CAN *Newsletter*

Hardware + Software + Tools + Engineering

30 years of CiA: Celebration and feedback

History and trends: CAN on construction sites

History and trends: CAN on rails

History and trends

www.can-newsletter.org

PCAN-Diag FD
New **J1939** Add-in

■ PCAN-Diag FD: CAN & CAN FD Diagnostic Device

The PCAN-Diag FD is a handheld device for the diagnosis of CAN and CAN FD buses at physical and protocol levels.

- High-speed CAN connection (ISO 11898-2)
  - Complies with CAN specifications 2.0 A/B and FD
  - CAN bus connection via D-Sub, 9-pin (CiA® 303-1)
  - Switchable CAN termination for the connected bus
- Power supply via rechargeable batteries or a supply unit
- Clear listing of the CAN traffic with various information
- Transmitting individual messages or CAN frame sequences
- Configurable, readable CAN ID and data representation
- Recording of incoming CAN messages
- Playback of trace files with optional loop function
- Measurement of the CAN bus load and termination
- Voltage check at the CAN connector for pins 6 and 9

Oscilloscope

- Function specially designed for CAN for a qualitative assessment of the signal course on the CAN bus
- Two independent measurement channels, each with a maximum sample rate of 100 MHz
- Display of the CAN-High and the CAN-Low signals as well as the difference of both signals
- Trigger configuration to various properties of CAN messages like frame start, CAN errors, or CAN ID

Now available with J1939 support

The new J1939 Add-in extends the functional range of the diagnostic device by the support for the SAE J1939 standard. The CAN data traffic is interpreted according to the included J1939 database and is represented in a way that is understandable for the user.

Features

- Representation of J1939 data interpreted according to PG and SP definitions
- SAE J1939 database with all definitions and the included parameters
- Decoding of multi-packet messages with payload data up to 1785 bytes
- Support for address claiming
- Display of DM and DTC diagnostic data

The J1939 Add-in is activated with a device-bound license which can also be purchased afterwards for a PCAN-Diag FD.

www.peak-system.com

Take a look at our website for the international sales 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

Applications

Interviews

Semiconductors

Brief news

Get your printed CAN Newsletter copy

CAN in Automation (CiA) participates at the following trade shows with an own stand: Innotrans (September 20 to 23, 2022), Bauma (October 24 to 30, 2022), and SPS (November 8 to 10, 2022). For this occasion, the September issue of the CAN Newsletter magazine 2022 is printed and distributed exclusively. All three exhibitions take place in Germany.

The Innotrans trade show for transport technology in Berlin is sub-divided into the five trade fair segments: railway technology, railway infrastructure, public transport, interiors, and tunnel construction. CiA staff can be found in hall 27, stand 290.

Bauma, which takes place in Munich is a trade fair for construction machinery, building material machines, mining machines, construction vehicles, and construction equipment. CiA's booth is in hall A2, stand 337.

At the SPS Smart Production Solutions in Nuremberg, the automation industry presents products, solutions, and the latest information about smart and digital automation. CiA staff can be met in hall 5, stand 410.

Table of contents

30 years of CiA: Celebration and feedback

On June 1 and 2, CiA and its members celebrated the 30th birthday of CAN in Automation in a nice location in Nuremberg in the midst of the city park.

(Source: CiA)

About 60 participants from 36 member companies and nine employees from CAN in Automation (CiA) joined the event. The event was an excellent opportunity to meet CAN fellows with different expertise and backgrounds. Besides the official program, there was plenty of time for individual talks in the breaks and on the first day's get-together. Most important for old and new CiA fellows was the opportunity to exchange experiences and knowledge, refresh personal networks, and establish new relations. Many participants took away new ideas for their future CAN product developments. The attendees also appreciated the detailed technical presentations and discussions with business partners, chipmakers, and competitors.

The success of the event may lead to the fact that more CiA community meetings will be held face to face. The newly-elected CiA Business Committee already discussed establishing of an annual event with technical presentations in conjunction with the General Assembly.

Day one: focus on new CAN technologies

Holger Zeltwanger (CiA Managing Director) has opened the day with a look-back to the CiA beginnings. Since the CiA establishment on March 5, 1992 with 13 member companies, the CiA membership increased to more than 720. CiA has released more than 25 000 pages of specifications and recommendations developed in about 40 CiA technical groups. There were published more than 120 issues of the CAN Newsletter magazine, and CiA organized 17 international CAN Conferences (iCC).

The first presentation session focused on recent CAN lower-layer developments CAN XL, CAN SIC XL, and CAN FD Light. Comparing features of the three CAN generations, Dr. Arthur Mutter (Bosch) gave an insight into the improvements achieved with the development of CAN XL. The achievable bit rates were shown in a graphics comparing Classical CAN, CAN FD, and CAN XL. Magnus Hell (Infineon) showed the different CAN physical layer options going through the history of CAN transceivers and Matthias Muth (NXP) compared the capabilities of the CAN SIC and CAN SIC XL transceivers regarding possible bit-rates and topology-dictated limits. A CAN SIC XL (signal improvement capability) transceiver can be used for bit rates of 10 Mbit/s and higher. The three experts are sure that CAN users are really good prepared for the future with CAN SIC and CAN SIC XL transceivers as they provide more freedom for different topologies.

In the next presentation, Fred Rennig (ST Microelectronics) gave an insight into CAN FD Light. The development was advanced by the automotive light industry, but industrial applications can profit from the simplified CAN FD data link layer as well. The solution offers cost ▷

Figure 1: Experts are sure that CAN XL brings great improvements on all areas and users are well prepared for the future with CAN SIC and CAN SIC XL transceivers (Source: CiA)

savings especially for industries deploying it in large piece numbers. In the second session Christian Schlegel (CS Consulting) and Uwe Koppe (Microcontrol) talked about the development and future of classic CANopen and CANopen FD.

On the General Assembly, Uwe Koppe, Christian Schlegel, and Holger Zeltwanger were re-elected as CiA Technical Director, CiA Business Director, and CiA Managing Director, respectively. Together, they group the CiA board of directors for 2022. Additionally, members of the CiA Technical Committee (TC) and the CiA Business Committee (BC) were elected. The permanent members of the TC are Bosch, emotas, Emsa, esd, and NXP. Emotas, Emsa, esd, HMS, and Vector were elected as permanent members of the BC.

Thirteen companies, which joined CiA in 1992 and are still members today were honored on the first evening of the anniversary event. These are Eckelmann, esd, G.i.N., Janz Tec, KEB, Kvaser, Moba, Moog, NXP (formerly Philips Semiconductors), Port, Selectron (today a part of Knorr-Bremse), Softing, and Vector.

Day two: applications and specifications

The second day comprised application-oriented presentations and insights to CiA specification developments. Sebastian Karrer (W&H Dentaltechnik, Austria) reported about CANopen networks connecting tools in dentist chairs. Bjørnar Wilsrød (Kongsberg Maritime) talked about ▷
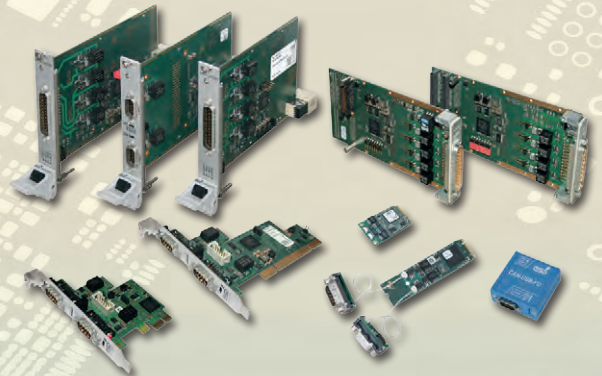

Figure 2: The event was an excellent opportunity to meet CAN fellows with different expertise and backgrounds (Source: CiA)

Figure 3: Many participants took away new ideas for their future CAN product developments (Source: CiA)

Figure 4: Christian Schlegel (left) and Uwe Koppe (right) congratulate Holger Zeltwanger for his 30-year engagement as CiA Managing Director (Source: CiA)

CANopen usage in vessels and ships, where long networks are needed.

The fourth session was provided by CiA employees. Yao Yao gave an overview on CiA technical groups. Thilo Schumann informed about the UML (unified modeling language) usage in CiA documents, and Reiner Zitzmann talked about the generic CAN bootloader specification.

In the afternoon, the SIG CAN XL and the SIG CAN FD Light have had their regular meetings. In parallel, the newly-elected CiA Business Committee had its first meeting discussing the CiA activity plan for 2023.

CiA member interviews

The anniversary event gave the CiA team a perfect possibility to get feedback about its work, to collect ideas, and to rethink the efficiency of some services. In an interview with Olga Fischer (CiA), experts from Microcontrol (Uwe Koppe), Port (Heidrun Scheller, Dietmar Franke), esd electronics (Dirk Flege, Oliver Thimm), ehb electronics (Harm-Peter Krause), emotas (Andreas Böbel, Torsten Gedenk), ifm (Dagmar Schymonski-Dederichs, Joachim Uffelmann), and Bosch (Dr. Arthur Mutter) answered four questions giving a valuable input for CiA work improvements.

Q What are the most important advantages of the CiA membership for your company?

Microcontrol: Of course, the work on CiA specifications and getting first-hand information. CiA is a basis platform to be contacted regarding all CAN issues. That's cool! Such possibilities as joint exhibition booths, product panels, and information distribution via CiA publications are very attractive marketing opportunities.

Port: Access to CiA specifications and the possibility to influence their content working under an independent umbrella. CiA also provides all-round information about CAN and gives support on further CAN inquiries. Beeing CiA member and providing specification-conform interfaces increases the customer's trust in our products.

esd electronics: Being informed! And, of course, to get and to work on specifications. A possibility to publish information about our new CAN products in CiA's media is important as well.

emotas: Networking within the CAN community and possibility to shape the future of CAN-based higher-layer protocols.

ifm: The possibility to work on and to access the CiA specifications. Nice is also that the members are really quickly informed about the ongoing and planned CAN-related activities. Being a CiA member, we are "sitting on the source" of the information. Available ideas can also be reused for work on other networking technologies, for example, to build gateways between them and CAN.

Bosch: CiA is a platform to exchange CAN-related information and a place where high quality specifications are worked out. To work together on an independent platform is of highest importance for us. At CiA, the topics can be specified together, no company is preferred. This is fantastic!

Q How important are the CiA publications, especially the CAN Newsletter magazine and CAN Newsletter Online?

Microcontrol: CiA's press work is a good multiplicator of recent CAN news. The online availability of the information is a valuable searching source for any CAN topic.

Port: I (Heidrun Scheller) regularly read the information in the CIM, CMN, and CAN Newsletter Online with great interest. (*Author's note:* CIM is the monthly sent CAN Info Mail and summarizes news and activities regarding CAN technology. The monthly CMN - CiA Member News email provides exclusive information and can be subscribed only by CiA members.)

ehb electronics: I read the articles in the CAN Newsletter magazine, if the topic is of my interest. I'm also regularly updated via the CIM and CMN. Unfortunately, I didn't know about the existence of CAN Newsletter Online. When I saw this name, I always thought that it is an online version of the magazine.

emotas: CiA publications are important to stay updated. The articles in the CAN Newsletter magazine are suspenseful and informative. We read the CAN Newsletter Online articles in a selective way, mostly the news about competitor companies.

ifm: We are mostly reading the CIM and CMN. In the CAN Newsletter magazine (Joachim Uffelmann stated), we can find a lot of ideas for new application areas.

▷

CAN Technology Symposium 2022
October 25, Stuttgart, Germany

Face-to-Face: Meet the CAN Experts

Discuss with us the latest developments in CAN technology. Renowned speakers from industry leading companies will show the current status and present solutions for the upcoming challenges.

The presentations will be rounded off with an accompanying exhibition in which the companies of the speakers and Vector will present tools and solutions for various CAN applications.

> Agenda & Registration:
vector.com/vCAN2022

Figure 5: The long-term CiA members (here Kvaser) were honored on the first evening of the anniversary event (Source: CiA)

Bosch: CiA publications are optically very nice! Unfortunately, the articles in CAN Newsletter magazine are mostly too long for my available time. But I regularly read the CIM and CMN, as these are short, laconic, and give a good overview on recent activities.

Q Which additional CiA services would you like to see?

Microcontrol: CiA should be more presentative and show its existence in a more widespread way. For example, on exhibitions, members could expose a symbolic item showing that a company is CiA-member. Social media (especially LinkedIn) is also a good opportunity to boost CAN image. A tip regarding videos: Make them short and put the issue in a nutshell to address the new engineer generation.

Port: At the moment, we are perfectly happy!

ehb electronics: We have no ideas for additional services.

emotas: We are very contented with the available services.

ifm: We have some ideas, but these relate to future technical group activities and we would discuss them first CiA-internally. On the whole, we are perfectly happy.

Bosch: I have no ideas for new services, but maybe some available services could be improved. As I work within several technical groups, I receive a lot of invitations, reminders, and working documents, which I have to handle. As a suggestion, CiA could prepare meeting invitations with a possibility to automatically save the date in Outlook. It would be nice to have a "standard" invitation text with only the required information. To have a clear view on documents, it could be sufficient to distribute a link to the group's download area, when a new document, minute, or comment is available. Please, do not distribute the same files twice.

Q How do you estimate the future of the CAN technology?

Microcontrol: As CAN is in a continuous development, it will live for at least the next 30 years.

Port: In industrial automation, Classical CAN will be on-duty for at least next ten years, which is a typical application lifetime. The protocol stack business is stable for last ten years. Former, there was a high growth of this. CAN FD is (yet) not really used in industrial implementations.

CAN FD Light is also more reasonable for use in cars, as its benefits (e.g. price-sensitivity) are suited for mass-production and industrial applications are mostly individual solutions. We think, CAN XL has more perspectives as CAN FD. It is a lower-priced alternative to Industrial Ethernet, offers real-time capabilities, and provides comparable data throughput, if required.

ehb electronics: You know the EIA-232 serial interface? It is still alive! I think, CAN will live for at least the next 30 years. As you see, CAN is still in development. Currently, we are working with Classical CAN and CAN FD. CAN XL is not yet considered so far.

emotas: As long as CAN will be used in cars, it will be alive.

ifm: "Those declared dead live longer…" As long as the CAN technology is not locked for further developments and improvements, it will be used. CAN provides "good genes", is well established, reliable, cost-effective, and proven in countless applications. The available toolchains simplify new developments. Looking at the conservative markets such as mobile machines (added Dagmar Schymonski-Dederichs), CAN will be deployed for a very long time, as they seldom change a running system.

Bosch: CAN will be needed forever… The three CAN generations offering respective benefits are predestined for their own application fields. Regarding CAN XL, we are just at the beginning! It is like a crystal, which is starting to grow. The base CAN XL specifications (the crystal core) were recently released. Supplementary specifications are in work and first implementations are showing up. When the required ecosystem is developed, the CAN XL crystal will live and grow for a very, very long time. The only drawback I see, is the education of the new engineer generation(s). At technical colleges and universities, the lectures about communication technologies are very Ethernet centric. The graduates barely know anything about CAN. When they start working at companies, they promote solutions they know… Thus, CiA and the CAN community should be "louder" and more active in promoting CAN to get more attention. ◀

Author and interviewer

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

History and trends:
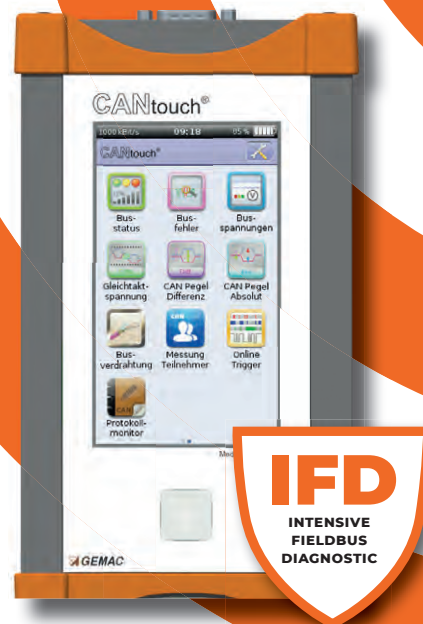
CAN on construction sites

In cranes, pavers, earth-moving machinery, and other equipment used on construction sites, embedded CAN networks are used for many purposes. CANopen and J1939 are the most applied higher-layer protocols. The next step is the migration to CANopen FD and J1939-22.

(Source: Adobe Stock)

In 1994, CAN in Automation (CiA) established already the Special Interest Group (SIG) for mobile applications. It was chaired by Alfons Horn working with Moba. The CiA working group started to develop a CAN Application Layer (CiA 200 series) communication profile for construction machines. When the CANopen application layer and communication profile was handed over to CiA, the group decided to follow this path. Nowadays, Moba provides CANopen products for levelling and quality control of pavers, compactors, and milling machines.

At the same time mid of the 90s, U. S. manufacturers of earth-moving machinery adapted J1939 to control diesel engines. It took some time, to introduce worldwide CAN-based networks into construction machines and equipment, because this industry is conservative in adapting new technologies. Good things come to those, who wait. End of the 1990s, Prof. Dr. Wolfgang Poppy from the Otto-von-Guericke-Universität Magdeburg (Germany) was the

pioneer developing an excavator prototype controlled by CANopen networks. Some years later, many German suppliers of construction machines utilized CANopen in their products. In the meantime, many other European companies implemented CANopen in their machinery. They are supported by host controller manufacturers (e.g. Epec, Intercontrol, ifm, Moba, and STW) as well as sensor and actuator suppliers. The benefits are the standardized interfaces for encoders (CiA 406), inclinometers (CiA 410), modular I/O devices (CiA 401), etc. Products compliant with these CiA profiles are interoperable with the CANopen host controllers. However, exchangeability of such devices is limited to the mandatory functions.

Paving the future

Modern paving machines need multiple sensors. This includes especially sensors to control the levelling of road construction machines. Moba is one of the early birds providing such sensors with CANopen connectivity. Apparently, Chinese companies copied them. Some of these copies looked from the housing like the originals, but the function and quality were different. Paving roads and highways as well as runways require a sophisticated temperature control of the asphalt. This was also achieved with CANopen-connectable sensors.

Furthermore, CANopen networks are used in vehicle-mounted lifting equipment. Hirschmann (today: Wika) was one of the early users of CANopen Safety (EN 50325-5) for overload protection purposes in container, gantry, ▷

Figure 1: The Big Sonic-Ski from Moba with four CAN-connected sensors for asphalt paving (Source: Moba)

Figure 2: ABN sensor with a 22-bit resolution and CANopen or CANopen Safety connectivity (Source: TWK)

lattice boom, telescopic, and other cranes. For such kind of applications functional safe sensors are needed. CANopen Safety has been developed at the beginning of the millennium, originally released as CiA 304 specification.

Today, several CANopen host controllers (e.g. from ifm, Intercontrol, and STW) provide CANopen Safety support. There are also functional-safe pressure sensors, encoder, inclinometers, etc. available. For example, FSG and TWK have recently introduced new CANopen Safety encoders.

