the ground. This fact makes it a suitable candidate to protect the CAN transceivers without undermining the signal integrity.

Conformance to level 4 IEC61000-4-2 standard and AEC-Q qualification are also mandatory requirements for automotive system design. µClamp2424PWQ provides transient protection to ESD events at ±30 kV (Air) and ±30 kV (Contact) as per the IEC 61000-4-2 standard. The device is available in a DFN (2,5 mm x 1,0 mm x 0,55 mm) package with state-of-the-art side wettable flanks for automatic visual inspection (AVI) post assembly. Figure 3 shows the features of µClamp2424PWQ.

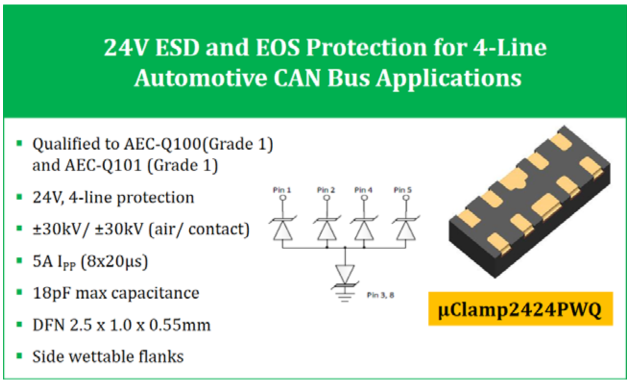


Figure 3: Features of µClamp2424PWQ (Source: Semtech)

Conclusion

Semtech is a leading manufacturer of TVS diodes that protects many of the world's high-speed automotive communication networks. In the harsh automotive environment, careful design and proper TVS diodes are crucial for safeguarding the communication networks and interfaces. Semtech's well-performing and reliable portfolio of TVS products protects high-speed automotive CAN as well as other communication networks. ◀

Author

Anindita Bhattacharya, PhD
Semtech
info@semtech.com
www.semtech.com

This article originally appeared on Inside Out, Semtech's corporate blog.

Automotive

Managing complexity of automotive software

Most cyberattacks remain undetected until it's too late, so early detection is a must. As the connected car evolves, it is recommended that cybersecurity configuration be performed remotely with an enterprise security management system.

The automotive industry is driven by a group of mega-trends called, "automation, connectivity, electrification, and sharing" commonly referred to as Aces. Aces represents a new opportunity for the automotive industry to meet an entirely new set of challenges. A key challenge is dealing with the increasing software in today's modern automobile. Today, there are more lines of code in the connected car than other more highly sophisticated machines such as the U.S. Air Force F-35 Joint Strike Fighter, Boeing 787 Dreamliner or the U.S. Space Shuttle1. Hardware today is more powerful and, as a result, millions of lines of code can be executed through a multitude of systems to perform complex functions inside the connected car. Soon, these vehicles will communicate externally by way of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Safety and security are paramount concerns, so all onboard systems must be secure while the vehicle is in motion – or sitting idle.

Cybersecurity threats are ever increasing

The "2020 automotive cybersecurity report" (Figure 1) from Upstream Security depicts a six-fold increase over a nine-year time period with numbers doubled from 2018 to 2019. The graph depicts a 94 percent year-over-year (YoY) growth in cyberattacks since 2016. New business models will have to evolve as complexity, reliability, risk, and liability become primary drivers.

The increased effectiveness and proliferation of automotive cyberattacks has created a new urgency for security solutions, driving new regulations by lawmakers to prevent cyberattacks globally. The U.S. Security and Privacy in Your Car Act, or also called the "Spy Car Act of 2017", defines requirements for protection against unauthorized data access and reporting. The bill directs the National Highway Traffic Safety Administration (NHSTA) to issue vehicle cybersecurity guidelines that require motor vehicles manufactured for sale in the United States to build in protection against unauthorized access to electronic controls and driving data.

Also in 2017, the U.S. House of Representatives passed H.R. 33886, "The Self Drive Act", a first-of-its kind legislation to ensure the safe and innovative development, testing, and deployment of self-driving automobiles. China established an automotive cybersecurity committee to ensure the safe operation of intelligent, connected, and electric cars, including research, standards, policies, laws, and regulations. Other data regulations are beginning to emerge, such as the EU's GDPR (general data protection regulation), Canada's Digital Privacy Law (Pipeda), and the European Parliament Transport Committee's call for EU regulation on access to car data.

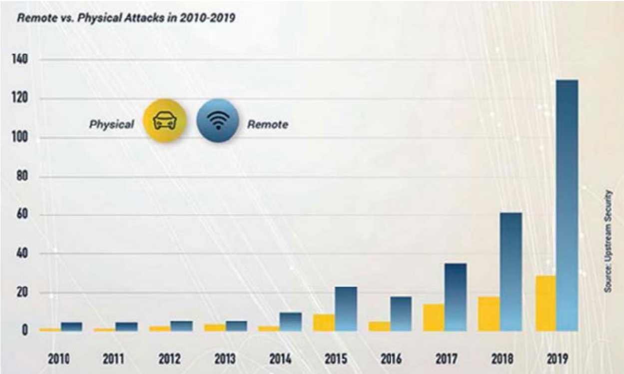


Figure 1: Over the past several years, remote automotive cybersecurity incidents have increased dramatically. As more connected vehicles enter the market, the potential for attacks rises exponentially (Source: Upstream Security)

NHTSA's automotive cybersecurity research program takes a threat analysis approach to cybersecurity, placing threats into six different categories:

- Spoofing – where a person, program, or device conceals itself as something it is not by manipulating data to gain an illegitimate advantage.
- Tampering – intentional data alteration to harm the consumer. For connected cars, this includes modifications to configuration data, software, or hardware used in vehicle control systems.
- Non-repudiation – where a statement's author cannot successfully dispute validity or authorship.
- Info disclosure – refers to many types of sabotage related to data leakage.
- Denial of service (DoS) – refers to a cyberattack where a machine is flooded with excessive requests from an attacker forcing it to become unavailable for legitimate users by overloading its systems and preventing legitimate requests from being fulfilled.
- Elevation of privilege – where an attacker can abuse a machine and perform unauthorized activities by gaining illegitimate access to systems resources and data, causing more damaging attacks.