The miniature rotary encoder of the MH609y-II-CAN series from FSG feature CANopen and CANopen Safety. The starting point for the development was a previous customer solution for a small rotary encoder with a downstream signal converter for CAN, explained the company. FSG then developed the MH609y-II-CAN series, a cheaper and more compact solution without additional separate converters, the company continued. Signal output was via two CAN interfaces using the CANopen protocol.

At Hannover Messe 2022, TWK exhibited its rotary encoders. They provide CANopen or CANopen Safety connectivity. The latest ABN encoder model has a resolution that divides the circle of 360° into over 4 million steps, which means a 22-bit resolution. This is impressive with better than ±10 arcsec, which is less than ±0,003°. Precise measurements of positions and speeds up to 10000 1/min are thus possible. These values are achieved by scanning an optical code disc. Equipped with the CANopen or CANopen Safety interface, the encoder can be used for safety-related applications. The requirements for SIL 2 (safety integrity level) according to IEC 61508 are fulfilled.

Moba has developed the MSS Slope CANopen Sensor family, which has been EN ISO 13849 certified by TÜV Nord. These sensors support CiA 301.

The next step: Migration to CAN FD

Some construction and earth-moving vehicles – nicknamed as "machines on wheels or caterpillars" – use multiple CAN-based networks. Some of them still use proprietary higher-layer protocols. But most utilize CANopen or J1939. In powertrain, J1939 dominates. CANopen is often used in the machine parts. If the CAN-based networks do not provide sufficient bandwidth, just another network segment is introduced. This is why many host controllers provide multiple CAN ports. In some applications, the separation of functions is not because of the busload, but because of functional separation provided by different development teams or sub-system suppliers.

If the busload is an issue, CAN FD could help. This second generation's CAN protocol is now available in most of the micro-controllers. CAN HS (high-speed) transceivers and transceivers featuring signal improvement capability (so-called SIC transceiver) are provided by several chipmakers. But there is a hurdle to migrate to CAN FD: There ▷

is no specification for the network system design. CiA is going to fill the gap. The nonprofit association is looking for an academic partner to develop design recommendations for larger CAN FD networks. The research results should be usable for CANopen FD as well as J1939-22 (CAN FD based transport and application layer). J1939-22 adopted the multi-PDU (protocol data unit) concept, originally introduced in the CiA 602-2 specification (withdrawn after publication of J1939-22).

CiA profiles for construction machinery

In 2003, CiA released the CANopen application profile for sensor systems in road-construction and earth-moving machines (CiA 415 version 1.0.0). The predecessor of this specification was jointly developed by the Osyris (open system for road information support) consortium (terminated) and the European Asphalt Pavement Association (EAPA, www.eapa.org). The CiA 415 version 2.2.0 was released in April 2009. This application profile specifies the communication interfaces for sensors and a sensor controller of such road construction and earth moving machines as pavers, compactors, graders, dozers, mills, heaters, and trucks.

Profile-compliant sensors require a sensor controller (application commander and CANopen manager) supporting self-configuration of the CANopen network. During the start-up, the sensor controller scans the entire network for available sensors. Then, the number of process data entries provided by each sensor is read and verified using a plausibility test. If the number is valid, each process data entry is read out. Then, the sensor controller creates the necessary TPDOs for each device and downloads them to the sensors via SDO. First the PDO mapping parameters are configured followed by the PDO communication parameters. The same procedure is repeated for the required process data whereby the RPDOs for each sensor are created. After this process, the sensor controller switches the involved devices to the NMT operational state and tests whether the established PDO connections are working correctly.
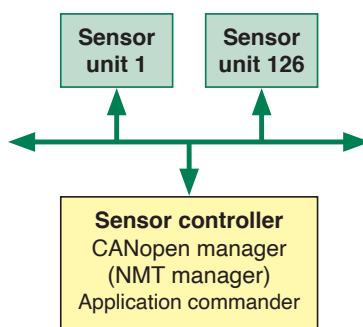

Figure 3: CiA 415 sensor system architecture example. Profile-compliant sensors require a sensor controller (application commander and CANopen manager) supporting self-configuration of the CANopen network. (Source: CiA)

Important system information is transferred with high priority using defined events for request/response of available sensor data, generic error transmission, machine state (stop, working etc.), leveling status (manual, auto, etc.), closed-loop control (automatic on/off), and begin of a new project (reset mode). Thus, the sensor controller device (usually residing in the on-board computer) is always informed on this information.

The general device parameters contain the ▷

CAN Newsletter Online

The CAN Newsletter already reported several times about applications and products regarding CAN on construction sites. Here a few examples:

Tunnel drilling
"Not-a-boring" competition
Elon Musk's Boring company has scheduled a competition to drill a tunnel faster than a snail.

Electrified
All-in-one solution for commercial vehicle PTOs
The Eworx product family from ZF enables commercial vehicle power take-offs (PTOs) that are locally emission-free. Via CAN, the solution can be integrated into the vehicle's battery and energy management system.

CAN Newsletter magazine
Faster drilling for faster Internet
Absolute CANopen encoders from Wachendorff provide position data in AT-Boretec's horizontal drill machines with automatic pipe feeding.

Moving detection
Mining safety kit for working in dangerous environments
To reduce the risk of accidents and equipment damage in quarries, mines, and construction sites, VIA showcased the VIA Mobile360 AI Mining Safety Kit at the Conexpo-CON/AGG.

Fanless box PC
For construction machines
The Rugged Computer Compact 8 by Syslogic complies with protection class IP67. It can be used in vehicles such as graders, wheel loaders, mining trucks, or dozers under extreme conditions.

Bauma 2016
Driver's cab monitors surroundings
Bosch was part of the Bauma 2016 and presents the Genius Cab. Using cameras and environmental sensors, drivers can monitor their surroundings and intuitively control vehicle functions via a display and joystick.

CAN network embedded
Radio-controlled crane
F.lli Ferrari (Italy) has developed the 900 series of truck-mountable cranes. The cranes use embedded CAN networks.

Leveling system
Asphalt paving with a digital controller
Leveling technology in asphalt pavers is a must for many projects. The Moba-matic leveling system and digital encoder helped level and pave a stretch of road in the north of Germany.

External CAN interfaces

End of the 1990s, the nonprofit Industrial Truck Association (ITA) developed some CANopen recommendations, how to use CiA profiles in forklifts. In the meantime, many OEMs (original equipment manufacturers) have implemented embedded CANopen networks in their battery-powered forklifts. One of the CANopen device suppliers is Curtis Instruments. The company offers color LCD displays, foot pedals and joysticks, sensors, I/O devices, and motor speed controllers for traction, steering, and hydraulic pumps. All these products implement configurable CANopen interfaces. Other features include motor auto-characterization routines and the proprietary Vehicle Control Language (VCL) application software helping OEMs to achieve maximum vehicle performance with minimum effort. For example, Curtis' CANopen motor controller (AC F2-A) and CANopen gauge (3140) are used in Chinese pallet trucks.

Vetter, another supplier, has introduced the CANopen-connectable Smartfork sub-system, which enables forklifts to become AGVs (automated guided vehicles).

Jungheinrich uses CANopen networks in its forklifts since many years. In 2022, the ERE 225i pallet truck won the Red Dot design award. It uses an embedded CANopen network as the bigger trucklifts from Jungheinrich.

(Source: Jungheinrich)

The CAN Newsletter already reported several times about CAN used in forklifts. Here a few more examples:

Electric forklift
Counterbalance truck with lithium-ion battery

Clark has relaunched the GEX and GTX series. The three and four-wheel electric forklifts in 48-V technology with load capacities of 1,6 t to 2 t are now also available with a lithium-ion (Li-ion) battery. The included control system uses CAN.

Read on

Battery charger
Energy storage in electric forklifts

In the V-Force Energy Storage System (ESS) by Crown the battery charger communicates with the battery management system via CAN.

Read on

CAN Newsletter magazine
Covid-19: More pallet stackers and forklifts are needed

In times of locked down economies with a lot of exit restrictions, online shopping increases. This causes more business for logistics companies requiring increasingly pallet stackers, forklifts, and other transportation equipment.

Read on

CANopen and J1939
RFID solution for forklift vehicles

The RFID (radio-frequency identification) industrial reader Bluebox Micro IA from Idtronic, is suited for industrial applications within intralogistical processes with a forklift vehicle.

Read on

information about the used machine (type, manufacturer, serial number etc.), provided and required process data, reference point for the measured coordinates, date and time as well as the operating hours. Process data includes the absolute 3D-position, angle position, curvilinear coordinates and angles, geographical coordinates, diverse

Figure 4: CANopen networks are used in vehicle-mounted lifting equipment. Wika, for example, uses CANopen Safety for overload protection purposes in container, gantry, lattice boom, telescopic, and other cranes. (Source: Adobe Stock)

deviation values, steering angle, machine speed, travelled distance, tool's rotational speed and extent, thickness of the laid or the removed layer, material volume and mass, flow values, diverse temperatures, road evenness, environmental conditions (wind, humidity, atmospheric pressure, and rainfall level) as well as the water tank level. For each consumed and each provided process data, a reference value parameter for configuration of a set-point is specified. The physical layer definitions accord to the CiA 301 and CiA 436 profile for construction machines. The latter defines also the error behavior of the sensor systems.

CiA 436 CANopen application profile for construction machines specifies the use of CANopen networks on construction machineries by introducing the virtual control architecture. The latter integrates the interfaces to the (diesel) engine control system, the drivers' desk, the sensor control system, the transmission control system, the fleet management control system, and the implement (superstructure) control system. CiA 436-1 specifies the integration network with the interfaces to the mentioned sub-systems. For each sub-system a separate application profile is specified (CiA 415 for sensor control) or is in development within further sub-parts of the CiA 436.
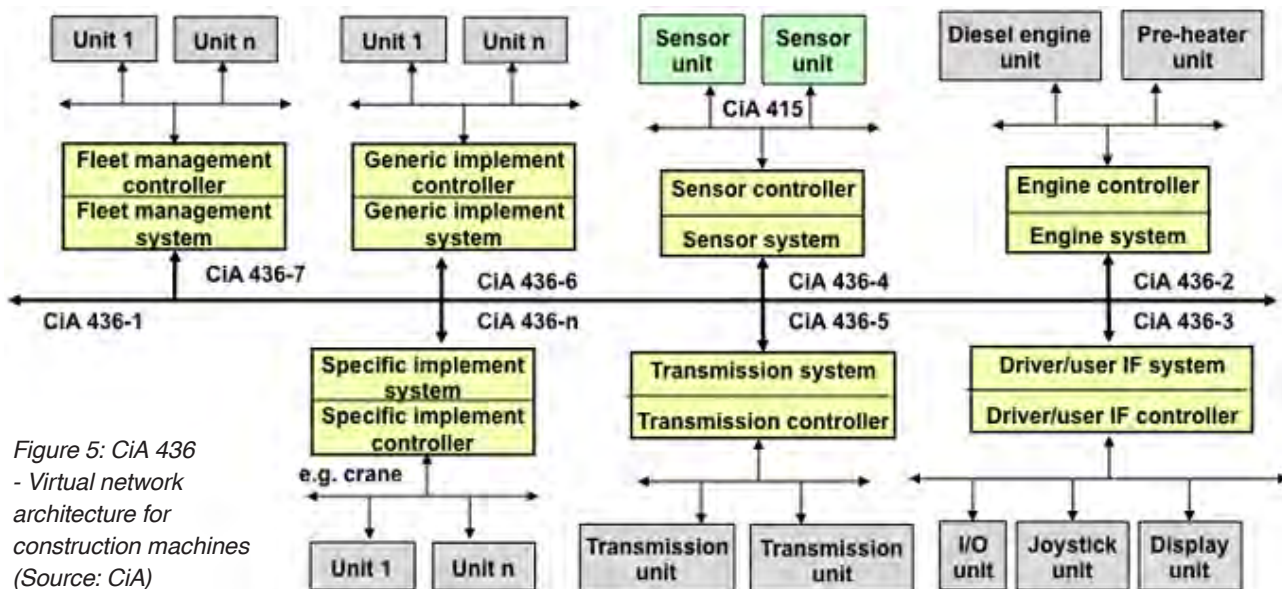
Figure 5: CiA 436 - Virtual network architecture for construction machines (Source: CiA)

The CiA 436-1 specification provides general definitions for construction machines. This series of documents has not been finalized yet. This is why CiA plans for 2023, to organize a workshop to discuss the demands for profiles related to any kind of construction and earth-moving
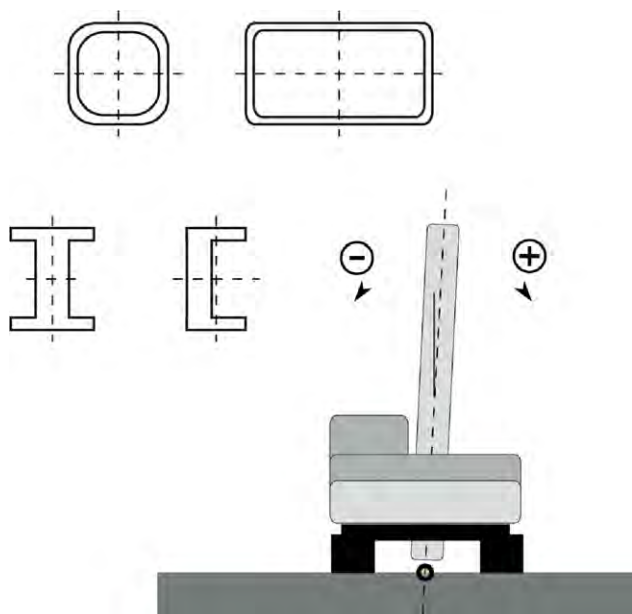

Figure 6: CiA 455 is suitable for all machines having a mast. Considering different mast profiles, the location of the reference point is illustrated in this Figure. (Source: CiA)

machines. The CiA 436-1 document recommends to use 5-pin micro-style (M12) connectors with a pin-assignment given in the CiA 106 technical report.

CiA has also developed a CANopen application profile for drilling machines. This CiA 455 specification covers the CANopen interfaces with regard on positioning and tool control. It is suitable for all machines featuring a mast, which is mounted in the upper carriage. On this mast, the tool(s) are mounted. Depending on the machine, the mast can be moved along several axes in space as well as change its extension. The position of the mast is to be handled independently of the position of the machine's carriage. But the tool position depends on the mast position and alignment.

The center axis of the mast is defined as the axis of the centers of area of the whole mast. This is a well-defined axis (being identical with the geometrical center on a dual axial symmetrical profile). The location of the reference point is specified as intersection point between the axis of the mast and the ground level. Considering different mast profiles, the location of the reference point is illustrated in Figure 6. The coordinate system's x-axis is oriented to the magnetic north, the vertical z-axis pointing vertically upwards. The definition of the flask of reference for drilling machineries as well as for the location of the reference point is illustrated in the full CiA 455 specification, which can be received from CiA (for members it is free of charge).

CAN in Automation has a joint stand at the Bauma Munich construction and mining machinery exhibition from October 24 to October 30, 2022 and can be found in hall A2, stand 337. ◀

Author

Cindy Weissmueller
CAN Newsletter
pr@can-cia.org
www.can-newsletter.org
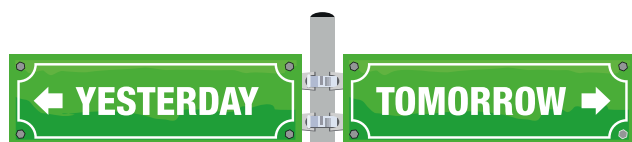
History and trends:

CAN on rails

CAN serves in many rail vehicles as embedded and deeply embedded network. Often CANopen is used as higher-layer protocol. CiA has developed several profiles, which need to be revised according to new feature requests.

Already in the early days of CAN in Automation (CiA) in mid of the 1990s, some members used CAN in rail vehicles. One of them was Kiepe Elektrik Today, the company belongs to the Knorr-Bremse group. An early bird in applying CAN in special train utility vehicles was Windhoff. Both companies adapted CANopen, when this higher-layer protocol was handed over to CiA. Selectron (today part of the Knorr-Bremse group) and Luetze, two other CiA members, started end of the 1990s to provide CANopen devices for locomotives and coaches. At the same time, Knorr-Bremse developed CANopen solutions deeply embedded in its rail-vehicle brakes. IFE (today a part of the Knorr-Bremse group) submitted a CANopen profile for rail vehicle doors to CiA, which was released as CiA 424.

From research projects to IEC standardization

In 1994, Deutsche Bahn (German railway company) and STZP technology transfer center initiated the Ebas system development project for CAN-based data acquisition, monitoring, and control in freight trains. The system should shorten train assembly procedure including train rearrangement, identification, and configuration of the vehicles, as well as the check and determination of train's braking performance. Ebas also supported all train operating phases providing brake and traction control, and monitoring the vehicle functions. CAN fulfilled the communication requirements providing high data integrity, low implementation costs, resistance in harsh environments, and minimal power

consumption especially during the long idle times. The system could be deployed in trains made of up to eight 900-m segments, each consisting of up to 60 vehicles. Considering these lengths and communication delays of the CAN repeaters, the chosen bit rate of 10 kbit/s was sufficient for real-time requirements while the train operation. CAL (CAN application layer), the predecessor of CANopen, provided required objects and services for network management, vehicle configuration, transmission of high-priority braking and traction control commands, and emergency notifications. In 1996 first trains were equipped with Ebas by Mannesmann Rexroth. Later, the successfully-introduced system was also deployed in Deutsche Bahn locomotives. The well-documented specification of the CAN-based communication paved the way for further usage of CAN(open) in railway applications and for international standardization.

Public transport vehicles for from Vossloh Kiepe have comprised CAN-based networks since 1995. The use of CANopen was introduced in 1997. On the iCC (international CAN Conference) 2003, the company presented the principles of the CANopen-based control for streetcars and trolley-busses. Figure 1 shows the structure of the CAN-based networks within a vehicle. As a first step only the network management and the process data objects (PDOs) were used. The network-managing device supervised all connected CANopen devices using the node-guarding mechanism. The control and status data were transmitted via PDOs. The more recent vehicles implemented service data objects (SDOs) to exchange diagnostic and maintenance information. ▷
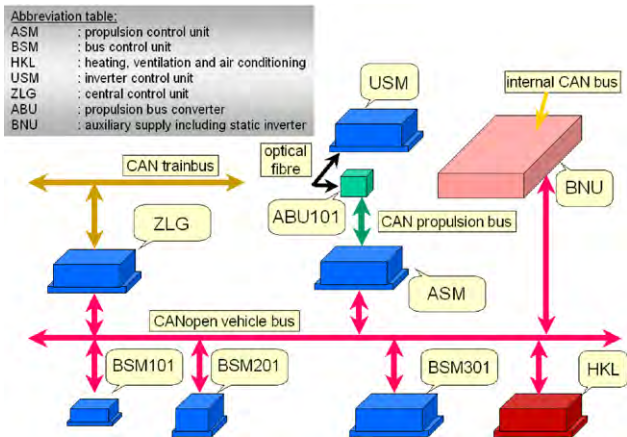
Figure 1: In-principle structure of the CAN-based networks within a vehicle (Source: Vossloh Kiepe)

On the same conference Knorr-Bremse spoke about the use of its CAN-based sub-systems (e.g. brake equipment, anti-skid system, door control, passenger information) in trams, metros, locomotives, and high-speed trains. As the base for its developments, the manufacturer used the Esra (electronic system for railway application) – a central electronic micro-processor system. At that time, the company implemented a proprietary higher-layer protocol similar to CANopen.

An expert from Deuta shown on the iCC 2005 how the company realized the CAN-based communication within the driver's desk comprising displays, dashboards, and control switches. The application implemented redundant CAN networks. A demonstration driver desk has been exhibited on the Innotrans 2004. In those days, the company considered to implement the CANopen Safety (EN 50325-5, former CiA 304) or the CANopen-based redundancy mechanism (former CiA 307) in its driver desks.

Figure 2: Demonstration driver desk exhibited on the Innotrans 2004 (Source: Deuta)

CiA profiles based on UIC leaflets

Based on UIC (international union of railways) leaflets, which specify process data for different rail-vehicle sub-systems, CiA members developed CANopen application profiles. These profiles standardize CANopen interfaces for logical units. The PDO (process data object) mapping is not specified. This enables an easy adaption by configuring the PDOs individually for each project. The following several-part profiles have been released:

Order to equip 130 regional trains

Alstom has commissioned Knorr-Bremse to equip at least 130 new regional trains from the Coradia Stream family with multiple systems, starting in 2023 and extending through to 2029. In addition to the contract for the entire braking systems, doors, and HVAC systems, it is also the first major contract for Knorr-Bremse in Europe to deliver integrated sanitary cabins from its brand Evac. The Coradia Stream high-capacity trains will operate in and around Stuttgart (Germany).

The electropneumatic braking systems for the trains will include Pistonsupply-Eco compressors, flexible brake control systems from the Flexcontrol-Modular family, Syscontrol brake electronics, and Sandgrip sanding systems. Knorr-Bremse will also be supplying pressure-tight, weight-optimized, low-maintenance entrance systems with sliding steps from the group's IFE brand, and modular, scalable, HVAC (heating, ventilation, air-conditioning) systems. Some of this equipment use embedded CAN networks. Additionally, Knorr-Bremse will be supplying Sansys sanitary systems from the Group's Evac brand, with three units to be installed in each trainset. The Sansys units include customized cabins comprising vacuum systems, tanks, and electronic control functions.

(Source: Knorr-Bremse)

The order was placed with Knorr-Bremse under the long-term framework agreement concluded between Alstom and Knorr-Bremse in 2021. Under the terms of the agreement, until at least 2025, whenever rail operators raise an order for trains in Alstom's Coradia Stream family, Knorr-Bremse will be a systems supplier for the trains. For Knorr-Bremse, this is the fourth order to be awarded under the Coradia Stream framework agreement by an Alstom customer in Germany, following orders for Coradia Stream trainsets from Expresskreuz Bremen and the Kinzigtal as well as Main-Weser regions.

Alstom's Coradia Stream design is a state-of-the-art low-floor electric multiple unit (EMU). As a matter of course, the train family offers specific technical configuration options that can be adapted to individual operators' requirements. At the same time, Alstom's efforts to further improve standardization have resulted in a single, versatile train family capable of acting as the ideal platform for both regional and intercity trains.

hz

- ◆ CiA 421: CANopen application profile for train vehicle control networks
- ◆ CiA 423: CANopen application profile for rail vehicle power drive systems
- ◆ CiA 424: CANopen application profile for rail vehicle door control systems
- ◆ CiA 426: CANopen application profile for rail vehicle exterior lighting control

▷

- ◆ CiA 430: CANopen application profile for rail vehicle auxiliary operating systems
- ◆ CiA 433: CANopen application profile for rail vehicle interior lighting control

CiA is going to revise these specifications. Therefore, a free-of-charge CiA webinar (open to the entire CAN community) and a CiA workshop (limited to CiA members and invited guests) have been scheduled. Additionally, CiA exhibits on the Innotrans 2022 trade show in Berlin (Germany) in hall 27, stand 290.

Internationally standardized

Since 2005, CiA experts joined the Working Group 43 of the IEC (international electrotechnical commission) Technical Committee 9. Reiner Zitzmann (now CEO of CAN in Automation GmbH) edited the IEC 61375-3-3 document named "Electronic railway equipment – Train Communication System (TCN) – Part 3-3: CANopen Consist Network". The existing CANopen-based profiles were submitted to IEC and were considered, when the CANopen Consist Network was standardized. The standard was finally approved in April 2012 and published in June 2012. IEC 61375-3-3 specifies the data communication based on CANopen, inside a single rail vehicle or a consist, in which several vehicles share the same vehicle bus. A standardized gateway, also defined in the document, enables the full integration of CANopen-based consists in trains that follow the TCN architecture (TCN: train communication network, see IEC 61375-1/-2).
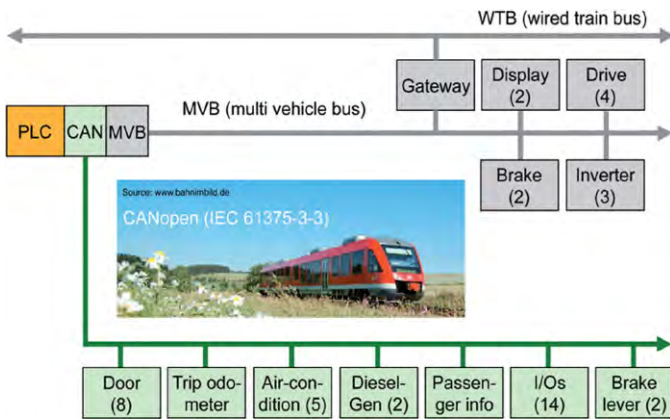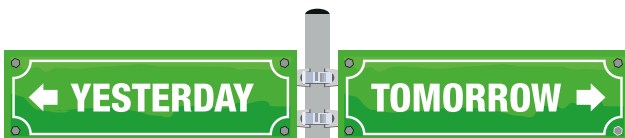

Figure 3: TCN architecture with CANopen (Source: CiA)

In general, the lower communication layers as well as the application layer are based on well-proven standards for CAN (ISO 11898-1/-2) and CANopen (EN 50325-4). This allows to use available CAN components (transceiver, controller) and tools, CANopen protocol stacks, CANopen configuration and diagnostic tools as well as CANopen off-the-shelf devices (I/Os, host controller, drives, etc.). Well-defined communication interfaces simplify system design and maintenance.

Proven in innumerable applications

Embedded and deeply embedded CAN(open) networks are not visible for the passengers, even if they travel daily by commuter trains, metros, or trams. CAN(open) networks do their duty already since many years, because rail vehicles have a long lifetime. In the CAN Newsletter we reported about a lot of developments for rolling stock applications. Here are several examples:

Railway computer
Compliant with EN 50155

Duagon provides CAN-enabled communication solutions for train networks, control, monitoring, and information systems.

Read on

Decentralized applications
Programmable logic controller for rail vehicles

The rail technology provider Luetze Transportation presented the Lion MicroPLC logic module for decentralized applications on rail vehicles.

Read on

Traction converters
For light rail vehicles

The Bordline CC400 series by ABB is dedicated for trams, metros, streetcars, trolleys, and monorails. The products provide CANopen connectivity.

Read on

Exhaust after-treatment
Modular control system

Heinzmann has developed the Xios hardware platform to manage engine control tasks in special-purpose and rail vehicles, construction machines, ships, and stationary generators.

Read on

Driver assistance system
Electronic co-driver for trams

Bosch released a system, which warns of collisions and even brakes independently. The company uses its CAN-connected radar and video sensors from the automotive sector in rail transport.

Read on

Rail vehicles
Control of hybrid drives with J1939

When used on rail vehicles, the Luetze Dioline PLC compact controller enables decentralized and autonomous preprocessing of functions below the main control level. The main control is thus relieved and becomes more reliable.

Read on

Interior lighting system
For rail vehicles

The Interior lighting control (ILC) by Teknoware (Finland) uses an embedded CANopen network and communicates with the TCMS (train control and management system). It is intended for use in rail coaches.

Read on

CAN over powerline

At the iCC 2002, Selectron introduced the CAN powerline application for rolling stock. Every time a train is composed, a new communication network has to be formed and set up. To achieve a reliable communication through a serial bus line, which has to be routed via a large number of contacts (from wagon to wagon), the serial bus line has to be operated at a higher voltage (50 V_{DC} to 60 V_{DC}). Using the powerline-communication principles, the CAN nodes are communicating via a loaded DC-line. A special power line transceiver was designed to achieve required bit rates and fulfill the immunity and emissions demands according to EN 50155. Two powerline communication principles (base-band method and signal-carrier method) were considered while development. Test results prove successful function of a CAN powerline system that is based on the base-band principle. Nowadays, for example, the new vehicles from Stadler are equipped with CAN powerline and CANopen solutions from Selectron.

Summary and outlook

CANopen networks embedded in railway vehicles' subsystems do their duty already since many years, because rail vehicles have a long lifetime. "For retrofit projects and new developments, CANopen FD could be a candidate," said Holger Zeltwanger, CiA Managing Director. "In the long-term also CAN XL is a good opportunity to be adapted in rolling stock for coach backbone applications."

The international standardization (IEC 61375-3-3 for train communication networks) provides CANopen the necessary acceptance in the application field of rail vehicles. Additionally considering the existing CiA specifications for diesel engine control, door control, light control etc. railway operators and vehicle manufacturers can benefit from a high degree of standardization. They are no longer dependent on one single supplier. Regarding system integration and maintenance, they can choose from a broad range of available tools of different manufacturers. Suppliers of single devices or entire sub-systems are enabled to sell their identically-configured products in several projects. This can reduce the diversity of device variants and the administration effort. ◄

Author

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

Photovoltaics for on-board charging

The Lade-PV project aims to investigate the profitability of photovoltaics use as an additional power source in commercial electric vehicles (EVs). A photovoltaic converter connects the PV solution to the in-vehicle CAN network(s) to manage the battery charging.

Figure 1: I drive electrically powered by photovoltaic on my roof (Source: Fraunhofer ISE)

Solar power produced on the vehicle can help to save power coming from the EV battery and, thus, improve vehicle's CO_2 emission balance. To demonstrate the marketability of PV (photovoltaic) applications in freight transport, several German companies teamed in the Lade-PV project sponsored by the Federal Ministry for Economic Affairs and Climate Action (German: Bundesministerium für Wirtschaft und Klimaschutz, BMWK). The project managed by Fraunhofer Institute for Solar Energy Systems ISE has started in summer 2019 and should end in summer 2022. Participating parties are Fraunhofer Institute for Transportation and Infrastructure Systems IVI, TBV Kühl-fahrzeuge, Sunset Energietechnik, Alexander Bürkle, as well as M&P Motion Control and Power Electronics.

In the project, suitable lighweight PV modules for subsequent on-roof mounting and full integration, as well as CAN-based components for power electronics are being developed. The cost-effective production of large PV-module quantities in a production line is conceptually developed. The modules and components are installed in electric commercial vehicles to conduct practical tests. First implementations of the concept are already under testing on the street-legal vehicles. An energy prediction model should estimate the irradiation potential and enable a cost analysis. The project's aim is to demonstrate energy savings of more than 5 % thanks to additional PV usage.

Connecting to the CAN in-vehicle network

The involved power electronics were adapted to the automotive requirements. Project partner M&P Motion Control and Power Electronics developed a DC power converter that collects and controls the solar power delivered by the PV modules. The converter is connected to the in-vehicle CAN network and manages the power exchange with the electric vehicle battery. Thus, the battery can be charged by the available solar power and the mileage provided by a battery-charge is increased. In refrigerated vans, the energy delivered by the PV solution can be also used for the electric Peltier cooling of the load.

PV modules and power electronics

The goal of the project is to develop particularly light and robust PV modules for subsequent on-roof mounting and ▷

Applications

Vehicle-integrated photovoltaics
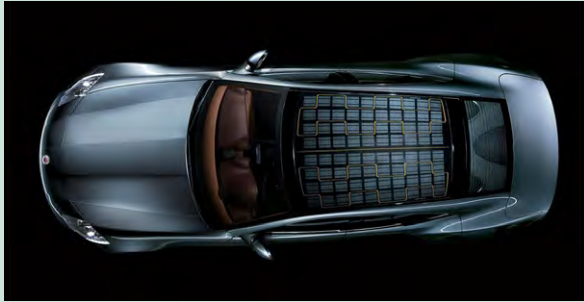
The PV car roof from A2-solar on the hybrid Fisker Karma car has an aesthetically attractive design (Source: A2-solar)

Vehicle-integrated photovoltaics (VIPV) designates the mechanical, electrical, and design-technical integration of photovoltaic modules into vehicles. The PV modules blend seamlessly into the vehicle exterior and are connected to electric loads or the drive battery in electric vehicles by means of the CAN networks. In general, the concept is also suitable for vehicles using combustion engines. Simultaneously, the PV modules replace other components of the vehicle, e.g. the roof or the bonnet. VIPV increases the mileage of electrically powered vehicles and improves their CO_2 balance. The aesthetic expectations on integration into the vehicle design are especially high for cars. For utility vehicles (e.g. trucks and buses), particularly lightweight PV modules are needed to avoid restricting the load capacity. Further application areas include caravans and mobile homes, coaches, buses, trucks, delivery bicycles, trams, trains, ships, aircraft, and drones. According to the Fraunhofer Institute for Solar Energy Systems ISE, the technical potential of at least 55 GWp is given in Germany.

Application examples are given by electric cars, which are additionally equipped with PV modules. The applied PV modules usually meet additional aesthetic requirements, e.g. special designs and curvature are possible. The additional PV power can increase the mileage by several kilometers per day. In refrigerated vans, the PV electricity can be used for the electric Peltier cooling of the load. In this way, the same cooling power can be generated with less usage of the refrigeration unit and the diesel consumption can be reduced. The integration of PV modules onto the refrigerated compartment requires particularly lightweight modules which do not compromise the thermal insulation.

of

Figure 2: The refrigerated van from TBV uses integrated PV modules to support the refrigeration of the compartment (Source: TBV Kühlfahrzeuge)

Due to space and weight requirements, the power volume and weight of the modules' connection to the EVs' electrical system should be minimized. New semiconductor technologies are tested. The integrated power electronics packaging and thus also the thermal management of the components are adapted correspondingly. Additionally, the power electronics and PV modules are tested according to the automotive requirements. The developed energy management concept should be suitable for connection to non-electric commercial vehicles as well.

Energy forecast, evaluation, and test

An energy forecast model considers the on-board energy-consumers and forecasts the PV power yield based on different routes, ranges, charging times, and energy quantities. The measurement data is collected from sensors installed on vehicles in the real traffic. This allows to record the irradiation potential for different route types, occupancy rates, as well as different usage and shading scenarios (e.g. cities, country roads, or motorways). The recorded data evaluation allows a specific estimation of the energy potential.

The demonstration vehicles are equipped with PV modules to test connection concepts, cable management, and integration of power electronics. The savings in real operation are to be tested with different users, route profiles, and travelling times (e.g. daytime, early morning, evening). In addition, the handling, compatibility to involved in-vehicle processes, and the applicability in practice shall be demonstrated. ◀

full integration. The application-optimized modules should be able to be produced in the price category of standard modules or even cheaper (less than 0,4 €/W respectively less than 75 €/m²). For this purpose, innovative material combinations for lamination are evaluated and tested. The targeted full integration of the PV modules into the roof surface saves additional costs for framing and material. To test the roadworthiness of the modules, relevant tests according to the relevant IEC standards are adapted and conducted.

Author

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

CANopen in photovoltaic systems

CAN is used in photovoltaic (PV) power generation for a long time e.g. in solar tracking systems, inverters, sensors, etc. As a standardized approach, the CiA 437 application profile for grid-based photovoltaic systems was developed by CAN in Automation (CiA) and companies from the photovoltaic industry. It defines the CANopen interfaces for PV systems including controllers, inverters, different sensors, solar panel trackers, etc. The profile specifies pre-defined communication objects and process data (current, voltage, power, etc.) to be exchanged in a standardized way. When implementing the profile, device manufacturers may supply diverse applications using the same standardized electronic CANopen interface implementation and simply adapting the required functionality. A system designer may combine CANopen devices from different manufacturers implementing the required profile-compliant functionality. The according spare parts can be also made available from different sources. For development, analysis, and maintenance of the devices, off-the-shelf CANopen tools may be used.

In PV systems solar radiation is directly converted to electrical current with the help of solar cells based on semiconductor technology. The CiA 437 profile specifies standardized communication interfaces to control the PV power generation solutions. (Source: Posital-Fraba)

of
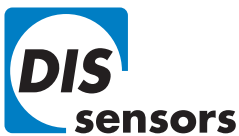
Vehicle network processing platform with functional safety

The NXP S32G274A vehicle network processor supports hardware security and functional safety according to ISO 26262. Microsys has integrated it in a system-on-module (SOM) with typical applications in connected vehicles, mobile machines, and automotive test equipment.

In today's age of digitalization, Industry 4.0, and the Internet of Things (IoT), high-throughput connectivity is one of the most critical functions for the interconnected devices. This particularly applies to the smart mobility sector, where the number of vehicles that is connected 24/7 via 5G to the service-oriented gateways, is growing. This continuous connectivity makes it possible to exploit the full potential of the vehicle data and to deploy new services and functional enhancements quickly and efficiently. Other domain controllers support functions such as infotainment and in-vehicle experience, body and comfort, powertrain and vehicle dynamics, as well as safety and security for ADAS (advanced driver assistance systems). Increasingly, autonomous driving functions are also required. The data transfer between the individual domain controllers or zonal computers/gateways and the local sensors and actuators must be processed and orchestrated with as little latency as possible.

The zero-downtime OTA (over-the-air updates) capability has to be considered as well. In addition, they must be real-time capable and secured in terms of ASIL D (automotive safety integrity level) safety and hardware security. This applies not only to major vehicle and mobility brands, but also to any latest commercial, construction or agricultural vehicle, overland and subway trains, and other types of mobile vehicles such as autonomous warehouse robots, and drones.