Connected car attack surfaces

By understanding these threats, OEMs (original equipment manufacturers) can look at four potential attack surfaces of the connected car:

- The first attack surface is direct physical, including access to the on-board diagnostics (OBD) port, charging port, or harness connectors. A car becomes vulnerable when a hacker has direct physical access, such as at the dealer or repair shop for maintenance or repairs, or when a second party has gained access to the vehicle, like a parking valet who could execute a direct physical attack.
- The second attack surface is indirect physical. Here, a carrier is needed to execute the attack, such as a USB stick or CD that compromises the car's firmware, or SD cards and firmware updates which open up all kinds of attack possibilities.
- The third possibility for attack is through wireless. Bluetooth and the mobile network are prone for wireless attacks and increased automotive systems connectivity has dramatically increased the potential for attack.
- The final attack surface is sensor fooling. Researchers have shown that these types of attacks are possible in a laboratory setting. Connected and autonomous cars often use light detection and ranging (Lidar) sensor technology, causing systems to be blinded or fooled with false information to harm the vehicle operator and occupants. GPS is another technology with vulnerabilities that could be exploited.

Mapping attack surfaces to a vehicle's architecture (Figure 2) depicts attack surfaces corresponding to a vehicle's architecture. This basic schematic highlights ▷

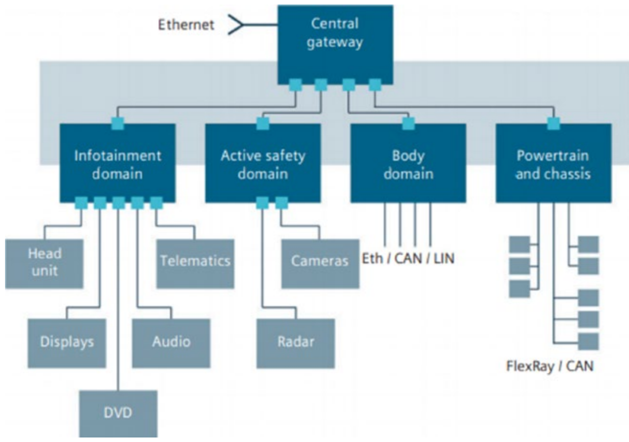


Figure 2: Attack surfaces and corresponding functional units (Source: University of California, San Diego, "Comprehensive experimental analyses of automotive attack surfaces")

connectivity within the car, including the use of automotive gateways and multiple vehicle networks, and different types of domains: infotainment, active safety (containing cameras and radar), and body. Chassis and powertrain ECUs (electronic control unit) utilize a CAN network that can be easily exploited. Also shown are a variety of networks to communicate data within the central gateway. The central gateway ECU is a focal point of attack because of its direct exposure to the outside world.

It is quite clear that modern connected cars have multiple entry points, which hackers view as both a challenge and opportunity. To prevent any type of cyberattack, all entry points must maintain an appropriate level of security.

Security can be broken down into three aspects. The first aspect includes authentication and access control. Authentication means who is allowed to do things inside a vehicle. Access control is what the individual or system is allowed to do once inside. The second aspect to security is protection against illegitimate access, data leakages, or harmful software or Trojans from being installed. The final aspect to defining security is to detect and report security incidents.

A multi-layered security approach is needed

Knowing the attack surfaces within the connected automobile provides the foundation for a multi-layered security approach. Automotive OEMs must secure all internal and external communications. An embedded firewall to protect the vehicle from accepting unauthorized traffic, data, or signals sent by a malicious IP address must be part of the mix. The following are critical components to secure a connected car:

Embedded firewalls: Building a firewall into a vehicle is a highly-specialized process tailored exclusively to the automotive environment. To build the firewall, a software development kit (SDK) is integrated directly into the communications stack, whether CAN, TCP/IP, or other connected solution. The embedded firewall must be highly configurable with built-in flexibility, operate across a range of vehicle ECUs, and work with a real-time operating system (RTOS) or even in the Autosar environment. Many cyberattacks begin by sending packets to the connected car, seeking weaknesses, so if the firewall can detect this ▷

CANcrypt for secure communication

As already mentioned, CANcrypt from Esacademy's (Emsa) can be used to secure communication. Commonly used security methods for authentication and encryption/decryption on the Internet cannot be easily applied to CAN/CANopen. Emsa's solution is a combination of scalable security features for CAN. The in-depth description of CANcrypt is available as book: "Implementing scalable CAN security with CANcrypt, authentication and encryption for CANopen, J1939, and other Controller Area Network or CAN FD protocols".

CAN Newsletter Online

The CAN Newsletter Online as well as the magazine, already reported several times about ways of cybersecurity and CAN, provided by Emsa.

Security column

Updates and outlook on securing CAN

Over the past years, Olaf Pfeiffer and Christian Keydel from Embedded Systems Academy (Emsa) have published several security-related CAN articles in the CAN Newsletter magazine. It's now time for an up-to-date summary, review, and outlook.

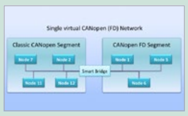
Read on

CAN Newsletter magazine

Classical CAN/CAN FD security threats

The authors of this article already have introduced various technical solutions for distinct security threats. This time, they want to take a step back to look at the bigger picture of CAN security.

Read on

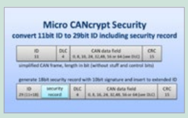


CAN Newsletter magazine

Smart-bridging CANopen and CANopen FD

This article gives an description on how to smart-bridge classic CANopen and CANopen FD networks.

Read on

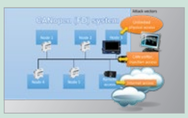


CAN Newsletter magazine

CAN security: how small can we go?

What kind of CAN security can still be added to a deployed CAN system if the processors have only medium performance and only adding a few kilobytes of extra code is possible?

Read on



CAN Newsletter magazine

CANopen FD multi-level security demonstrator

Many CAN-based networks open multiple attack vectors for hackers, especially after they have gained access to the system either remotely through a gateway or even physically.

Read on

activity early and ensure certain packets are not allowed to be received or forwarded, a potential attack will be thwarted before it even begins. Controlling what ports and protocols used to receive messages for the vehicle is crucial to protect and report suspicious activity.

Embedded firewalls for ECUs: Adding a firewall to a central gateway requires portable source code that can be integrated and configured into the ECU. Filtering rules built into the firewall block specific IP addresses and recognize unwanted activity with quick response to prevent an attack – firewall support of different types of filtering capabilities (CAN network, rules-based, threshold-based, static) is critical, including stateful packet inspection. Logging and reporting attacks enable intrusion detection, which is knowing when something unusual is happening. The connected vehicle must be able to report nefarious activity back to a vehicle operations center allowing security operations teams to take the necessary action and share that information across the security network.

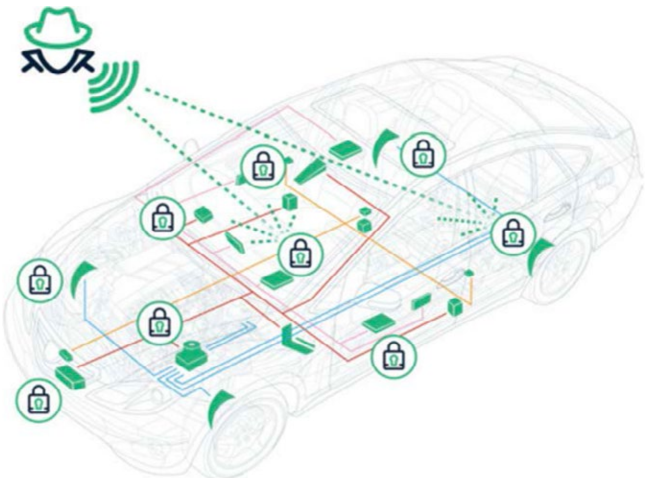


Figure 3: Securing ECUs from cyberattacks by employing an embedded firewall and certificate-based authentication (Source: Sectigo)

A firewall on an external gateway ECU manages communication with all outside entities, serving as the bullseye for attack by enabling filtering rules for all vehicle communications. Its job is to detect and block attacks before they reach the target ECUs. A firewall on an internal gateway ECU is another option. With multiple networks within the car, an internal gateway ECU allows communication between different networks to isolate safety critical functionality – the more critical internal systems are protected from potentially malicious network traffic. Finally, a firewall can be on an endpoint ECU, the actual control ECU that manages critical functionality in the vehicle. Control ECUs include anti-lock brakes, airbags, steering control, etc., so it is advisable to deploy a firewall on multiple endpoint ECUs.

Secure communication: There are numerous use cases for secure communication, including communication between the car and external systems, V2V communication, and communication within the car. V2V communication is more common and critical today, so it must be protected. To achieve secure communication within the car, all ECUs must be protected. As a communication session begins, the origin of that communication is known, so encryption is recommended. Encrypted communication uses IP protocols such as TLS, DTLS, and SSH. If running over a CAN network, CANcrypt can be used. All data encrypted using strong cryptography is required to ward off cyberattacks.

Authentication: During a communication session (Figure 3), authentication verifies that who you are communicating with is actually who they say they are, i.e., is the other device or process really who it claims to be? For authentication, a public key infrastructure (PKI) to manage and issue digital certificates is crucial. Every ECU must be identifiable and PKI-based certificates provide strong authentication for machine-to-machine communication. Another aspect of PKI security is code signing to enable secure boot and secure updates. With V2I communications, high-speed automated certificate issuance is mandatory since hosting and managing the entire process securely is essential. Where is the certificate authority hosted? How is certificate issuance performed? Is it automated? Is it secure? How are private keys protected?

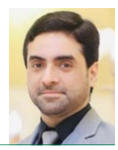
Finally, an OEM may have its own internal strategy for securing the connected car with a proprietary safety ecosystem. But when considering V2I or V2V communications, where vehicles from multiple OEMs travel the same road, vehicle manufacturers must construct a shared ecosystem with the same requirements for security, management capabilities, and other safety-related capabilities to ensure interoperability among all vehicles on the road.

Conclusion

To protect today's connected cars, multiple layers of security are required, and all attack surfaces must be taken into consideration. Most cyberattacks remain undetected until it's too late, so early detection is a must. As the connected car evolves, it is recommended that cybersecurity configuration be performed remotely with an enterprise security management system. This integration provides centralized management of security policies, situational awareness, and device data monitoring, event management, and log file analysis for data analytics. Security needs to be a shared common resource. Embedded firewalls, secure communication, and strong authentication techniques are vital elements that constitute a multi-layered security approach. ◀

Reference

[1] Robert N. Charette. "This car runs on code", IEEE Spectrum, February 2009.



Author

Dr. Ahmed Majeed Khan
Siemens Digital Industrie Software
info@siemens.com
www.siemens.com

Automotive

CAN measuring unit for mobile machines

Micro-electro-mechanical system (Mems) inertial sensors are commonly used for orientation, pose estimation, and tracking. Due to their size and cost, they are used in automotive and industrial applications. Gemac introduces its point of view.

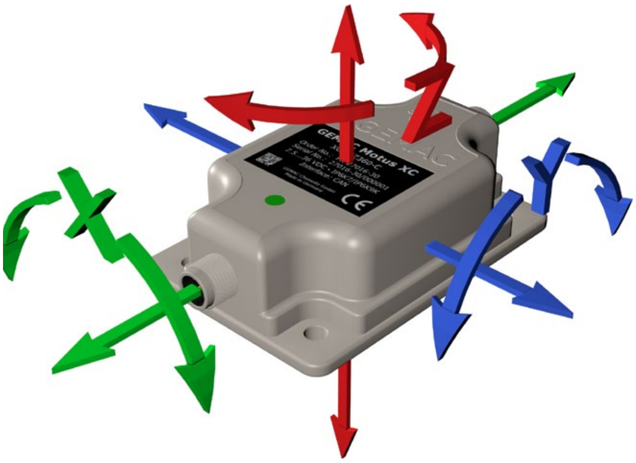


Figure 1: Gemac Motus is a 6 degrees-of-freedom inertial measurement unit with a 3-axis accelerometer and a 3-axis gyroscope (Source: Gemac Chemnitz)

With Gemac Motus, a configurable sensor measuring unit was designed for the most varied fields of application to perform 6-axis motion acquisition on mobile machines, such as construction vehicles, agricultural machines, forestry machinery, cranes and hoisting equipment, as well as vessels.