Compared to NXP's previous automotive gateway platforms, the S32G274A delivers 15900 Dhrystone Mips (million instructions per second), which translates into more than ten times faster real-time and network performance. To achieve this performance leap, the S32G2 processors integrate micro-controllers, application processors, network accelerators and a dedicated hardware security engine (HSE) on a single chip. This gives developers access
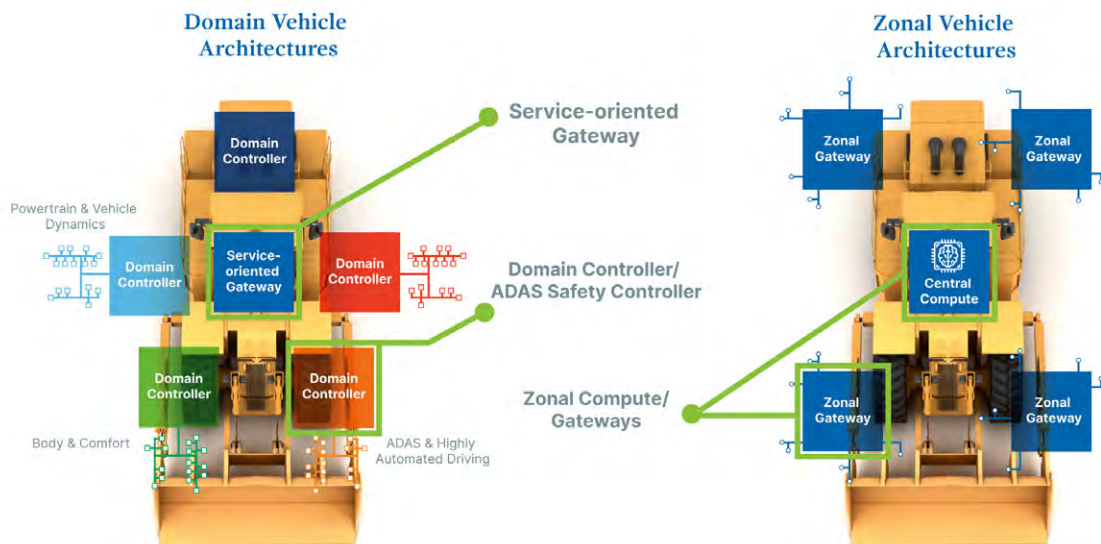

Figure 1: NXP S32G2 automotive processors power service-oriented gateways, domain controllers and ADAS safety controllers, or serve as zonal computers or gateways (Source: Microsys)

Increasing data throughput

Such gateways are expected to deliver increasing processing performance and data throughput to satisfy recent requirements such as cloud connectivity for fleet management or vehicle subscriptions, V2X (vehicle-to-everything) communication, ADAS functions, and autonomous driving.

to enough high-bandwidth processing power and high-performance connectivity to run tactile Internet applications with real-time 5G communication. The performance boost is possible by integration of several previously separate functions in a single-chip design, thereby combining more overall performance on one die. This also allows direct communication via the integrated safe fabric offers and ▷

lowers latencies. The integrated lockstep functionality for detecting errors during execution and data transmission, along with monitoring of other hardware-related faults, is yet another feature for safety applications.

On-chip interfaces and processing cores

Connected vehicles and mobile machines also require native support of all relevant peripheral interfaces, such as CAN (FD), Flexray, and LIN. Alternative connected vehicle designs using generic extension components to connect CAN controllers generate high interrupt loads that slow the main processor down unnecessarily. FPGAs (field-programmable gate arrays) are not a cost-effective alternative either and require additional development resources for FPGA programming. Providing on-chip automotive interfaces (up to 20 CAN FD, 2 Flexray, and 7 LIN) ensures that the most complex sub-systems are addressed without the latencies caused by the otherwise required USB-to-network components. This also avoids the need for expensive FPGA designs. The low-latency communication engine (LLCE) for CAN (and others), and the packet forwarding engine (PFE) for processing IP packets from Ethernet networks, reduce the CPU (central processing unit) workload. A fire-walled hard-ware security engine (HSE) for secure boot, security services, key management, and encrypted data transfer provides a root of trust, which is essential for secure IoT edge systems.

The processor orchestrates four 1-GHz Arm Cortex-A53 cores organized in two clusters for applications and services. They provide up to 23 Dhrystone Mips per core for multi-purpose applications. In addition, there are also three integrated Arm Cortex-M7 dual-core lock-step processors. Applications requiring dedicated co-processors, e.g. for motion control applications, can take advantage of the three dual-cores. They support real-time operating systems such as Autosar or FreeRTOS.

Integrated functional safety and safe communication

For safety-critical applications, the Arm Cortex-M7 and A53 cores can be operated in lock-step mode. Where required, the M7 cores can work in a 2oo3 (two-out-of-three) voting mode to ensure that when the three core pairs provide different results, the same result provided by two core pairs is valid. This way, the heterogeneous computing cores can support ASIL D applications as well as any other functional safety standard according to IEC 61508.

The integrated HSE provides comprehensive security functions for data and application security. These include data encryption and decryption as well as the generation and verification of MACs (media access control), and signatures. Secure boot provides a memory check at system startup. In addition, the engine pro-vides real-time, hardware-accelerated SSL/TLS (secure ▷
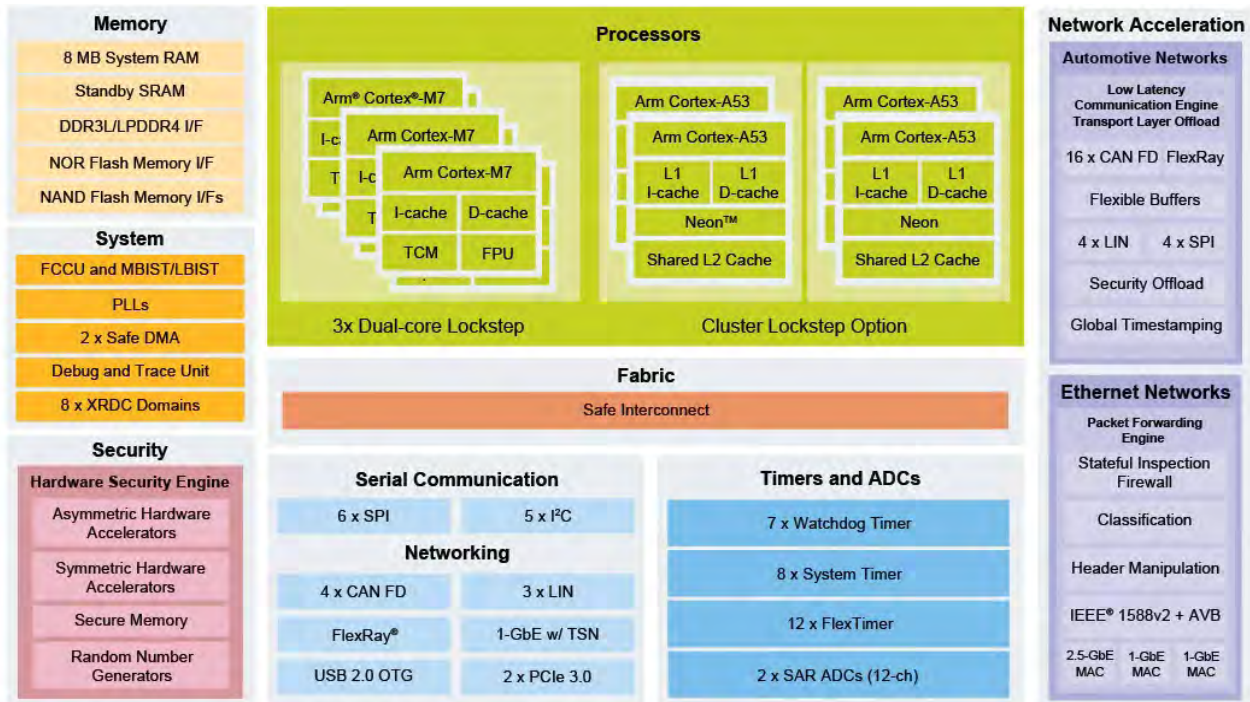
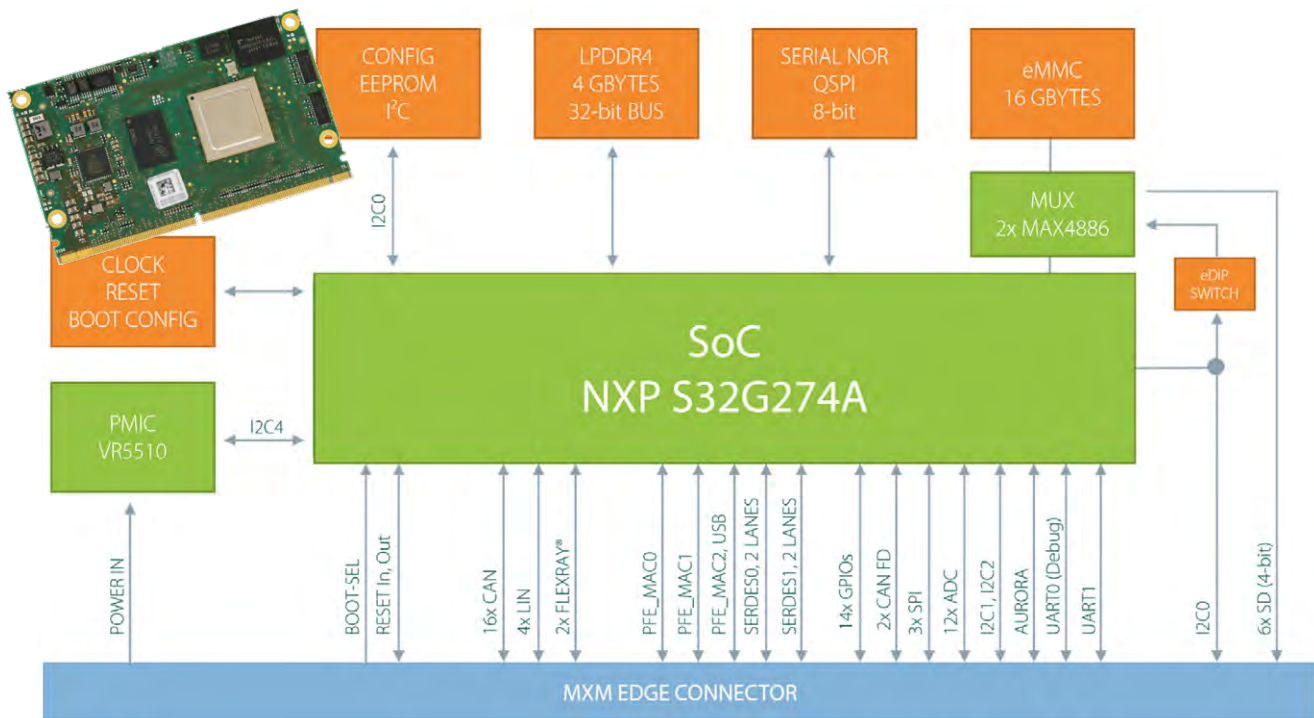Figure 2: NXP S32G2 processor block diagram (Source: NXP)

Figure 3: The Microsys Miriac MPX-S32G274A is the world's first system-on-module integrating the recent NXP S32G2 automotive processor. It provides developers with an easy-to-integrate platform including required core components and interfaces. (Source: Microsys)

socket layer, transport layer security) network communication and supports IPsec. It also provides random number generation capabilities and secure key management capabilities, along with resistance against side-channel attacks.

System-on-module

Developers of applications for commercial vehicles, mobile machines and e-mobility solutions that are only manufac-tured in industrial batch sizes, cannot afford to develop and integrate such complex gateway processor technology, along with all the required additional components and complex BSP (board support packages), into their systems from scratch. Instead, they have to concentrate on their core competencies, which are primarily in application development and which differentiate them from the competition. This is where application-ready COTS (commercial off-the-shelf) platforms help as they enable the development of customized solutions without the need to ▷
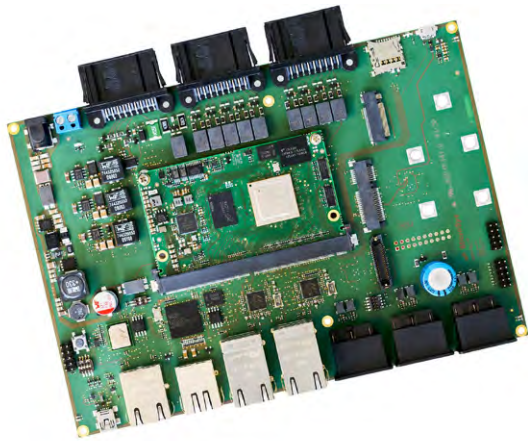
Figure 4: The application-ready Miriac SBC-S32G274A single-board computer is also available as a starter kit serving as an evaluation and target system for development (Source: Microsys)

spend a lot of time on the design of the central computing core. System-on-modules, which are delivered as COTS components with everything needed for application development and certification, are increasingly popular for this purpose. They already integrate function-validated drivers for all supported interfaces and provide ready-to-use OS (operating system) images from boot up to login. This saves time and increases design security, especially since the modules are not just used for one but different designs and therefore come with a comprehensive set of pre-validated functions. As a result, they provide a solid basis for the efficient design and implementation of customized control and gateway solutions for vehicles as well as mobile and stationary machines.

NXP's partner Microsys Electronics has integrated the S32G2 on the Miriac MPX-S32G274A system-on-module with a guaranteed availability of at least 15 years. This is a sufficient length of time to allow for the average 2-3 year integration and acceptance period for such solutions, while also ensuring a long product life and sustainable spare-part procurement. All components on the module are specified for the temperature range of -40 °C to +85 °C. The processor is designed for the AEC-Q100 Class 2 temperature range (at least from -40 °C to +115 °C). A low TDP (thermal design power) also makes passive cooling an option. The system platform is therefore optimized by design for the challenging operating conditions in mobile vehicles. The SOM is available as an application-ready, off-the-shelf component or as a development kit with a carrier board, cable set, and cooling solution. It integrates 4 GiB of soldered LPDDR4 RAM at 3200 MT/s (mega transfers per second), a 32-GiB eMMC non-volatile memory, and a 64-MiB QuadSPI flash. External SD card storage can be multiplexed with the onboard eMMC.

For connectivity, the SOM offers 18 CAN FD ports, four Serdes interfaces configurable as PCIe, four 1-Gbit/s Ethernet, two Flexray, and four LIN. 14 GPIOs, 12 analog inputs, three SPI, two UART, an USB and three I²C complete the interface range. For trace and debug tasks, the module supports Aurora and JTAG interfaces.

A board support package for Linux, including bootloader configuration and the required drivers, rounds off the ▷
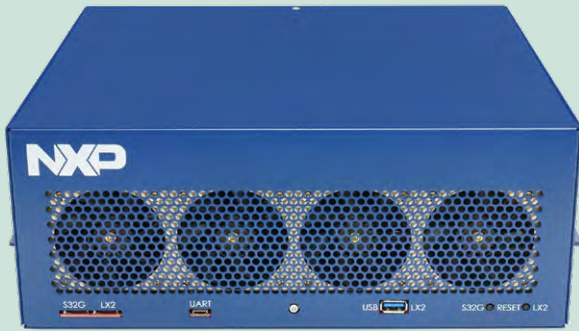
Example SOM implementation

NXP's Bluebox 3.0 computing platform (Source: NXP)

NXP's Bluebox 3.0 is an example implementation that illustrates the efficiency of SOM-based designs. The processor manufacturer NXP has chosen this approach and integrated the Miriac MPX-S32G274 SOM into the scalable development platform for safe automotive high-performance computing. The reason: It is much easier and more efficient to design-in an application-ready component that already integrates the processor, RAM, and flash than to start a full custom design from scratch. Developers are therefore well advised to use SOMs when designing their own board. One major challenge, for example, is ensuring signal integrity and quality. At very high frequencies, length matching, line impedance and impedance jumps are particularly taxing. Therefore, it is necessary to use a special PCB (printed circuit board) material. And, as the BGAs (ball grid arrays) are packed extremely densely, the PCBs need to have more layers. With SOMs, customers get a less complex PCB for the custom carrier board. The result: a simpler layout, lower PCB costs, and high signal integrity.

feature set. Besides standard automotive support from NXP, Microsys also offers optional support for dedicated FreeRTOS implementations for the Arm Cortex-M7 processors.

The modules come with the necessary documentation to simplify reuse in customers' certifications and documentation. This reduces the complexity of the approval process for customers. Another benefit is that OEMs (original equipment manufacturers) have access to competent experts helping them with any questions, for instance regarding safety-relevant software implementation, which is crucial for developers of IEC 62443 compliant industrial cyber security as well as ISO 26262 compliant functional safety solutions. The company also offers customer-specific design services at carrier board and system level. These extend to SIL (safety integrity level) certification for all sectors in which functional safety standards analog to IEC 61508 are required. This includes railway technology (EN 50155), stationary and mobile machinery (ISO 13849), industrial robots (ISO 10218), control systems (IEC 62061), and drive systems (IEC 61800-5-2). Approvals in the aviation context (DO-254/DO-160) are also simplified by the existing manufacturer documentation.

Suited for different applications

Due to extended temperature support, the Miriam SOMs are suited for industrial applications at a fixed outdoor location. Possible applications include e-mobility charging stations, critical infrastructures (Kritis) for trains, electricity, oil and gas pipelines, public safety systems, etc.

Anything that is deployed in vehicles must be extensively tested and logged in the prototype phase to track down errors and optimize the entire vehicle electronics. Microsys develops individually customized carrier boards and system designs for automotive test equipment and service providers. Since such platforms do not require complex certifications due to their intended use, the company's development teams can quickly deliver them in small to large quantities, not least thanks to close collaboration with the local component manufacturers.

The stationary and car-mounted test and measurement equipment used in automotive workshops must keep up with the rising performance of the chips installed in vehicles and be able to take more and more measurements at ever higher data rates and data depths. Test systems built on the same platforms as those used in the vehicles can keep up providing support of the given vehicle interfaces. If test and measurement systems are already developed for the prototype phase, the path to certified series production is not long. ◄

Authors

Lukas Steinert
Christian Bauer
Microsys Electronics
info@microsys.de
www.microsys.de

Interviews with providers: CAN SIC transceivers

CAN SIC (signal improvement capability) transceivers can be used in Classical CAN, CAN FD, and CAN XL networks, reduce signal ringing, improve achievable bit rates, and provide more design flexibility regarding topology. Four semiconductor manufacturers answered questions about their CAN SIC transceivers.

(Source: Adobe Stock)

As new functions have entered the modern vehicles, the need for increased data exchange pushed Classical CAN networking systems beyond their limits. CAN FD enables bit rates from 500 kbit/s up to 5 Mbit/s. Despite the benefits, the CAN FD technology is hindered by the signal ringing stemming from the signal reflection. Considering the network topology, this effectively limits the technology to 2 Mbit/s for many networks, restricting them to highly linear topologies. Thus, wiring harnesses need to avoid long cable stubs, which results in more convoluted harness routes around the vehicle, adding cost and weight.

The CAN SIC technology overcomes these signal integrity issues by actively improving the CAN signal and using of stricter timing. As a result, OEMs (original equipment manufacturers) can encounter more freedom in the design of their networks and on the location of ECUs (electronic control unit). Associated benefits include shorter cables, less weight, and fewer connectors. The SIC technology also enables bit rates higher than 5 Mbit/s on multi-node networks. Thus, CAN FD is expected to support a higher range of applications at a relatively low-cost point.

The CAN SIC transceivers are specified in the CiA 601-4 document developed by CAN in Automation (CiA) members. There are two implementations available: one suppresses the ringing when transmitting; the other filters the ringing when receiving. CiA 601-4 also specifies additional requirements for HS-PMA (high-speed physical media attachment) implementations compliant with ISO 11898-1:2015 and ISO 11898-2:2016. These aim to reduce differential and common-mode ringing on the CAN_H and CAN_L wires, especially for the transition from the dominant to recessive state. The HS-PMA implementations with additional signal improvement functionalities support communication in the presence of defined unterminated wire stubs without requiring configuration, for example the bit-rate settings. Furthermore, CiA 601-4 specifies the EMC (electromagnetic compatibility) tests for HS-PMA implementations with additional signal improvement functionalities.

Provider interviews

Teun Hulmann (NXP), Johann Pries (Infineon), and Wes Ray (Texas Instruments) answered five questions about the availability and features of their CAN SIC transceivers.

Teun Hulman (NXP)

Johan Pries (Infineon)

Wes Ray (Texas Instruments)

Q Has your company CAN SIC (signal improvement capability) transceivers in its portfolio? If yes, how many and how are these named?

Teun Hulman: NXP has released its first CAN SIC transceiver family for mass production in 2020. In the meantime, the TJA146x has been widely adopted among OEMs and Tier1s and is the first CAN SIC transceiver to be on the road in a vehicle. ▷
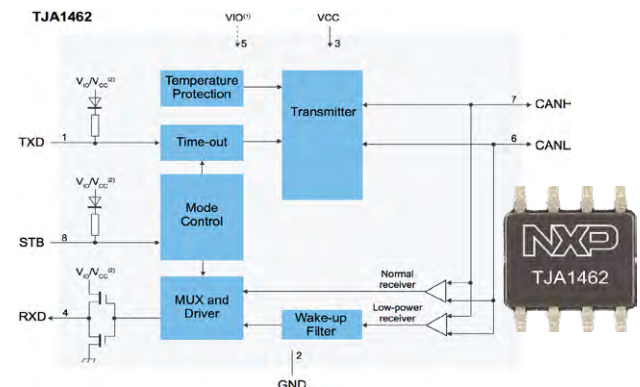

Figure 1: The TJA1462 transceivers are available in SO8 package (Source: NXP)

Interviews

Product	Low-power mode	Vio pin (3,3 V to 5 V)	Package	Automotive grade
TJA1462AT(K)	Stand-by	Yes	SO8 (HVSON8)	Grade 1
TJA1462BT(K)	Stand-by	No	SO8 (HVSON8)	Grade 1
TJA1463AT(K)	Sleep	Yes	SO14 (HVSON14)	Grade 1
TJR1462AT(K)	Stand-by	Yes	SO8 (HVSON8)	Grade 0
TJR1462BT(K)	Stand-by	No	SO8 (HVSON8)	Grade 0
TJR1463AT(K)	Sleep	Yes	SO14 (HVSON14)	Grade 0

Table 1: NXP's CAN SIC transceivers with features (Source: NXP)

The family as shown in Table 1 is the first wave of NXP's CAN SIC components, combining a strong signal improvement technology with reliable performance. It consists of two stand-by transceivers and a sleep-mode transceiver, plus variants supporting higher temperature Grade-0 applications. NXP is currently expanding its portfolio, having multiple CAN SIC products with additional features in development.

Johan Pries: These are the TLE9371SJ and TLE9371VSJ transceivers.

Wes Ray: Yes, we have both 8-pin (TCAN1462-Q1) and 14-pin (TCAN1463-Q1) standard CAN SIC transceivers available today via our website. A dual CAN SIC device (TCAN1466-Q1) will sample soon. TI continues to invest in additional CAN SIC products with more news on that subject coming soon. TI also wrote a technical white paper about the signal improvement capability of CAN FD transceivers.

Figure 2: The TLE9371SJ transceivers are available in DSO-8 package (Source: Infineon)

Q Which maximal bit rate is achievable with the corresponding SIC transceiver? Are there some-features, which are not offered by other providers?

Teun Hulman: An extension of the maximum bit rate of CAN FD transceivers has been claimed in the past, even with the possibility of going up to 8 Mbit/s with standard CAN FD devices. For CAN FD transceivers, which are only fulfilling the bit timing requirements of ISO 11898-2:2016 standard, the speed limit is essentially 5 Mbit/s in a point-to-point link (a discussion of this has been published in an earlier CAN Newsletter article).

The TJA146x CAN SIC family improves upon the bit timing performance – tightening it significantly – and with this, it guarantees bit rates up to 8 Mbit/s under all worst cases conditions. This does not take into account topology effects, which are a separate factor for the achievable bit rate.

The TJA146x CAN SIC transceivers are fully compliant to the CiA 601-4 specification and all CAN SIC related compliance tests, such as C&S IOPT Test and IBEE Zwickau CAN SIC EMC test. Furthermore, NXP includes full CAN FD backwards compatibility by fully guaranteeing all aspects of the CAN FD protocol arbitration and error frame detection under all circum-stances, including during SIC phases like active recessive.

Johan Pries: Up to 8 Mbit/s.

Wes Ray: Support up to 8 Mbit/s. We offer the world's smallest, automotive CAN FD and CAN SIC devices with our SOT packaging. Customers can retain the device package leads and retain smaller footprints than VSON packaging.
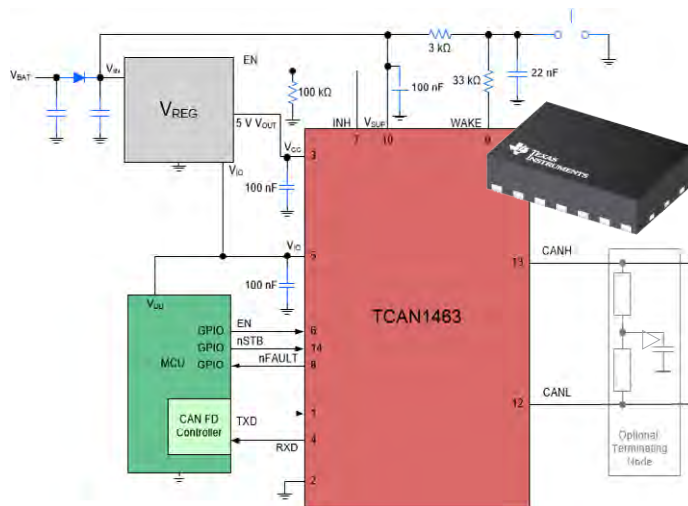

Figure 3: Simplified schematics of the 14-pin TCAN1463-Q1 transceivers (Source: Texas Instruments)

Q The SIC transceiver features are specified in the CiA 601-4. Does your company require some improvements of the specification?

Teun Hulman: With CAN SIC being more and more adopted into the market, there might be a need for a standardized definition of how to conduct a topology assessment. This would support network owners in having a unified approach and common reference to make sure their networks can operate reliably, also in mixed-vendor networks.

Johan Pries: No.

Wes Ray: Not at this time. However, we are closely monitoring global OEM adoption and testing requirements and may request updates as adoption progresses globally.

Q CAN in Automation (CiA) organizes plugfests to test CAN components and devices as well as their interoperability. Is there a need to test the CAN SIC transceiver features?

Teun Hulman: It is important for CAN SIC solutions to ensure full compatibility with the CAN FD protocol. As a result, all arbitration and error handling scenarios need to be fulfilled under all conditions, not only on a single-device level, but also in a mixed-vendor network. Plugfests would be a good opportunity to test compatibility of CAN SIC devices to the CAN FD protocol, such as arbitration and error handling.

These tests could be combined with worst-case timing criteria, which would also be able to give insight into topology effects. However, this will not replace the need for topology simulations, able to show worst case corner-case effects, to provide conclusions about achievable bit rate and signal integrity in real topologies.

Johan Pries: No, we see no need for this. It is covered by the C&S IOPT test.

Wes Ray: The standard C&S IOPT and emissions testing is sufficient for OEM / Tier 1 use in our opinion; however, we understand the value and encourage them and we will always support plugfests if we can.

Q Does your company plan to provide CAN SIC XL transceivers? If yes, when are they to expect?

Teun Hulman: NXP has developed its first proof of concept silicon for a CAN SIC XL transceiver. This transceiver was first showcased at the CiA plugfest in 2021, demonstrating CAN XL bit rates up to 20 Mbit/s in complex networks. ▷

Companies background

NXP: The global semiconductor company creates solutions enabling secure connections for a smarter world. Headquartered in Netherlands, the round 29 000-employees team works on technologies for automotive connectivity and electrification, 5G edge computing, Industry 4.0, safely-connected lifestyles, smart cities, and smart homes. The company's history started as Motorola semiconductor development group (USA) in 1949. Rebranded to Philips in 1991, it developed its first CAN/LIN transceiver for in-vehicle networking. This year, the manufacturer celebrates 15 years as NXP.

Infineon: The Germany-based, worldwide semiconductor provider was founded in 1999, when the semiconductor operations of its parent company Siemens were spun off. In April 2020 the manufacturer bought Cypress Semiconductor (USA). With 56 R&D (research and development) locations and 20 manufacturing sites worldwide,

Infineon employs circa 50 280 people around the globe. The company aims to make life easier, safer, and greener by linking the real world to the digital one. Thus, it develops solutions for efficient energy management, smart mobility, and secure, seamless communications.

Texas Instruments: Founded in Dallas (Texas, USA) the company designing, manufacturing, testing, and selling analog and embedded semiconductors claims to have been a pioneer in the transition of the world from vacuum tubes to transistors and then to integrated circuits (ICs). It engages about 31 000 people in the 15 manufacturing locations worldwide. The goal is to create a better world by making electronics more affordable through semiconductors. The provider's semiconductors should help their customers to create applications for industrial, automotive, personal electronics, communications equipment, and enterprise systems markets.   of

NXP's CAN XL transceiver is currently in development and more details can be made available for customers on request.

**Johan Pries:** It is planned, yes, but we have no expected date.

Wes Ray: Yes, TI is investing in both CAN FD SIC and CAN XL technologies. Our development for CAN XL is active. TI will continue to monitor the market needs for this next generation technology and will develop our CAN XL portfolio accordingly. More detailed information can be provided to customers upon request.   ◄

Interviewer

Olga Fischer
CAN Newsletter
pr@can-cia.org
www.can-newsletter.org
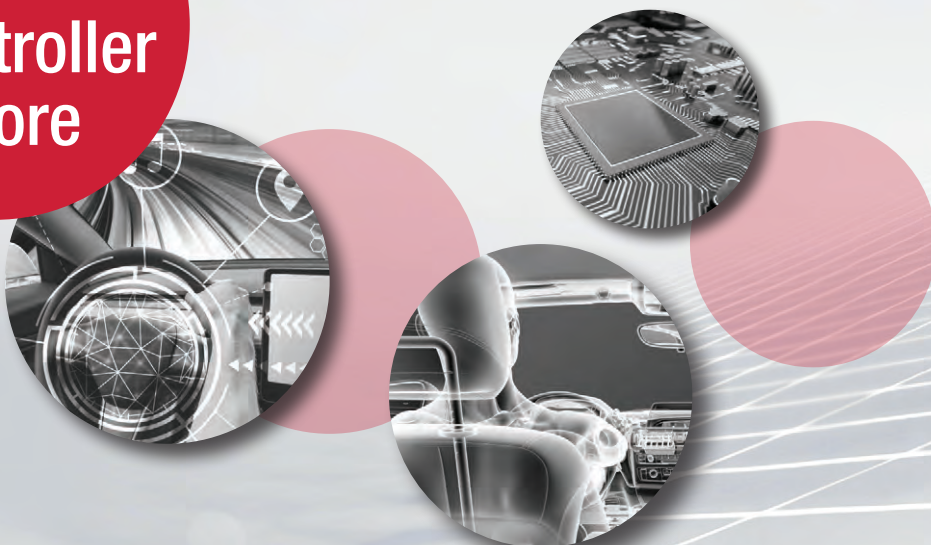
Securing CAN networks in commercial vehicles

(Source: Adobe Stock/NXP)

The UNECE (United Nations Economic Commission for Europe) demands cybersecurity for road vehicles. In order to protect the CAN network from compromised ECUs (electronic control units), a CAN transceiver with built-in security functions can be used. This avoids the complexity of end-to-end security solutions, which are especially hard to implement on commercial vehicles.

Commercial road vehicles are the backbone of the modern consumer economy. Almost any business from construction, to energy, to online retail, at some point relies on the delivery of goods by commercial vehicles. These commercial vehicles are in turn becoming increasingly connected both to the external world and to each other via telematics. This enables commercial vehicle owners to optimize and manage their fleets via platooning for safety and efficiency improvements as well as cost and fuel consumption reduction to meet the increasingly stringent CO_2 emissions requirements necessitated by climate change. However, the increased connectivity brings with it an increase in cyberattack surfaces and commercial vehicle fleets are prime targets for cybercrime due to the high value of the cargo they carry, and their importance to large businesses and the greater economy. [1]

Remote scalable cyberattacks have high adverse impacts

While commercial vehicle manufacturers are familiar with and prepared for the risk of physical attacks, typically carried out on one vehicle, such as odometer manipulation, or theft, they may risk being caught by surprise at the scale and impact of what is possible with remote cyberattacks. Remote security breaches have been demonstrated to impact the safety[2] of the vehicle, resulting in the recall of millions of vehicles. Hackers can exploit a vehicle's wireless network or internet connection to gain entry into the vehicle's communication network and compromise security to access a vehicle's CAN (Controller Area Network) network and take over remote management of the vehicle while it is in motion. Modern ECUs in commercial vehicles run on millions of lines of code, which opens up vulnerabilities for compromising them[3]. Even conservative estimates predict a bug every 1000 lines of code[4]. A range of activities can then be carried out with malicious intent from fraudulent manipulation of data to complete control of safety critical functions such as steering, acceleration, and braking. Location tracking and theft are also among the potential motivations for hackers to inject malicious CAN data frames into the CAN network.


Figure 1: Securing CAN networks in commercial vehicles with NXP Secure CAN transceivers (Source: NXP)

UNECE R155 – Mandatory cybersecurity compliance

The increase in connectivity brings with it an increased risk of malicious cyberattacks. These risks are relatively new to commercial vehicles and industry experts are looking at several approaches to mitigate these risks. However, there is already the expectation from regulatory bodies such as UNECE that it is no longer a question of if there is an attack but when there is an attack on a vehicle network. This has resulted in mandatory cybersecurity compliance regulation R155. It is applicable at first for new vehicle types but will then become applicable to all vehicles on the road, increasing the sense of urgency for the implementation of cybersecurity measures within vehicles that will be on the road in one of the 54 countries[5] that are party to the agreement. The R155 has explicit requirements such as "The vehicle shall verify the authenticity of the messages it receives" because in CAN data link layer communication, the sender is unknown and the intended receiver acts on a CAN data frame it receives, even if spoofed. Other ▷

High-end Connectivity and Data Management

Telematics and Cloud Systems for IoT and Service 4.0
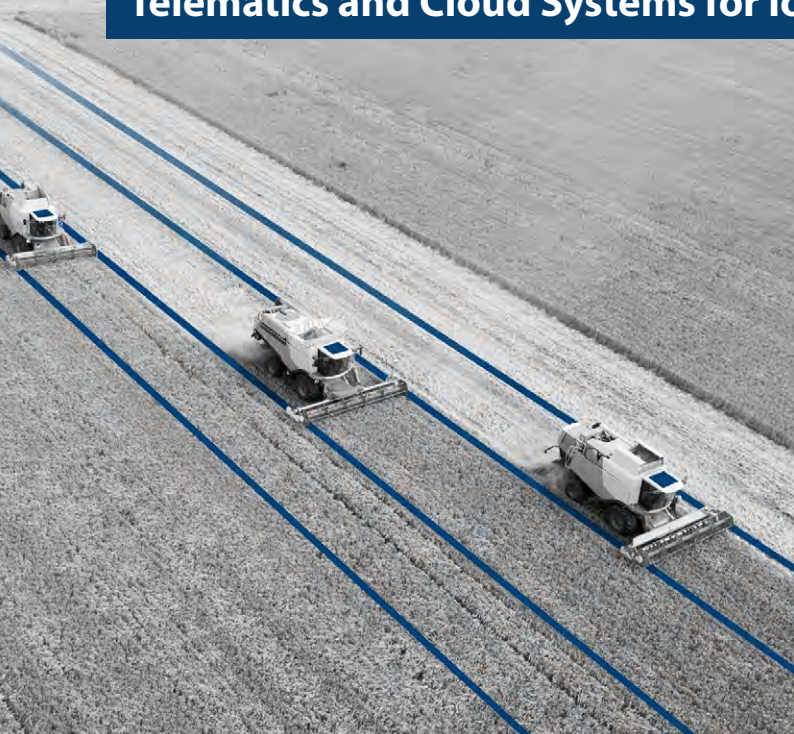
Continuous digitization for smart vehicles

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

CAN
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

www.s-i-e.de

requirements are important for safety, such as "Measures to detect and recover from a denial-of-service attack shall be employed", because a jammed CAN network could prevent the timely transmission of control and safety-critical messages. This makes it important not only to detect attacks, and implement fixes to avoid a repeat, but also to find ways to prevent them from causing harm in the first place.

Figure 2: Long life platforms, integration of several sub-assemblies, software complexity for end-to-end security, the lack of a secure communication standard, cost pressures, and cyber regulation compliance are among the challenges faced by commercial vehicle manufacturers (Source: NXP)

Absence of a standard for secure communication

Several OEMs (original equipment manufacturer) who make passenger vehicles protect their CAN network via secure onboard communication implementation of Autosar SecOC[6]. However, commercial vehicles employ the CAN-based SAE J1939 higher-layer protocol, which does not yet provide standardized cybersecurity measures. For example, there is no way to authenticate the origin of the message. There are ongoing efforts to arrive at a secure communication standard for J1939 but this is still several months from being finalized.

Long life platforms with legacy ECUs and architectures

Eventually there will be a secure communication standard on J1939 called the J1939-91C. However, implementation would require micro-controllers supporting cryptographic functions. As most commercial vehicles have a long lifetime once commercially released, there is typically several micro-controllers without the required security features, not only the advanced ones for hardware acceleration of cryptographic key generation, but also more basic features of modern micro-controllers such as secure boot. Another vulnerability from the long life of commercial vehicle platforms is that these architectures were not designed with security as a focus. As a consequence, they do not have sufficient network separation between the individual CAN branches leaving a wider footprint of vulnerable devices in the event of an attack. To be able to implement such a secure communication standard effectively once

released would still require a major in-vehicle network overhaul to implement. Moreover, there is a lot of know-how and infrastructure that will need to be put in place before the standards are widely adopted within the supply chain. This would still be out of reach for small truck and bus OEMs.

Custom security solutions are complex and prohibitive

As the owner of security in the vehicle, some passenger vehicle makers opt to secure their networks with custom security implementations in spite of the large one-time expense due to the security benefits they perceive. However, implementation of a custom end-to-end security solution is a challenge for commercial vehicle OEMs as they don't build the entire truck themselves but bring together different sub-assemblies which are integrated into the vehicle. Cryptographic security solutions that require complex software implementations can also be cumbersome for the commercial vehicle manufacturer's security teams to co-ordinate across their vast swath of suppliers. This would be an integration and testing nightmare. Besides, most small OEMs buy off-the-shelf solutions, thus providing little room for the Tier-I supplier to take on such one-off security projects.

Open architectures

Commercial vehicles are susceptible to malicious access to the vehicle network from the way they are constructed. As a single commercial vehicle chassis can be transformed into any of a number of different variants, this means that the CAN network might well come all the way to the exterior of the vehicle, for example to establish the connection between the vehicle chassis and a trailer. These could become easy entry points to malicious hackers. As the vehicle is put together from different sub-assemblies, the suppliers need to be able secure each sub-assembly's network locally, and independently, so that when they come together at the OEM, there aren't additional security vulnerabilities introduced.

Affordable security is a must

Last but not the least is the commercial aspect of implementing security measures. While there is an increasing number of commercial vehicles hitting the road, driven by demand from industries such as construction, and e-commerce, the numbers are still vastly lower than those of passenger cars. This places significant pressure on the development costs of commercial vehicles. Commercial vehicle security solutions, therefore, need to not only be easy to implement but also affordable.