The sensor consists of a 3-axis accelerometer measuring the external forces acting on the sensor in all three spatial directions, including gravity. This makes the accelerometer the perfect choice for measuring the orientation or inclination of the device for static cases which means, without the influence of external forces besides gravity. The 3-axis gyroscope allows the measurement of the turn rate as angular velocity around the three sensor axes. The orientation can also be calculated from the gyroscope data by integrating the turn rate over time. The advantage of the measurements from the gyroscope is that it is not affected by external accelerations, which makes it suitable for dynamic applications. By combining the accelerometer and gyroscope data using a so-called sensor fusion filter, the sensor can provide precise orientation information in static and dynamic applications, making the sensor fusion technology crucial for mobile machines.

Integrated calculations for precision

Traditional IMU's (inertial measurement unit) only provide the raw data for acceleration and angular rate to a controller unit, where further calculations, like integrating the signals, are performed. This brings potential inaccuracies, resulting from signal delays, different time stamps, or rounding of the numbers. Gemac Motus includes calculations in the measurement unit, like, for example, the integration of the angular rate to angle values using internal high precision timestamps. With the internal calculation, the stability of the gyroscope output data can be im-proved essentially (see Figure 2). The already preprocessed data can then be output on the CAN network, thus saving computation time and memory in the controller unit.

Besides the acceleration and angular rate in all three directions, Motus provides the output of inclination values in the format of quaternion, Euler angles, or perpendicular ▷

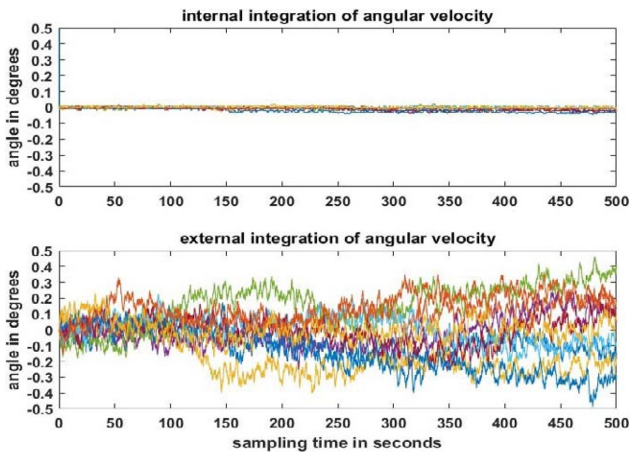


Figure 2: Comparison of the integration of gyroscope data by the sensor itself (top) and by an external control unit (bottom). The integrated data processing leads to a lower standard deviation of the signal and thus to more precise data (Source: Gemac Chemnitz)

Figure 3: Example application with different mounting positions (Source: Gemac Chemnitz)

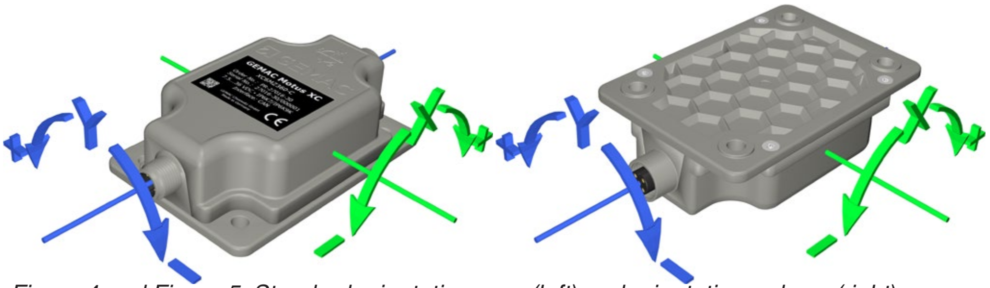


Figure 4 and Figure 5: Standard orientation z-up (left) and orientation z-down (right) (Source: Gemac Chemnitz)

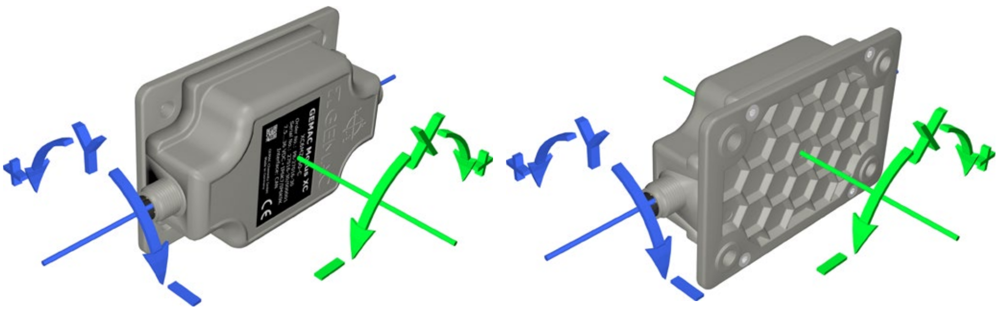


Figure 6 and Figure 7: Orientation y-up (left) and orientation y-down (right) (Source: Gemac Chemnitz)

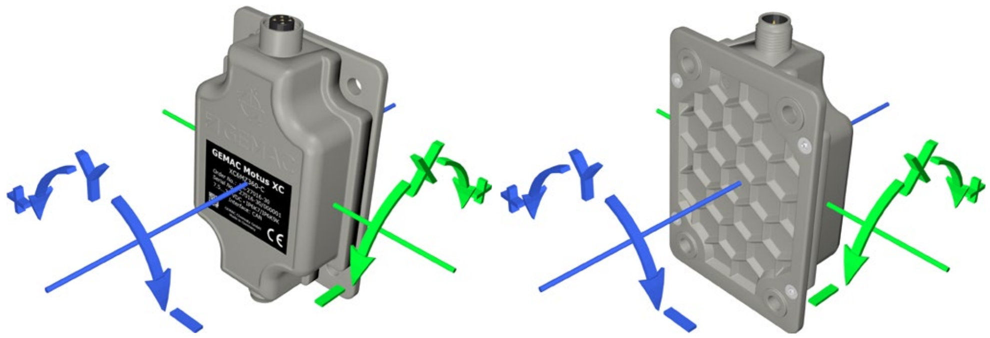


Figure 8 and Figure 9: Orientation x-up (left) and orientation x-down (right) (Source: Gemac Chemnitz)

angles. Both angle formats can be output with or without sensor fusion, covering both static and dynamic applications.