The absence of a readily implementable secure communication standard, long lasting platforms with legacy components, deployment across a complex production hierarchy, open architectures for functional integration, and pressure on development costs require an affordable, easy to configure, integrate and validate solution. ▷

Secure CAN transceivers

Figure 3: The TJA1152 Secure CAN transceiver features stand-by mode and the TJA1153 supports sleep mode; both are compliant with ISO 11898-2:2016. The block diagram shows a secure CAN transceiver. (Source: CiA/NXP)

Local network authentication

The NXP Secure CAN transceivers can serve to ensure authentication of communication on a local network, i.e., for CAN data frames not transmitted over a gateway. It does so using a configurable transmission pass-list, or list of user pre-configured CAN-IDs, built into the transceiver itself. This ensures that the local host is only allowed to send these legitimate CAN data frames. A CAN-ID block-list ensures that no other node uses the CAN-IDs that are legitimately owned by the aforementioned local host. The J1939 protocols spec-ifies unique source addresses (SA) for ECUs (to be assigned by the network designer), which can be masked using the ▷

secure CAN transceivers to enable securing the communication based on a pass-list and block-list for CAN-IDs as determined by the OEM in order to fulfill the network's security requirements.

Tamper protection

To circumvent the secure CAN spoofing protection, a hacker could attempt to carry out a man-in-the-middle attack to manipulate a legitimately initiated CAN frame by taking control at the data field to insert rogue data along with an appropriately altered CRC value. In Error Active state, the CAN controller detects and invalidates the manipulated frame. However, in Error Passive state, the modifications are not signaled by an error frame. The secure CAN transceiver has tamper protection on transmit and receive paths to protect from a man-in-the-middle attack by generating the requisite error frame when the CAN controller of the legitimate sender is in the Error Passive state.
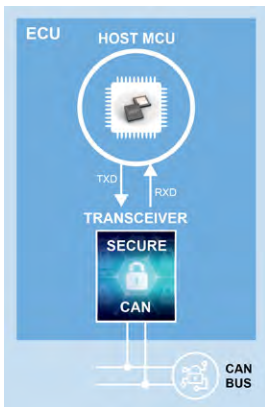
Flooding denial-of-service protection

Figure 4: The Secure CAN transceivers have configurable pass and block lists for CAN-IDs, rate limiting, and an integrated CAN controller for generating error frames and switching to secure mode (bus off for TX) (Source: NXP)

One of the significant benefits of the NXP TJA1152 and TJA1153 transceivers is the provision for adding user configurable flooding protection thresholds, to prevent a compromised local host from flooding the network with high-priority CAN-IDs that are part of the transceiver's transmission pass-list. In a shared communication channel such as a CAN network, a timing failure can have serious consequences, especially for control and safety functions. With the exception of braking, most systems in commercial vehicles do not have a back-up CAN channel, which raises the importance of keeping the network available at all times. The flooding protection can also help avoid impact to the CAN network on critical pathways where a babbling-idiot failure triggered from the local host's software could cause bus overload with an excessive transmission of the permitted CAN-IDs.

Software and MCU independent security

As the provided security functions are without cryptography or dependence on any other micro-controller features, they are compatible with all MCUs including legacy ones. Moreover, the security functions being built into the transceiver, there is no software impact, as is usually the case with a key-based security approach. By implementing the transceiver with security measures into commercial vehicles, the need for updating network architectures and software to include sophisticated cryptographic solutions and the associated expensive hardware is avoided.

How secure is secure CAN?

The transceivers have an option to be fully locked after the initial configuration making the CAN-IDs effectively hard-coded for complete security. However, to provide flexibility to the OEMs, there is provided the possibility to locally or remotely reconfigure the transceiver using a secure boot microcontroller. This should be done only in the first few seconds after the microcontroller goes through a secure boot to prevent a runtime compromised ECU from updating the Secure CAN transceiver's configured CAN-IDs or flooding thresholds maliciously. The Secure CAN transceivers have a configurable parameter that can be set to ensure this limited time window for configurability.

Drop-in security

The TJA1152 and TJA1153 Secure CAN transceivers are key enablers for addressing challenges for commercial vehicle cybersecurity. The transceivers are available as drop-in replacements to legacy CAN HS (high-speed) and CAN FD transceivers, enabling a simple populating of the solution in an application. The transceivers serve as a one-size-fits-all security enabler for Tier-1s that are implementing security across a wide variety of commercial vehicle OEMs. An initial configuration of the transceivers is sufficient to secure vehicles equipped with a different mix of legacy and new ECUs, and varying levels of software flexibility, while reducing cost for network security.

Improving time to root cause on cyber-incidents

Imagine a remote fleet spoofing attack on a business's commercial vehicles for theft of valuable cargo. OEMs implement IDS (Intrusion Detection System) systems to quickly understand the details of such an attack, in order to carry out forensics on the compromised ECU, and issue a fix to avoid a repeat of the incident. But what if one could prevent the attack from bringing harm in the first place? The secure transceivers prevent a successful attack on the victim ECU by invalidating the malicious CAN data frame with a CAN error frame, and switching to secure mode preventing any communication by the compromised ECU temporarily. This provides a ready signal to a network monitoring IDS on which node in the local network was hacked due to the ▷

Reference

[1] Road transport study: Digitalization is progressing rapidly, but cybersecurity awareness still in its infancy (press release by Continental, 2020)
[2] Charlie Miller and Chris Valasek, Remote Exploitation of an Unaltered Passenger Vehicle, 2015
[3] Addressing the cybersecurity risks
[4] The danger of complexity: More code, more bugs
[6] "Transceiver with cyber security functions", Bernd Elend, Tony Adamson (both NXP Semiconductors)
[7] „Autosar SecOC for CAN FD", Dr. Tobias Islinger, Yasuhiro Mori, Jennifer Neumüller, Martin Prisching, Dr. Robert Schmidt (all Denso Automotive Deutschland)
[8] Gloria D'Anna, Cybersecurity for commercial vehicles (hardcover), SAE, Detroit 2018

absent ECU heartbeat. This latter feature will help the OEM immensely to reduce the time to root cause on the incident and implement a security fix quickly, having to search through only the identified compromised sender, and not the entire subnetwork.

The commercial vehicle industry is in as much of an inflection as the passenger vehicle industry. Their security experts are working hard on meeting the cybersecurity compliance requirements, given the unique challenges they face. NXP's TJA1152 and TJA1153 Secure CAN transceivers help bring the industry one step closer to securing their in-vehicle CAN network communication. ◄

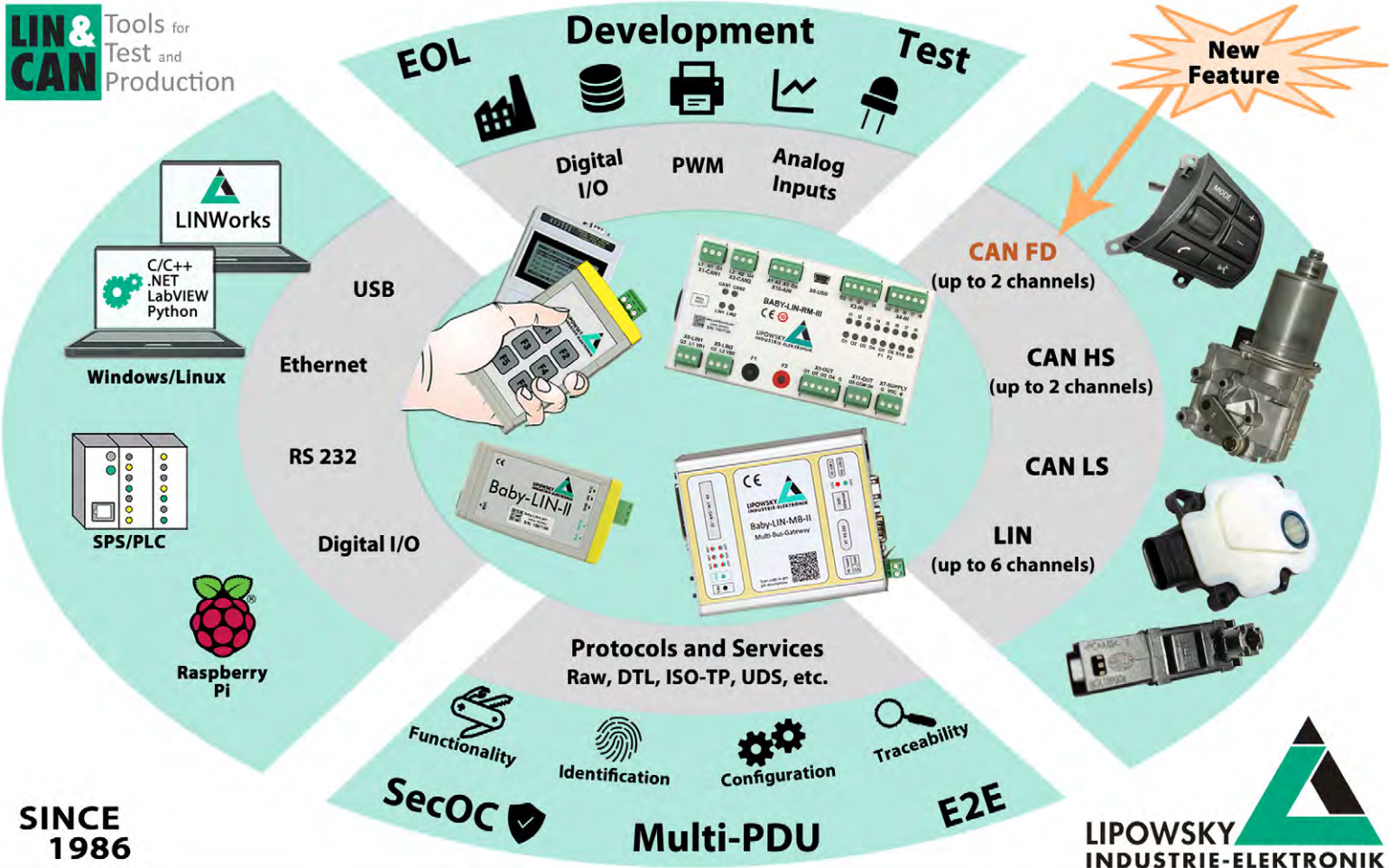| REF	MITIGATION ACCORDING TO UNECE R155 (ANNEX 5)	
M1-M5	(not relevant for embedded software)	
M6	Systems shall implement security by design to minimize risks	NXP ISO/SAE 21434 certified
M7	Access control techniques and designs shall be applied to protect system data/code	
M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data	
M9	Measures to prevent and detect access shall be employed	
M10	The vehicle shall verify the authenticity and integrity of messages it receives	TJA115x configurable CAN ID passlist and blocklist
M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)	
M12	Confidential data transmitted to or from the vehicle shall be protected	
M13	Measures to detect and recover from a denial of service attack shall be employed	TJA115x configurable flooding protection
M14	Measures to protect systems against embedded viruses/malware should be considered	
M15	Measures to detect malicious internal messages or activity should be considered	TJA115x rule set
M16	Secure software update procedures shall be employed	
M17	(M17 is not defined in the standard)	
M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege	
M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions	TJA115x enables IDS identify compromised sender node

Figure 5: The NXP CAN transceivers TJA1152 and TJA1153 enable meeting some of the UNECE R155 security mitigation requirements for CAN networks (Source: NXP)

Author

Karthik Sivaramakrishnan
NXP Semiconductors
karthik.sivaramakrishnan@nxp.com
www.nxp.com

CAN: Much more than just an interface

Megatron expands its range of CAN-capable products. First of all, more CAN sensors will be added to the range. They already preprocess the raw sensor signal inside the sensor housing, so no cost-intensive extra I/O or gateway modules are required to connect to a CAN network.

(Source: fotolia.com – Aleksey Stemmer)

Megatron is continuously expanding its range of CAN-capable products, as more and more customers employ the reliable serial network system. Sensors and joysticks with CAN ensure more efficiency in the industry. First addition to the portfolio will be even more sensors with CAN. They already preprocess the raw sensor signal inside the sensor housing, so that no cost-intensive extra I/O or gateway modules are required to connect to a CAN network.

The CAN system was developed in the 1980s to facilitate the networking of control units in passenger cars. The engineers created a serial interface that offers high data transmission safety, is insensitive to electromagnetic interference, and enables a direct connection of numerous electronic components. As a result, significantly fewer cables are required and thus the total cable length is reduced drastically.

The advantages of bus systems are now appreciated in all areas of industry and medical technology. This is not least due to the extended overall function of the devices: Sensors with CAN feature built-in error checking and filtering. Customers therefore benefit from lower costs for the development of their own electronics or separate evaluation unit. Additional sensors and input devices can be integrated into the CAN network without a great deal of programming effort. This is supported by a modular system that can be optimally adapted to the application requirements.

Figure 1: The CAN rotary encoders of the HTB36E series are the new flag ship product in the Megatron portfolio
(Source: Megatron Elektronik)

CAN sensor

Products with CAN-based higher-layer protocols such as CANopen and J1939 differ significantly from sensors with simple analog outputs. In the case of the former, the measurement signal is smartly processed in the housing of the sensor itself - before it is transmitted to the receiver. The raw signal of the sensor is not only stored, but also undergoes a check, filtering or averaging before it is sent via the CAN.

These products are also flexible when it comes to the power supply. The sensors usually accept a wide input voltage range of up to 32 V. Thus, the sensors can be supplied with power directly from the on-board power supply of a battery-operated machine, for example, without additional conversion or stabilization. This saves additional costs for development, integration, and material. In addition, CAN also allows the history of the device states to be recorded. Errors, alarms, and warnings can be logged and saved. This extended and improved functionality offers more safety, comfort, and information.

Signal processing and transmission with CANopen and J1939

Megatron's CAN products are supplied either according to CANopen or SAE J1939 standards. The CANopen interface is widely-used for applications in various areas of automation technology, in plant construction, and in mobile machines. The CAN J1939 higher-layer protocol is a standard for use in commercial and special vehicles.

The advantages of CANopen can be demonstrated for the case of rotary encoders because various modes for smart signal transmission are available for CANopen. In the asynchronous operating mode, measured values are only transmitted via the network when an internal event occurs, for example only when there is a change of the measured value or after an internal timer has expired. In the synchronous operating mode, the measured value is regularly-transmitted to other network participants as a reply to an external SYNC command. In addition to measured values, these sensors can also output calculated values. In the case of rotary encoders such parameters may be rotational speed or angular velocity, calculated from the angular position.

Figure 2: The fingertip joysticks of the TRY120 series are suitable for mobile applications. They are optionally available with CANopen or J1939 and are therefore predestined for use in mobile machines and vehicles (Source: Megatron Elektronik)

Rotary encoders with CAN

In the rotary encoder product area, Megatron's portfolio is constantly growing - the latest examples are the high-precision CAN rotary encoders HTB36E and FHB58. The digital interface ensures the reliable and digital transmission of the measured values to the application and guarantees smooth integration and monitoring of the rotary encoder. With their magnetic measurement value acquisition and digital signal processing, the sensors form the ideal basis for transmitting measurement signals via CAN. They are metal-housed and are therefore suited for use in harsh environments. In addition, the rotary encoders have a double ball-bearing for a particularly long lifespan and high bearing load and have a high IP protection class. They are available as a multiturn variant with an energy self-sufficient counter (without battery or gear, energy harvesting) for counting revolutions. In addition, due to the patented technology, these variants achieve remarkable system accuracy and repetition accuracy (better than ±0,09°) and can count to 2^{43} revolutions (multiturn resolution up to 43 bits). Another advantage is the free choice of single and multiturn resolutions as well as the automatic detection of the bit rate.

HTB or FHB rotary encoders implement the CANopen device profiles for encoders (CiA 406, version 3.2). The CiA 406 profile series specifies the application interface for absolute rotary and linear encoders. The CANopen specifications were defined by the CiA. Concerning the HTB and FHB rotary encoders the following specifications are from special importance: CiA 301 (CANopen application layer and communication profile), CiA 106 (connector pin assignment), CiA 303 (cabling, representation of units, indicator specification), CiA 305 (configuration of bit rate and node-ID via LSS, CiA 306 (electronic data sheet), and CiA 406 (device profile for encoders).

Mechanisms of communication

There are several different CANopen communication services.

SDO (service data object): for access to the CANopen object dictionary. There is one single SDO channel. Two CAN-Identifiers are assigned to the SDO channel, one for each direction of transmission. For SDO the 8-byte CAN frame is divided into a 1-byte command, a multiplexor of 2-byte index and 1-byte sub-index of the object dictionary, and 4 byte of payload. For bigger payloads either segmented or block transfer is used. An SDO transmission will always be acknowledged by the receiver. In case of a failure an "abort message" is sent. The internal delay time of the HTB and FHB rotary encoders is 1 millisecond maximum.

PDO (process data object): for transmission of process data. The HTB or FHB encoders provide up to four PDOs. A PDO uses the full length of the data field of a CAN frame (8 byte) for the process data without additional overhead. PDOs will not be acknowledged and are suitable for time critical applications. By using the full 8 byte for data, there is no additional information about transmitted objects. Therefore, the PDO producer and the PDO consumer have to define the PDO mapping. ▷

PDOs can be sent on different ways:

- On request: A node sends an RTR frame with the CAN-ID of the designated PDO and the encoder returns the PDO. (CAN in Automation strongly recommends not to use RTR frames. Therefore, RTR is not supported by Megatron rotary encoders)
- Synchronously: On the reception of a SYNC message the node sends its PDOs.
- Asynchronously: The sending of the PDOs is triggered by an internal event (e.g. the internal event timer).

Figure 3: This year, Megatron also launches the 3D joystick Spacemouse Module with CAN. The joystick was specially developed for human-machine interaction in an industrial environment and is used in medical technology and robotics. (Source: Megatron Elektronik)

Joysticks with CAN

Megatron has built up extensive application know-how in numerous customer projects and is very familiar with the requirements. The demand for products with CAN is therefore constantly increasing: "There is great interest in our high-precision rotary encoders and joysticks," reported Christoph Haude, head of product management. That is why Megatron is equipping more and more products with CAN interfaces. Special mention should be made of the Spacemouse Module with CAN interface, which will be launched this year. The innovative 3D joystick was specially developed for human-machine interaction in the industrial sector and enables intuitive control of complex movements - e. g. in robots. And even with classic joysticks, many series are now available with CAN. In addition to the compact fingertip joysticks from the TRY100 and TRY120 series and medium-sized models such as the TRY50 and TRY52, it is above all the robust, large hand grip joysticks from the TRY54 series that rely on the bus system. The latter is only available with CAN, since this protocol is regular in machines for heavy-duty use.