The CANopen version implements the CiA 301 (version 4.2.0) CANopen application layer and communication profile. The CANopen device profile for inclinometers (CiA 410 version 2.0.0) is supported for the inclinometer function. The output signals can be mapped to up to four TPDOs (Transmit Process Data Objects). The J1939 version provides several standardized Parameter Groups like slope sensor information - Parameter Group Number (PGN) 61481, acceleration sensor (PGN 61485), and angular rate information (PGN 61482). Further, a set of proprietary messages is available, allowing flexible and user-specific mapping of the required output signals.

Motus provides 360-degree orientation estimation independent from the mounting position of the sensor. The user can define the measurement axes by selecting one of six possible device orientations. Furthermore, the sensor can determine its mounting position by user command and automatically transform its internal coordinate system to best match the device orientation. Additionally, the user can enter an offset to both axes for inclination measurement without restricting the sensor's measurementrange. Thus, the sensor can be adapted to every possible measure-ment scenario.

Key parameters for IMU selection

Scale, offset, and alignment errors, nonlinearities: One of the main error sources of Mems-IMUs comes from misalignment of the measurement axis to the sensor housing and from gain and offset errors of the inherent sensing elements. As these types of errors tend to be stable, they can be measured and corrected during production of the sensor. At Gemac, each sensor is calibrated on a high precision rotation stage, limiting all these combined errors to an angular precision of 0,15 ° (typical 0,1 °). ▷

Table 1: The variants NB, NC, and IB compared (Source: Gemac Chemnitz)

Variants	***NB***	***NC***	***IB***	
General parameters	Inclination		Accelerometer	Gyroscope
Measurement range	360 °/±90 °		±8 g	±250 °/s
Resolution	0,01 °		0,244 mg	0,00875 °/s
Temperature	±0,01 °/K	±0,0016 °/K	0,2 mg/K	0,005 °/s/K
Static accuracy	±0,3 °	±0,1 °		
Dynamic accuracy	±0,5 °	±0,25 °		
In run bias stability				2,5 °/h
Angle Random Walk				0,1 °/√h
Interface	U, I, CAN, CANopen, SAE J1939		CAN, CANopen, SAE J1939	

Table 2: The variants XB and XC compared (Source: Gemac Chemnitz)

Variants	***XB***			***XC***		
General parameters	Inclination	Accelerometer	Gyroscope	Inclination	Accelerometer	Gyroscope
Measurement range	360°	±8 g	±250 °/s	360°	±8 g	±250 °/s
Resolution	0,01°	0,244 mg	0,00875 °/s	0,01°	0,244 mg	0,00875 °/s
Temperature coefficient	±0,005 °/K	0,2 mg/K	0,005 °/s/K	±0,0016 °/K	0,02 mg/K	0,005 °/s/K
Static accuracy	±0,3°			±0,1°		
Dynamic accuracy	±0,5°			±0,25°		
In run bias stability			2,5 °/h			2,5 °/h
Angle Random Walk (ARW)			0,1 °/√h			0,1 °/√h
Interface	CAN, CANopen, SAE J1939			CAN, CANopen, SAE J1939		

Temperature effects: Temperature changes in the sensor's environment result in shifts of scale factor and offset in Mems, inducing an error in orientation. Because these shifts are not linear and highly device-specific, the temperature effects cannot be foreseen. The maximum angular deviation due to temperature changes for Gemac Motus is 0,2 ° over the whole temperature range from -40 °C up to +85 °C.

Gyroscope bias stability: The offset or bias of the gyroscope output changes over time due to flicker noise in the Mems components. This noise with a 1/f spectrum is usually observed at low frequencies, leading to a long-term drift of the gyroscope data. The bias stability is typically expressed in °/h. Correcting the gyroscope bias during runtime is essential, especially when integrating the angular rate over time to calculate angle values from the gyroscope data. For example, an error of only one resolution step (0,00875 °/s for Motus) cumulates to an error of 31,5 ° during a one-hour measurement. The gyroscope bias can be ten or a hundred times higher in practice. Motus incorporates a dynamic gyroscope offset correction that adjusts the bias automatically during runtime or manually on request by the user.

Random walk: Another type of noise, the thermo-mechanical noise, is causing a randomly distributed error in the data, the random walk. This error can be observed for the accelerometer as velocity random walk and the gyroscope as angular random walk. Due to the noise, the integration of the signal will drift over time, where the standard deviation of the drift equals the random walk multiplied by the square root of the observation time.

Vibration rectification error: This error is also called g^2-sensitivity and causes a bias shift due to oscillatory linear accelerations. It is caused by asymmetries and nonlinearities in the sensor design and applies to both accelerometers and gyroscopes.

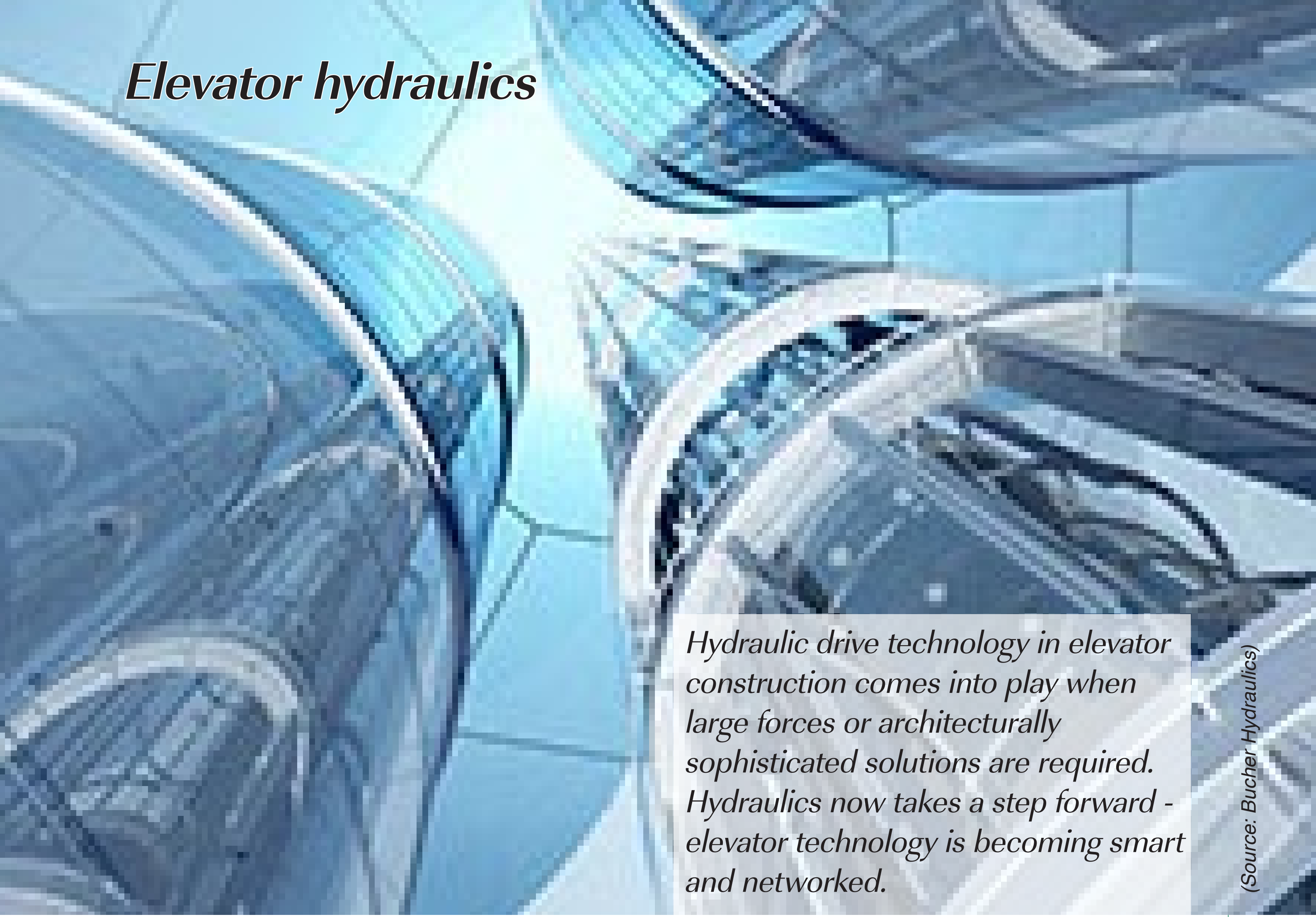
The IMU is available in 29 different application-related configuration options. The ISD-Control software for the IMU parameterization is available for a free download. It works with CAN adapters from various manufacturers. The units are dedicated for use in construction machinery, agricultural machinery, forest machines, cranes, lifting technology, and ships.

Depending on the customer's needs, the Motus offers different variants: Recording of inclination (Gemac Motus NB and NC), recording of acceleration and rotation rate (Gemac Motus IB), and recording of inclination, acceleration, and rotation rate (Gemac Motus XB and XC). In Table 1 and Table 2 the variants are compared. ◀

Author

Rico Gräßler
Gemac
info@gemac-chemnitz.de
www.gemac-chemnitz.com

Elevator hydraulics



(Source: Bucher Hydraulics)

Hydraulic drive technology in elevator construction comes into play when large forces or architecturally sophisticated solutions are required. Hydraulics now takes a step forward - elevator technology is becoming smart and networked.

Tony Aschwanden, Head of Product and Application - Elevator at Bucher Hydraulics in Neuheim, Switzerland, explained: "Freight elevators with high loads are the domain of hydraulic elevators. Equipped with one or more cylinders, they can lift loads of more than 40 tons over 25 meters and higher". A clear benefit of hydraulics: the forces can be transferred directly via the building foundation, whereas in the case of traction elevators they usually make their way into the building structure via the shaft head.

But these powerhouses can also look elegant: another area of application is architectural elevators featuring large areas of glass, but with no sign of suspension ropes, which would have a negative visual impact and be distracting. A central cylinder, often a telescopic design below the car, slim and shining, appears delicate and aesthetic. Modern designs even work without any lateral car guidance at all, for example with round glass cars. This allows elevator doors to be installed in any direction. The hydraulics themselves also keep a low profile: the power unit and other equipment fit in a wall cabinet or in the shaft.

Frequency inverter - No more oil than necessary

There are about five million elevators in the EU. They use about 18 terawatt hours of electricity per year, about 0,7 percent of the total electricity demand. That's why within the foreseeable future, elevators are to become subject to the EU Ecodesign Directive. A pilot study has already been completed under the leadership of the Fraunhofer Institute for Systems and Innovation Research (ISI). In terms of energy efficiency, however, hydraulic elevators have already been heading in the right direction for quite a long time. In fact, looking at their whole service life, they are usually superior to traction elevators, according to a study by the Spanish technology ▷

Figure 1: The iValve is an electronically controlled lift-control valve for controlling hydraulic elevators (Source: Bucher Hydraulics)