The electronics expert Megatron specializes in customized sensor and joystick solutions. The product range is based on the needs of customers and is constantly optimized. Customer proximity, flexibility, and product quality obviously pay off: More and more manufacturers of special vehicles, mobile machines as well as plant manufacturers use CAN products from the company in their applications. The portfolio also includes rotary encoders with analog or incremental interfaces, as well as numerous joysticks in analog or USB versions. The Bavarian company offers a special service: All products are individually modified on request, even in relatively small quantities. "Our goal is to find the best possible solution for the customer in terms of functionality and cost-effectiveness of the application," said Managing Director Thomas Volkwein, describing the company's philosophy. ◀

Author

Matthias Hermann
Megatron Elektronik
info@megatron.de
www.megatron.de

CAN FD open-source IP core

The Faculty of Electrical Engineering (FEE) at Czech Technical University in Prague (CTU) reached another milestone in July 2022. Their CAN FD IP offer is fully supported by a mainline Linux kernel. According drivers, emulation, and applications are available.

(Source: Adobe Stock)

Now, the CTU FEE team offers CAN FD solutions fully supported by the mainline Linux kernel version 5.19 after four years of the out-of-tree support. The VHDL (very high-speed integrated circuits hardware description language) design integration is available for PCI-express Cyclone FPGA-based cards, Xilinx Zynq, and Intel SoC (system on chip) systems. The work is ongoing on optional extension with the parity bits support for fault-tolerant space applications. The core functional emulation is available in the QEMU (open-source system and user-level emulator) emulator out of the box from the year 2020. This enables continuous integration testing against the actual Linux kernel and provides a valuable tool for the driver-porting to other operating systems.

Historical background

The CTU CAN FD design started at the CTU FEE Department of Measurement under the lead of Jiří Novák to extend their long-term CAN testing support for Volkswagen and Skoda Auto by CAN FD.

CTU activities in the area of real-time distributed control and communications (fieldbus area) started in the early 1990s when the CTU experts were invited to participate in the joint project with PTB Berlin (Physicalisch-Technische Bundesanstalt, German Metrology Institute) focused on electromagnetic susceptibility of fieldbus technologies in harsh industrial environments. Simultaneously the university cooperated with the Czech company Unicontrols on the implementation of an extensive CANopen design and development

system. Within this cooperation, the team has focused on a dual-CAN interface implementation. This included the channel redundancy, message queuing, and timestamping in both directions. The developers also have worked on the interface's driver support for several hardware platforms as well as real-time operating systems (e.g. OS9, VxWorks) and generic OS systems (e.g. GNU/Linux, Windows).

In the middle 1990s, the CTU team was contacted by Volkswagen to design and develop an in-vehicle system for identification of the CAN network error sources within the car. On this basis, a long-term cooperation with Škoda Auto began, which is still ongoing. Within the 20 years, the engineers designed, developed, and deployed many technologies that were used for testing during the vehicle development. Here are two examples. The first is an automated test system for CAN/LIN ECUs (electronic control unit). It implements a list of tests that ECUs should pass at the physical, data-link, and application layers. The tests are focused on the behavior within the networked system, not on the individual ECU functionality. The second example is a HIL (hardware in the loop) system for overall vehicle integration tests. The Skoda Fabia and Skoda Scala vehicles were completely tested using this system.

Pavel Píša (FEE Department of Control Engineering at CTU) and his students from the department also contributed to the open-source technologies as well as the real-time and control-related projects starting in the 1990s. Drivers for data acquisition, control cards, and devices have been developed during the years. Investments into the generic Linux CAN (LinCAN) support preceded even ▷

Semiconductors

the SocketCAN sub-system. When the community chose SocketCAN as the preferred solution, the knowledge and some card supports were reused. An updated bit-timing-parameter computation algorithm has been developed and is the base for the generic CAN and CAN FD bit-rate setup till now. The need for a common platform for the CAN driver development and testing emerged during the work on the RTEMS system (real-time executive for multi-processor systems). The QEMU emulator CAN sub-system has been designed based on previous experience with the Humusoft data acquisition cards emulation. The work, initially supporting SJA1000 CAN controller (NXP) only, has been accepted for QEMU mainline in 2018 and is a base for the Xilinx controllers and CTU CAN FD emulation support.

CTU CAN FD IP core

Figure 1 shows the CAN FD IP core structure with Rx and Tx paths. The IP core provides the following features:

◆ VHDL design with no vendor-specific libraries required, yet RAM for buffers and Rx FIFO automatically inferred by Xilinx and Intel tools
◆ Compliant with ISO 11898-1:2015
◆ Rx buffer FIFO with 32 to 4096 words (1 to 204 CAN FD frames with 64 bytes of data)
◆ 2 to 8 TXT buffers (one CAN FD frame in each TXT buffer)
◆ 32-bit device memory interface (APB, AHB, RAM-like interface)
◆ Support of "ISO and non-ISO" conform CAN FD implementations
◆ Time-stamping and time-triggered transmission
◆ Interrupts
◆ Loop-back mode, bus monitoring mode, ACK forbidden mode, self-test mode, restricted operation mode

The CTU CAN FD IP core is optimized for 32-bit register access from the main CPU (central processing unit) connected over APB, Avalon, AXI bridge, etc. The core provides a synthesis-time-configurable depth FIFO on the reception side and four (optionally two or eight) transmission buffers, of which the transmission order can be controlled by individually assigned priority. Priority assignment is controlled by up to eight four-bit fields in one register, which allows maintaining the Tx FIFO order: a requirement for standard SocketCAN setup. Still, it allows a division of the Tx buffers into multiple priority queues or can even be combined with the time-triggered postponed release of selected buffer(s).

The design allows precise hardware time-stamping of the received frames. A time-stamp counter common for multiple CAN channels can be integrated into FPGA or SoC design with a resolution of up to 64 bit. Hardware time-stamp support for the corresponding SocketCAN driver is already developed and will be contributed to the 5.20 or following Linux kernel releases. Precise (10 ns in CTU's design) time-stamping and deep Rx FIFO make the core suitable for latency evaluation and continuous integration checks of operating systems, different CAN controllers, and software performance. Such quality-assuring setup ensures that the kernel update is safe and will not cause problems for a given project or third-party controller in the future.

To prevent regressions in their own CTU CAN FD development process, the developers have set up complete systems, which allow analyzing of multiple CAN cores connected with a parametrized connection jitter and topology. More than 160 unit-tests and complex tests have run, as well as almost 200 another tests were precisely reimplemented according to the ISO 16845-1:2016 standard. All these pipelines have run in the environment based on the open-source GHDL GCC frontend for each design change. The complete synthesis of the Xilinx Zynq SoC design and the build driver have run nightly after each CTU CAN FD core repository
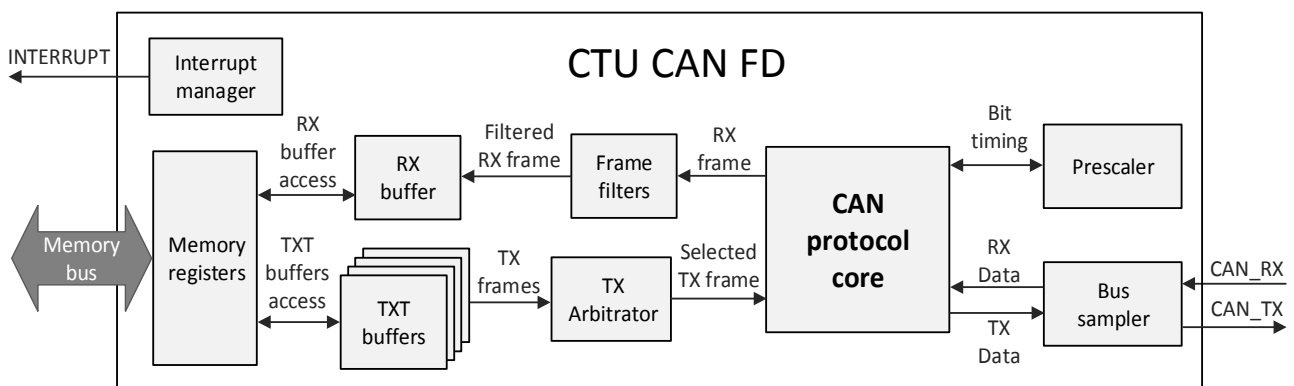

Figure 1: CTU CAN FD IP core structure (Source: CTU)

Ondrej Ille is a digital design expert working for several chip design centers. The initial goal of his work on a new core VHDL design was a specialized controller for CAN FD Skoda Auto analyzer update with support for time-based transmission of messages. In 2018, it was extended into development of a generic CAN FD controller to support the needs of the Volkswagen subsidiary to replace the commercial core. The latter did not fit in a required count into their Xilinx Zynq based project limited by the already produced hardware.

update. Generated artifacts were copied to Xilinx Zynq based MZ_APO education kit, where multiple tests, including interoperability with the Opencores SJA1000 controllers, have run.

CAN latency testing

One of the CTU CAN FD IP core applications is the latency testing of a CAN gateway based on the team's own or on third-party controllers. Figure 2 shows the testing setup. ▷

There are two MZAPO boards based on the Xilinx Microzed boards with Zynq 7000 SoC. The bottom board does the benchmarking, and the top board is a device under test (DUT). Any CAN gateway device can be used as a DUT. The FPGA in Xilinx Zynq SoC is loaded with a design composed of four CTU IP cores and a software-controlled 4 x 4 x 2 CAN cross-bar. The goal of the latency testing is to continuously evaluate new versions of the Linux kernel, specifically the latencies of CAN gateways in the kernel and the user space.
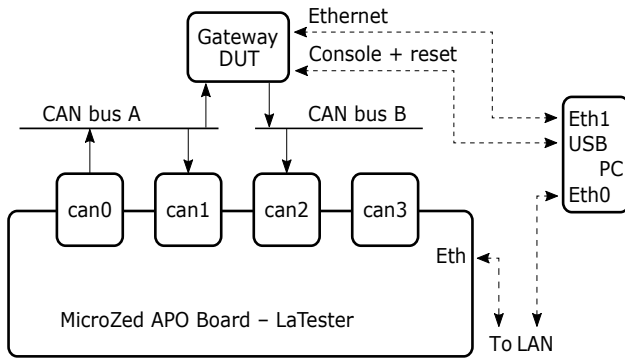

Figure 2: Testing setup for latency testing (Source: TCU)

The kernel is compiled for every new kernel version, booted on the DUT board, and tests are started on the Latester board (Latency Tester) equipped with CTU CAN FD. During the tests, a CAN message is repeatedly sent from the Latester interface can0 and immediately received on can1 to obtain a precise hardware time-stamp. And, after the gateway (DUT) copies the message from CAN bus A to CAN bus B, the message is time-stamped again when received on the Latester can2 interface. The gateway latency is obtained by simply computing the difference of the time-stamps. Then, the distribution of latencies can be plotted and analyzed. Integration of this latency testing into OSADL's QA farm is in progress.

The system has been successfully used even during the development of CAN NuttX RTOS driver for Espressif ESP32C3 RISC-V based micro-controller.

The Latester setup uses a 64-bit time-counter, and the CTU CAN FD design is running on 100 MHz, which provides an excellent 10-ns time-stamp resolution. Linux driver for CTU CAN FD IP core has been already mainlined, and the time-stamping support in the driver is on the way. ◄

References

[1] CTU CAN FD IP core project
[2] CTU CAN FD IP CORE Datasheet, Czech Technical University in Prague, Faculty of Electrical Engineering, Department of Measurement
[3] CAN bus related projects list and CTU CAN FD IP core automatic tests results at Czech Technical University in Prague, Faculty of Electrical Engineering
[4] CTU CAN FD Driver Linux kernel mainline documentation
[5] QEMU CAN emulation and subsystem documentation
[6] Martin Jeřábek: FPGA Based CAN Bus Channels Mutual Latency Tester and Evaluation, Bachelor Thesis, CTU FEE, 2016
[7] Martin Jeřábek: Open-source and Open-hardware CAN FD Protocol Support, Master Thesis, CTU FEE, 2019
[8] Matěj Vasilevski: CAN Bus Latency Test Automation for Continuous Testing and Evaluation, Master Thesis, CTU FEE, 2022

Authors

Ondrej Ille
Czech Technical University in Prague (graduate)
ondrej.ille@gmail.com
www.cvut.cz

Jiří Novák
Czech Technical University in Prague
FEE, Department of Measurement
jnovak@fel.cvut.cz
meas.fel.cvut.cz

Pavel Píša
Czech Technical University in Prague
FEE, Department of Control Engineering
pisa@fel.cvut.cz
control.fel.cvut.cz

Matěj Vasilevski
Czech Technical University in Prague (graduate)
matej.vasilevski@gmail.com
www.cvut.cz

Semiconductors

CANopen powers subway auxiliary inverters

Leroy introduces how to implement some key features of auxiliary inverters' management onto commercial-off-the-shelf (COTS) technologies: the Brio hardware platform. In the context of the New York City Transit – R211 subway project, the platform acts as a remote input/output module based on CANopen.

Leroy Automation is manufacturer of automation systems for on-board train and rail signaling control-command systems. For several decades, they have been accompanying major rolling stock manufacturers, locomotive subsystem integrators, and original equipment suppliers for rolling stock vehicles as well as for many train fleet overhaul projects.

As part of on-board train architectures, energy management is an important topic where efficient power converters are key subsystems. Thanks to the auxiliary power converters or inverters, the current-voltage characteristics can be adjusted to match the requirements of subsystems installed into subway cars and railway vehicles. They also fulfil a significant role in safety by protecting the entire system, as they are resistant to over-voltages and short-circuits. The intelligence of the auxiliary inverters is implemented onto powerful embedded controllers, where high-speed digital signal processing tasks are common.

Figure 1: The Brio R107 CANopen-based PLC (Source: Leroy)

The hardware platform

Brio is an Ethernet-based decentralized-remote input/output module, designed to be embedded on-board in rolling stock vehicles. It is available as a product range offering different digital and analog inputs/outputs configurations, and several communication interfaces such as CAN, Ethernet, EIA-485, MVB, etc. In general, Brio finds its use cases in embedded railway systems like a programmable logic controller (PLC) or a remote input/output module (RIOM); where digital and analog I/Os are managed from one or several communication ports. Nevertheless, its internal hardware architecture is based on a powerful STM32 micro-controller and an FPGA device, which makes it suitable for various applications.

In the context of the New York City Transit – R211 subway project, the platform acts as a remote input/output module based on CANopen. Fully compliant with the EN 50155 railway standard, it counts not less than 55 I/O signals on a thin size-6U board footprint. It is the ideal COTS solution to be integrated in train propulsion systems. In parallel, the company has been asked to think about an innovative solution for the Brio to be able to detect in real-time a ripple voltage on a high-voltage DC line around 900 V_{DC}. The technical specification was restrictive: the AC ripple signal can range from 0,35 V_{rms} to 70 V_{rms}, and can be on any two frequencies between 0 kHz and 1 kHz. In addition, the system had to be fully configurable and monitored from the CANopen interface (ripple frequencies to be detected, detection temporal window, V_{rms} threshold to declare the ripple present or not, measured energy for both frequencies), and had to activate specific digital outputs on frequency detection.
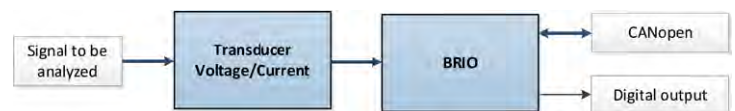

Figure 2: The final system solution could be presented as the following system-level block diagram (Source: Leroy)

In digital signaling processing (DSP), the DFT (discrete fourier transform) is a tool to find a specific frequency in a signal. Simulations have shown that a DFT linked to Hann windows, gave good results with an acceptable accuracy on signals recorded on train. The DFT equation by itself is not so complex:

$$X(k) = \sum_{t=0}^{N-1} x(t) e^{-i\frac{2\pi k}{N}t}$$

It just says that "X(k)" is the level of the frequency "k" in the complete signal represented by a set of "N" samples "x(t)" of the analyzed signal.

The Hann window consists in deforming the analyze signal before applying the DFT algorithm. Indeed, the DFT implies a temporal windowing of the signal over N samples, which affects the signal spectrum. Applying a pre-deformation such as Hann windows prior to the DFT improve the frequency response of the DFT.

The Hann window is also not very complex in terms of digital signal processing function. For a set of N samples, it gives a coefficient to apply on the sample "t" by the following formula:

$$w(t) = 0.5 \times \left[1 - \cos\left(\frac{2\pi t}{N}\right) \right]$$

In order to illustrate the efficiency of the Hann window, let's take a pure sinus signal. ▷
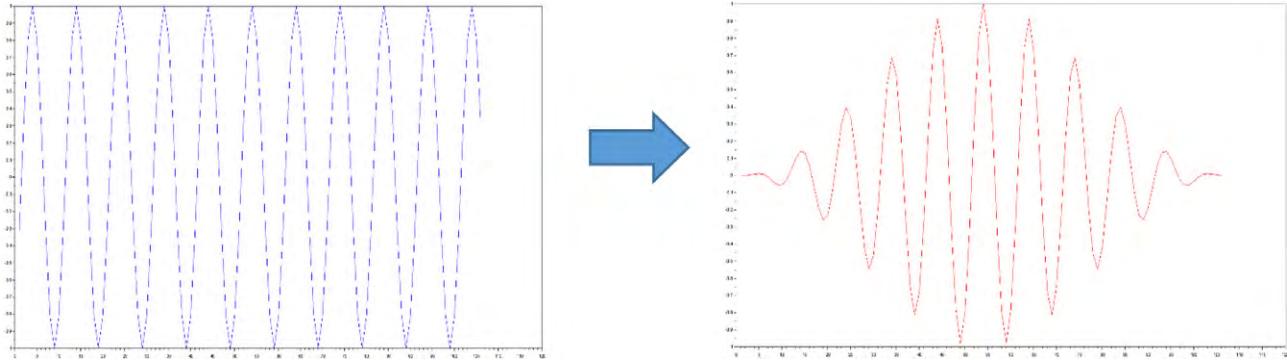
Figure 3: Representation of Hann function in time domain (Source: Leroy)
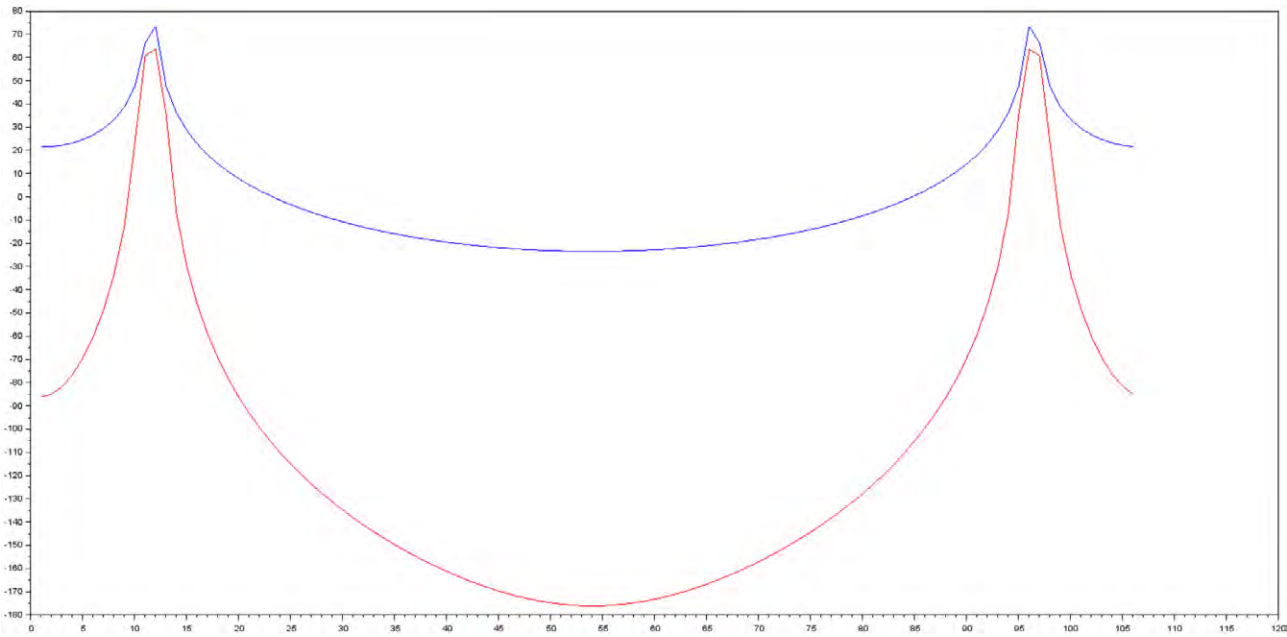

Figure 4: Representation of Hann function in frequency domain (Source: Leroy)

We can see that in frequency domain, the spectrum representation gives much better results with Hann window than without. Indeed, the energy peaks that characterize the harmonics of the original signal are much clearer in red, which allows a frequency detection with a better accuracy. Thus, in order to detect two specific frequencies "K1" and "K2" in the analyzed signal, the algorithm to implement can be seen in Figure 5.
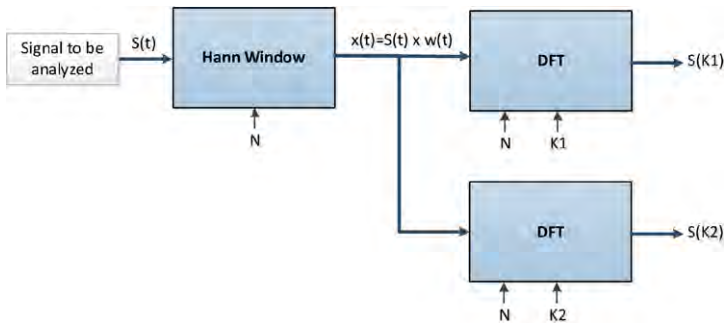

Figure 5: Digital signal processing – Hann window and discrete fourier transforms (DFT) (Source: Leroy)

It is one thing to make an offline simulation on a Windows-based PC, with mathematical tools. But it is another challenge to make the same in real-time, in an on-board PLC, with the very same accuracy.