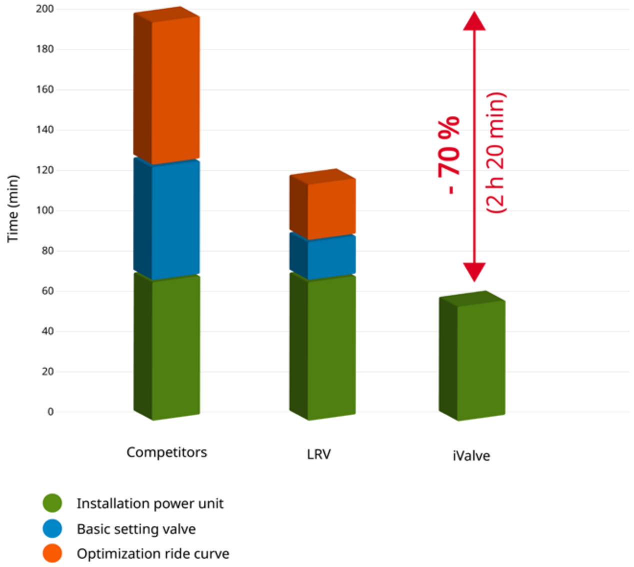


Figure 2: The iValve eliminates the basic valve settings and optimizes the travel curve (Source: Bucher Hydraulics)

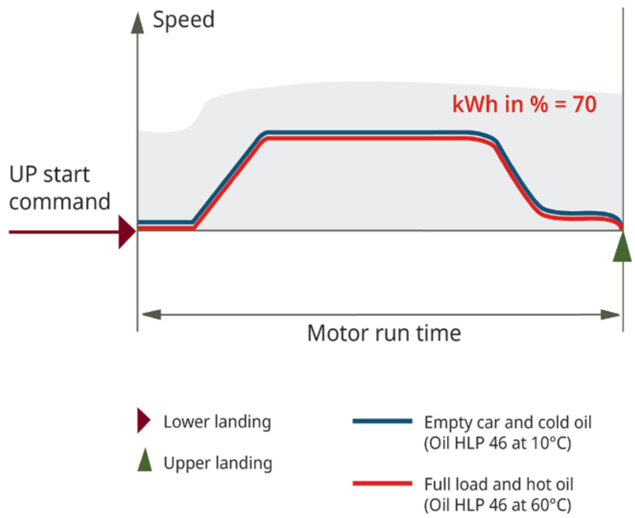


Figure 3: The lift-control valve automatically compensates for varying loads and oil temperatures (Source: Bucher Hydraulics)

center Instituto Tecnológico de Aragón (Itainnova). The Swiss Federal Office of Energy, in its study "Electricity Consumption and Savings Potentials in Elevators," also attests that typical hydraulic elevators in apartment buildings have lower maintenance costs than traction elevators.

A major factor in saving energy: the use of frequency inverters. Without a frequency inverter the pump's drive motor runs at full speed right from the start. The travel curve - i.e. acceleration, full speed, and deceleration - is controlled by a valve. The surplus oil is fed back to the tank in an energy wasteful manner, causing it to heat up unnecessarily. As a result, an oil cooler may even become necessary.

Frequency inverters, on the other hand, control the motor from as low as zero speed. As a result, only as much oil is pumped as is needed for the ideal travel curves. "With 30 to 40 percent energy savings, the extra cost of the frequency inverter pays for itself, especially in frequently used elevators," reasoned Aschwanden.

But there's more. One example: the use of supercapacitors, or supercaps for short. They can be charged and discharged much faster than rechargeable batteries. In addition, they withstand far more charging cycles. Among other applications, they became known for storing electrical energy in Kers, - the Kinetic Energy Recovery System - used in Formula 1 racing cars, and for regenerative braking in buses and trains. ▷

About Bucher Hydraulics

Bucher Hydraulics is an international provider of drive and control technologies, from the initial project phase to the finished product, for mobile and industrial hydraulic applications. Production facilities and sales centers are located in Europe, India, China, Brazil, and the United States. Target industries are construction machines, materials handling and lifting technology, municipal equipment, renewable energy, agricultural technology, mechanical engineering, and elevator technology.

Elevator builders worldwide, including not only global market leaders but also many medium-sized companies, use hydraulic elevator components from Bucher Hydraulics. The valves, power units, and cylinders can be found in passenger and freight elevators in airports, train stations, shopping centers, and commercial buildings. The elevators reach travel heights of 25 meters and more. The payload ranges from 320 kilograms to over 40 tonnes. The components can also be used to modernize existing installations and offer architects a wide creative scope. Machine room-less (MRL) hydraulic systems, for example, solve the problem of space and also meet design requirements. The systems are characterized by low maintenance requirements and high energy efficiency. They are long lasting, offer a very good cost-benefit ratio and can be modernized to make a decisive contribution to the deduction of the environmental footprint. Last but not least, passengers appreciate the ride comfort.

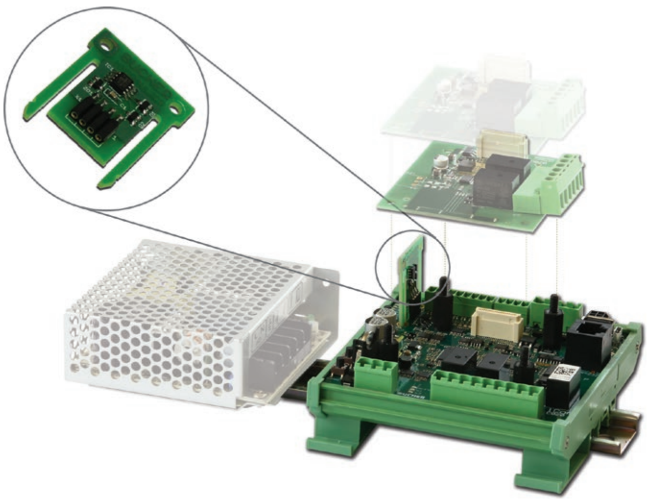


Figure 4: The iCon-2 electronic card checks the electronic control actions, the valve conditions, and the ride comfort. Travel curves are recorded in the electronic system. During operation, the travel curves for that particular elevator are optimized by the learning algorithm iTeach (Source: Bucher Hydraulics)