As mentioned earlier, the Brio is based on a STM32 micro-controller and an FPGA device. It could have been easy to implement the algorithm in the micro-controller. A few ANSI-C programming lines would have been enough. Nevertheless, the micro-controller was already busy to manage the other functionalities of the Brio itself, including CANopen messages, and the real-time criteria would have been difficult to meet. It was then decided to implement the algorithm in the FPGA device. At this point, the difficulty remains in implementing calculus in the hardware chip. Indeed FPGAs, and specifically small matrices, are not adapted well for floating-point computing with cosine and sine functions. The idea was to take benefit of each device strength with a modular design approach: micro-controller for complex floating-point and cosine/sine off-line calculus, FPGA for real-time fixed-point computing. The real-time part of the algorithm implemented in the FPGA can be represented as shown in Figure 6.

Each time a parameter is modified (window size, K1, K2, sampling frequency), the micro-controller computes only once the five tables that contain cosine and sine coefficients needed by the Hann window and the DFT. Furthermore, the FPGA only needs to perform simple operations such as multiplications and additions, for which it is very well suited. The digital part of the algorithm worked fine but a challenge remains. The signal to analyze is composed of a DC part that can be up to 1000 V_{DC}. On the other hand, the ripple ▷

Figure 6: FPGA algorithm implementation – Hann window and DFT (Source: Leroy)
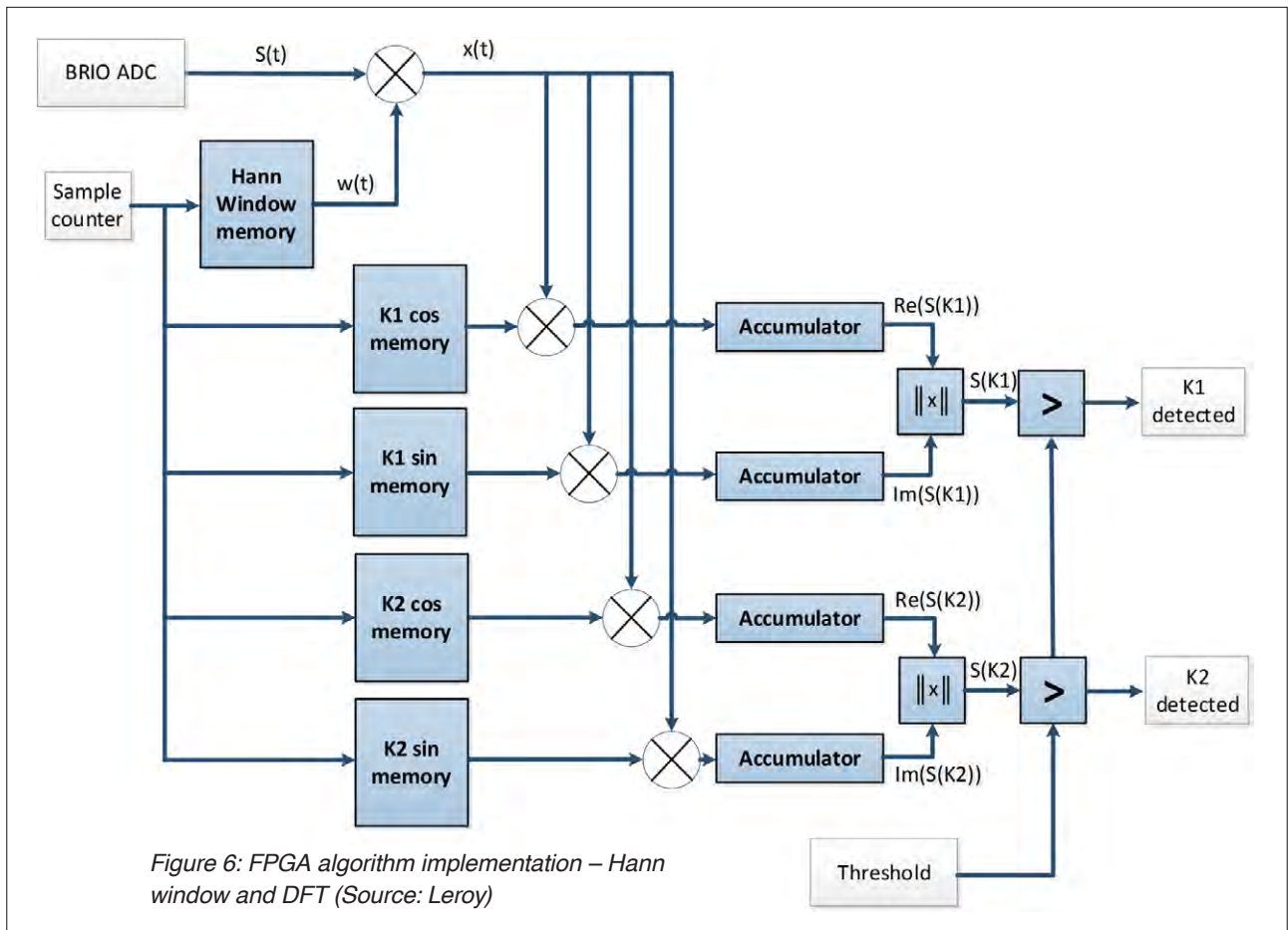
can be as low as 0,5 V_{AC}. It was necessary to remove the DC part of the signal in order to keep most of the ADC (analog digital converter) resolution for the AC part. It was also necessary to keep the low-pass filter required before any analog-to-digital conversion. The resulting band-pass filter has then required a lot of calculus and simulations to be flat enough over the required frequency range, and for the whole temperature range (from -40 °C to +70 °C). It had also to fit the small footprint available on the Brio printed-circuit board (PCB). At the end, we were able to modify one analog input of the Brio to implement the band-pass filter shown in Figure 7.
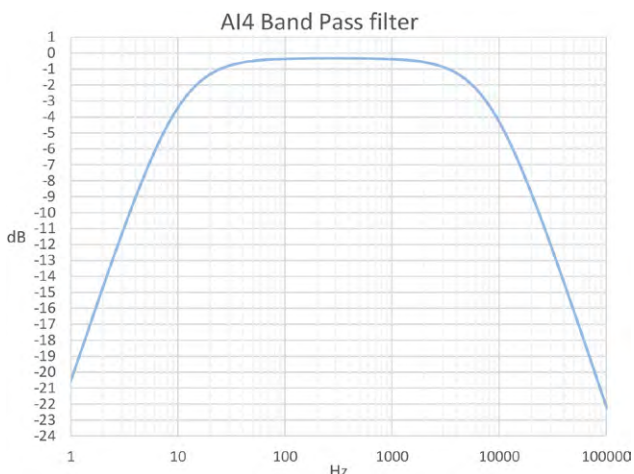

Figure 7: Implementation of band-pass filter in FPGA device (Source: Leroy)

At this time, interfacing the frequency detection system with the CANopen stack was the easiest part of the project. Some specific PDO messages have been implemented to configure dynamically the detection parameters and to report the detection results in a very efficient way.

As a conclusion, this project has been a great engineering success. Operational tests on-board subway cars gave excellent results, totally in line with theory and simulations. Brio was already known as a highly available and reliable I/O module with PLC-programming capabilities. But this particular auxiliary inverter application has revealed all the potential and benefits of the Brio hardware with the partitioning of digital signaling processing algorithms and techniques onto a mixed FPGA and micro-controller platform. ◄

Author

David Rambaud
Leroy Automation
info@leroy-autom.com
www.leroy-automation.com

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.

SAE J3271/2 references CAN

SAE has launched the SAE J3271-Air7357 Megawatt Charging System Standards (MCS) for all large-battery vehicles that roll, fly, or float. A task force of industry stake holders and subject matter experts was launched in 2018 as the CharIN Megawatt Charging System (MCS). As an industry group, it developed documents and specifications that can be used by Standards Developing Organizations (SDOs). The white paper of MCS specifications is due to be released in summer of 2022. SAE has developed the J3271/2 Technical Information Reference (TIR) document referencing a CAN communication. ◼

ISO 11898-2 submitted for DIS ballot

The reviewed and updated ISO 11898-2 standard (Controller Area Network – Part 2: Physical medium attachment sub-layer) has been submitted to national standardization bodies for DIS (Draft International Standard) balloting. It comprises requirements for high-speed (HS), signal improvement capability (SIC), and SIC XL (mode switching) transceivers. The HS and SIC transceivers use non-return-to-zero (NRZ) coding. The CAN XL transceivers supports additionally a pulse-width modulation (PWM) coding. The benefit for chipmakers, all requirements are in one document including sleep and selected wake-up functionality. ◼

ISO 11783-13 (file server) released

ISO has released a new edition of the Isobus file server standard. The ISO 11783-13 document specifies a set of messages providing access to a file server (FS). An FS is a distinct control function (CF) on the mobile implement control system that enables all CFs to store or retrieve data from a file-based storage device. The ISO 11783 series specifies a CANbased communication based on J1939 protocols, intended for agricultural and forestry vehicles. ◼

New SAE 1939 documents

Beginning of August, SAE has published the next version of the J1939 Digital Annex (DA). The DA is updated quarterly. Among others, this spreadsheet specifies suspect parameters or parameter groups.

In August, also the SAE J1939-73 application profile specification has been released. It specifies the SAE J1939 diagnostic messages (DMs) to accomplish diagnostic services. Additionally, it identifies the diagnostic connector to be used for the vehicle service tool interface. DMs provide the utility needed when the vehicle is being repaired. They are also used during vehicle operation by the networked ECUs (electronic control units) to allow them to report diagnostic information. DMs include services such as periodically broadcasting active DTCs (diagnostic trouble codes), identifying operator diagnostic lamp status, reading or clearing diagnostic trouble codes, reading or writing control module memory, providing a security function, stopping/starting message broadcasts, reporting diagnostic readiness, monitoring engine parametric data, etc. California-, EPA-, or EU-regulated OBD requirements are satisfied with a subset of the specified connector and the specified DMs. ◼

CiA 1305 released

The CiA 1305 document specifies the layer setting services (LSS) for CANopen FD. These services are used to communicate between an LSS manager (typically residing in the CANopen FD host controller featuring NMT manager functionality) and LSS servers. They enable the LSS manager to modify the LSS server's CANopen FD network-ID and node-ID. LSS provide means to modify the CAN FD bit-timing parameters (for nominal bit rate and data-phase bit rate) in all CANopen FD devices.

The entire 128 bit of the CANopen FD identity array (vendor-ID, product-code, revision number, serial number, as specified in CiA 1301) make the LSS address. The LSS address is a worldwide unique identifier addressing a CANopen FD device. Therefore, an LSS manager can differentiate between several LSS servers, by means of the LSS address, even if these LSS servers do not own a valid network-ID or node-ID. Via the LSS switch state selective FD command, the LSS manager forces exactly one LSS server to enter the LSS configuration state. In this state, the LSS server accepts a new network-ID or node-ID that is determined by the LSS manager. It is the LSS manager's task to ensure that during the assignment of the network-ID or node-ID, there is only one LSS server in the LSS configuration state.

In case the LSS addresses of the LSS servers are unknown to the LSS manager, the LSS manager can have several means to detect the LSS server's address. In case the LSS server own already a valid network-ID and node-ID, the LSS manager just reads the content of the identity array (data object 1018_h) of all LSS servers in the network using the USDO (universal service data object) service. In case the LSS servers do not own a valid network-ID and node-ID, the LSS manager has to rely on additional LSS services. The LSS switch state selective FD service, enables the LSS manager to scan via 4-bit-nibble-masks, whether there exists an unconfigured LSS server, that's LSS address is in a given LSS address range. By executing several scanning cycles, the LSS manager can identify exactly one unconfigured LSS server and provides subsequently a valid CANopen FD network-ID and node-ID.

LSS enables the LSS manager to switch the entire CANopen FD network from one pair of nominal bit rate and data-phase bit rate, to another. The LSS manager configures via LSS in all CANopen FD devices in the network the intended bit-timing parameters, individually. After the successful configuration, the LSS manager requests the bit-timing switch, by means of a global LSS service. After a switch delay, all devices in the CANopen FD network operate on the new nominal and data-phase bit rates.

It is recommended to use the switching of LSS bit-timing parameters carefully. In case there is at least one device that is not switching correctly, a proper CANopen FD communication is not more guaranteed. One or more CANopen FD interfaces enter the CAN bus-off state. They cannot be accessed anymore. Only in another network, running on the configured bit rates, these devices can be re-configured. For the initial adjustment of the CANopen FD bit-timing parameters, the LSS bit-timing switch service is not suitable. For such scenarios, methods such as the CANopen automatic bit rate detection (CiA 801) can be used, in an adapted format, suitable for CANopen FD.

If several unconfigured LSS servers exist in a CANopen FD system, they can be identified by means of the
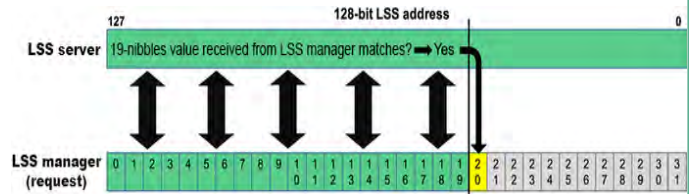

Figure 1: The LSS manager sends a request for nibble 20 of the 128-bit LSS address; the LSS servers, which have matched the previous 19 nibbles provide a response with the nibble 20 values indicated by the CAN-ID (e.g. $07DA_h$ for the value A_h)

LSS switch-state selective FD service. To perform this service, the 128-bit LSS address is divided into 32 pieces (nibbles). The LSS manager consequently asks the LSS servers for the values of each nibble. Sixteen CAN FD data frames with the CAN-IDs from $07D0_h$ to $07DF_h$ are used as possible feedback. When the LSS manager requests the value of the first nibble, the LSS servers reply with the CAN-ID $07D0_h$ if their first nibble is zero. The CAN-ID $07D1_h$ is used, if the nibble is one and so forth (CAN-IF $07DF_h$ if the nibble values 0Fh). The LSS manager takes the first response (all others are ignored for this cycle) and packs the first nibble value into the next request. The LSS servers with the first matching nibble inform the LSS manager about the second-nibble value using the 16 LSS messages with the mentioned CAN-IDs. This cycle is repeated until all nibbles have been processed and a single, unconfigured LSS server is identified. Then, the LSS manager can assign the network-ID and the node-ID to a single LSS server.

To decrease the boot-up time in CANopen FD systems this procedure can be modified. The LSS manager software can store LSS addresses that have been identified. On each power-up, the LSS manager can try those LSS addresses first and if there is then still an unconfigured LSS server left in the system, the LSS switch-state selective FD cycle is started. ∎

CiA profiles released as DS

CiA has released several profile specifications in DS (Draft Specification) status. This means, they are now part of the CiA 400 series subscription. CiA specifications in DSP (Draft Specification Proposal) state are available only for CiA members. Documents in PAS (Public Available Specification) state are downloadable free of charge from the CiA website.

The DS stage upgraded profile specifications include:
- CiA 442: CANopen profile for IEC 61915-2 compatible motor starters
- CiA 444 series; CANopen profiles for container-handling machine add-on devices
- CiA 445: CANopen device profile for RFID devices
- CiA 453: CANopen device profile for power supplies
- CiA 458: CANopen device profile for energy measurements

CiA plans to upgrade additional CiA profile specifications to DS state, to make them available for the entire CAN community. Several profile specifications are under review to follow the new profile specification structure. In the future, profile specification series will comprise a Part A with parameter specifications, a Part C specifying the mapping to classic CANopen and a Part F for the mapping to CANopen FD. Additionally, there could be specified mappings to J1939 (Part J) or to other higher-layer protocol approaches. ∎

Brief news

Get the CAN-related knowledge!

Online seminars	Date	Language
CAN	2022-09-27	English
CANopen	2022-09-28	English
CAN	2022-11-30	English
CANopen	2022-12-01	English

Onsite seminars	Date	Language
CAN	2022-10-12	German
CANopen	2022-10-13	German

Webinars	Date	Language
CAN in rail vehicles	2022-09-08	English
CAN XL - Status 2022 and future	2022-10-06	English
CANopen FD - Status 2022	2022-11-17	English
CAN XL - Status	2022-12-08	Chinese

Technology days	Date	Language
Chinese CiA technology day	2022-09-19	Chinese
CiA in action technology day	2022-12-06	English

Workshop	Date	Language
CAN in rail vehicles	2022-09-30	English
CAN in laboratory automation	2022-10-06	English
Battery and energy management	2022-12-13	English

Subject to change without notice.

CiA in-house seminars

CiA engineers discuss your urgent CAN-related issues that are currently of high interest with regard to your projects.

For more details please contact CiA office: events@can-cia.org

www.can-cia.org