Figure 5: Is everything ok with the elevator? The iCon-2 controller delivers information directly to the lift controller via CANopen Lift (Source: Bucher Hydraulics)

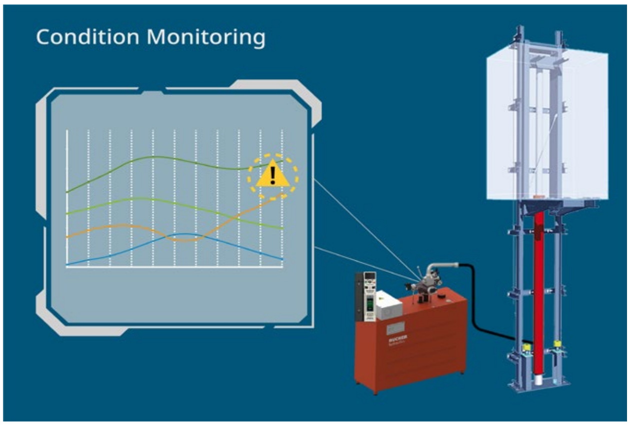


Figure 6: The iValve, in conjunction with the iCon-2 controller, provides data for predictive maintenance that helps prevent breakdowns (Source: Bucher Hydraulics)

Bucher Hydraulics has adapted this technology for elevators. It can even be retrofitted to existing units - with the appropriate software modifications. The oil displaced from the cylinder by the car drives the pump. The pump turns backwards and the motor generates electrical energy, which is temporarily stored in the supercaps via the frequency inverter. During the next UP travel, this energy is available and reduces the power consumption from the grid. Depending on the application, energy savings of 20 to 30 percent can be achieved this way. The system is particularly worthwhile in highly utilized industrial installations.

iValve in elevator hydraulics

Bucher Hydraulics is a member of the VDMA Bluecompetence initiative and has committed itself under the motto Ecodraulics. Based on this, they develop and manufacture products with a particular focus on energy-savings, low-emissions, long life, lightweight, and space-savings. A prime example: the intelligent hydraulic valve iValve for the elevator industry, with flow rates of 250 and 500 liters per minute (66 and 132 US gpm).

The iValve is a strategic optimization of the LRV (lift control valve) towards industry 4.0. It can be installed and put into operation significantly faster. Thanks to sensors and corresponding software the valve is self-learning and self-optimizing. In addition, it has extensive networking capabilities. This makes the iValve a future-proof choice, as it can be substantially retrofitted thanks to its modular design. Installation time is reduced by up to 70 percent compared with a mechanical hydraulic valve. Besides, it saves up to 30 percent energy. A very precise closed-loop control circuit ensures first-class ride quality and excellent leveling accuracy (± 3 millimeter) in both directions, regardless of the temperature and viscosity of the oil. "Smart" is the upcoming predictive maintenance, which makes it possible to respond before any damage occurs.

iTeach ensures commissioning

The installation and commissioning time for an iValve is only 60 minutes as opposed to 120 minutes for an LRV series valve or 200 minutes for a conventional valve. The installation time is shortened because only two connecting lines between the electronics and the valve are used instead of several cables to the pressure sensors. The major part of the time saving, however, is due to the complete elimination of the basic valve settings and the optimization of the travel curve. This is done by the iValve itself using iTeach based on the shaft information supplied by the lift control system. An initial travel curve after installation looks like this: start with long start-up phase and slow speed, full speed, deceleration, and again a long travel distance at slow speed until the valve stops. For a typical travel distance, this takes about 14,5 seconds between starting and stopping the car. The iValve optimizes itself during the first five travels via iTeach and reduces the total travel time to 8,5 seconds, which saves a lot of energy.

Networking made easy with CANopen Lift

In combination with the iCon electronics, the iValve offers every option for modern networking. The bus system used is CANopen Lift (read more on page 6), an open source quasi-standard in elevator engineering. This simplifies the wiring effort for the overall system and communication with the drive. Initial systems with this CANopen connection are in operation in Germany, the Netherlands, and Switzerland.

Thanks to the optional CANopen connection via plug-in card on the iCon controller, no additional terminals are necessary. The parameters can be changed centrally via the lift control system. The iCon board is equipped with a fault memory, which can be read out for analysis on site, or remotely using smart devices. For the elevator manufacturer, this is the direct path to predictive maintenance: the iValve can pass on status information, data log files, and warnings, which are sent to the lift control system, and from there they can be shared globally. And this does not just apply to new systems: it can also be retrofitted to approx. 50 000 systems worldwide. ◀

Authors

Bucher Hydraulics
elevator@bucherhydraulics.com
www.bucherhydraulics.com

1992 - 2022

On June 1 and June 2, CiA celebrates its 30th anniversary with an in-person event in Nuremberg (Germany).

30th CiA anniversary days

Day 1	
10:00 to 11:00	Registration and welcome coffee
11:00 to 12:30	**Session I (three 30-min presentations)** - Dr. Arthur Mutter (CAN XL) - Magnus Hell (CAN physical layer options) - Fred Rennig (CAN FD Light)
12:30 to 14:00	*Lunch break*
14:00 to 15:30	**Session II (three 30-min presentations)** - Christian Schlegel (Classic CANopen - The universal and flexible communication standard) - Uwe Koppe (The CANopen FD Story – Fast & Furious) - Holger Zeltwanger (J1939-based networks)
15:30 to 16:00	*Coffee break*
16:00 to 18:00	CiA general assembly
18:00 to 22:00	Get-together

Day 2	
09:00 to 10:30	**Session III (three 30-min presentations)** - CAN applications and implementations
10:30 to 11:00	*Coffee break*
11:00 to 12:30	**Session IV (three 30-min presentations)** - Thilo Schumann (UML usage in CiA documents) - Yao Yao (Overview on CiA technical groups) - Reiner Zitzmann (Generic CANopen bootloader)
12:30 to 14:00	*Lunch break*
14:00 to 16:30	BC and CiA group meetings

Subject to change without notice.

Reserve not just the date, but also a seat. The number of participants is limited due to the event location.

For registration please contact CiA office at events@can-cia.org

www.can-cia.org